



User's Manual

Wireless LAN Access Point/Bridge

Model No.: SP912GH

<http://www.micronet.info>

Table of Contents

1	INTRODUCTION	4
1.1	FEATURES & BENEFITS	4
1.2	PACKAGE CONTENTS	5
1.3	UNIT DESCRIPTION	5
1.4	SYSTEM REQUIREMENTS	5
1.5	APPLICATIONS	5
1.6	NETWORK CONFIGURATION	6
a)	Ad-hoc (peer-to-peer) Mode	6
b)	Infrastructure Mode	7
2	UNDERSTANDING THE HARDWARE	8
2.1	HARDWARE INSTALLATION	8
2.2	IP ADDRESS CONFIGURATION	8
3	CONFIGURE SP912GH IN BRIDGE/ BRIDGE ROUTER/ AP	10
3.1	BRIDGE/BRIDGE ROUTER TO ACCESS POINT	10
3.2	ACCESS POINT TO BRIDGE / BRIDGE ROUTER	11
4	BRIDGE MODE – WEB CONFIGURATION	12
4.1	LOGGING IN	12
4.2	MANAGEMENT	13
4.2.1	OPERATION MODE	14
4.2.2	STATUS	15
4.2.3	STATISTICS	16
4.2.4	LOG	17
4.2.5	UPGRADE FIRMWARE	18
4.2.6	SAVE / RELOAD SETTINGS, RESET TO DEFAULT	19
4.2.7	PASSWORD	20
4.3	TCP/IP SETTINGS	21
4.3.1	LAN INTERFACE	21
4.3.2	SNMP SETTINGS	22
4.4	WIRELESS	23
4.4.1	BASIC SETTINGS (INFRASTRUCTURE, ADHOC)	23
4.4.2	ADVANCED SETTINGS (INFRASTRUCTURE, ADHOC)	24
4.4.3	SECURITY	26
4.4.3.1	ENCRYPTION DISABLED	26
4.4.3.2	WEP 64-BIT / 128-BIT	27
4.4.3.3	WPA / WPA2 PASSPHRASE	28
4.4.3.4	WPA / WPA2 RADIUS AUTHENTICATION	29
4.4.4	SITE SURVEY	30
5	ACCESS POINT MODE – WEB CONFIGURATION	31
5.1	LOGGING IN	31
5.2	MANAGEMENT	32
5.2.1	OPERATION MODE	33
5.2.2	STATUS	34
5.2.3	STATISTICS	35

5.2.4	LOG	35
5.2.5	UPGRADE FIRMWARE	36
5.2.6	SAVE / RELOAD SETTINGS, RESET TO DEFAULT	37
5.2.7	PASSWORD	37
5.3	TCP/IP SETTINGS	38
5.3.1	LAN INTERFACE	38
5.3.1.1	STATIC IP ADDRESS	38
5.3.1.2	DHCP CLIENT	39
5.3.1.3	DHCP SERVER	40
5.3.2	SNMP SETTINGS	41
5.4	WIRELESS	41
5.4.1	BASIC SETTINGS	41
5.4.2	ADVANCED SETTINGS	42
5.4.3	SECURITY	45
5.4.3.1	ENCRYPTION DISABLED	45
5.4.3.2	WEP 64-BIT / 128-BIT	46
5.4.3.3	WPA / WPA2 / WPA2 MIXED PASSPHRASE	47
5.4.3.4	WPA / WPA2 / WPA2 MIXED RADIUS AUTHENTICATION	48
5.4.3.5	ACCESS CONTROL	49
5.4.3.6	WDS	50
5.4.3.7	WDS SECURITY SETUP	50
SPECIFICATIONS		52

1 Introduction

Micronet Wireless LAN Access Point/Bridge SP912GH operates seamlessly in the 2.4 GHz frequency spectrum supporting the 802.11b (2.4GHz, 11Mbps) and faster 802.11g (2.4GHz, 54Mbps) wireless standards. It's the best way to add wireless capability to your existing wired network, or to add bandwidth to your wireless installation.

SP912GH has high transmitted output power and high receivable sensitivity. High output power and high sensitivity can extend range and coverage to reduce the roaming between APs to get more stability wireless connection. It also can reduce the expense of equipment in the same environment.

To protect your wireless connectivity, it can encrypt all wireless transmissions through 64/128-bit WEP data encryption and also supports WPA/WPA2. The MAC address filter lets you select exactly which stations should have access to your network.

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

1.1 Features & Benefits

Features	Benefits
High Speed Data Rate Up to 54Mbps	Capable of handling heavy data payloads such as MPEG video streaming
High Output Power and High Sensitivity	Spreads the operation distance and reduce the roaming between APs to get more stability wireless connection
Point-to-point, Point-to-multipoint Wireless Connectivity	Let users transfer data between two buildings or multiple buildings
WPA2/WPA/ IEEE 802.1x Authenticator support	More Powerful data security
WDS (Wireless Distribution System)	Make wireless AP and Bridge mode simultaneously as a wireless repeater
Watertight and Weatherproof	Avoid water invaded and weather corroded
Wide temperature range and robust mechanical design	Delivers reliable, top performance in the most demanding environments
MAC address filtering (AP Mode)	Ensures secure network connection
Power-over-Ethernet (IEEE802.3af Compliant)	Flexible Access Point locations and cost savings

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 SP912GH Unit
- One Power Adapter (12V/ 1A)
- One Omni directional Antenna
- One CD-ROM with User's QIG

1.3 Unit Description



1.4 System Requirements

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

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

1.5 Applications

SP912GH is 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

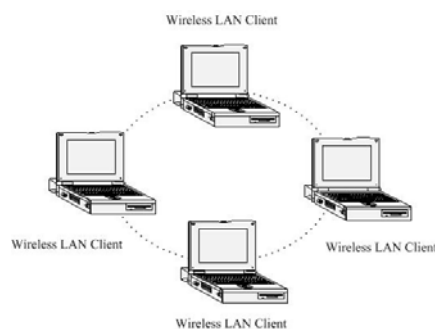
Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

1.6 Network Configuration

To better understand how SP912GH 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:

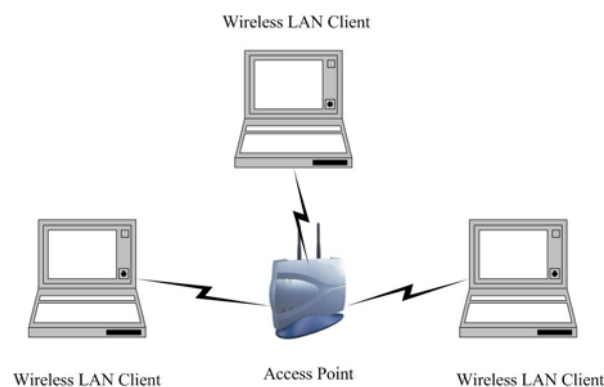
a) Ad-hoc (peer-to-peer) Mode

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.

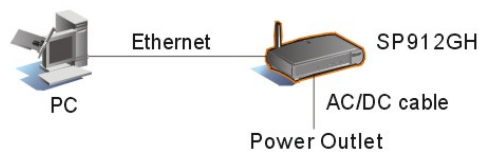


2 Understanding the Hardware

2.1 Hardware Installation

1. Plug one end of Ethernet cable into your PC/Notebook and the other end into SP912GH port labeled “RJ-45/PoE”.
2. Insert the DC-inlet of the power adapter into the power socket on the wall.

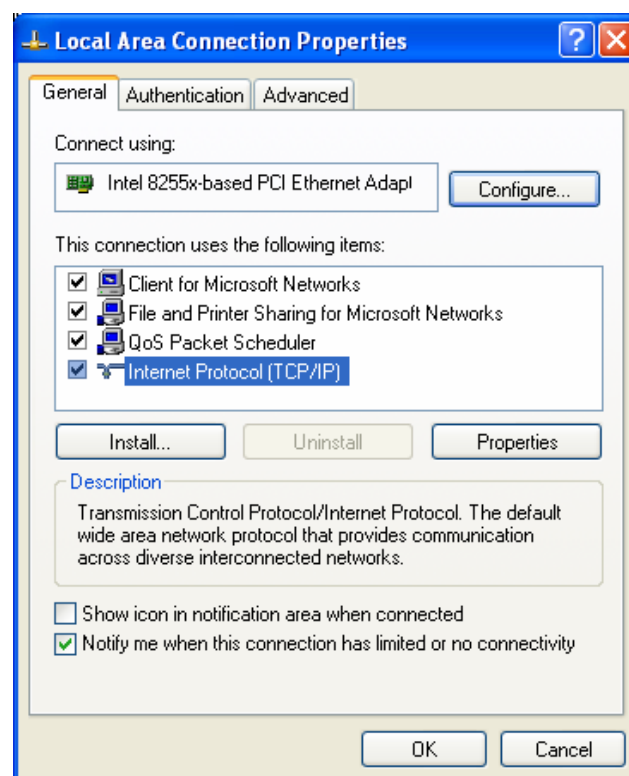
This diagram depicts the hardware configuration



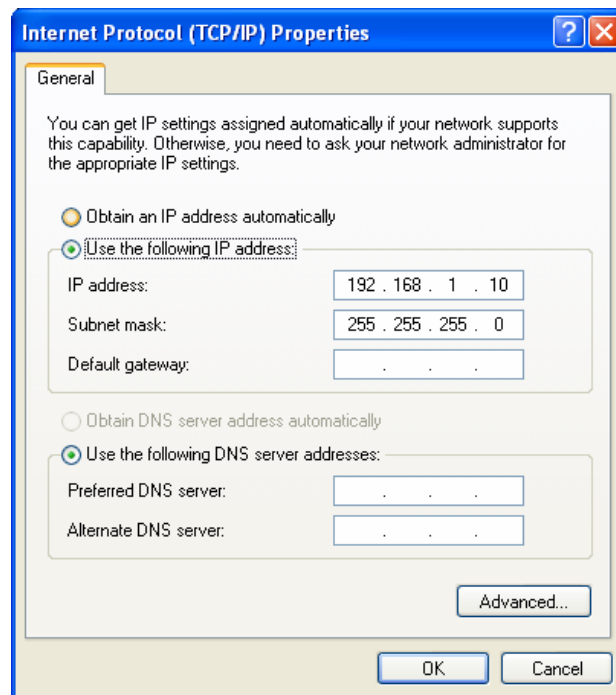
2.2 IP Address Configuration

This device can be configured as a Bridge or Access Point. The default IP address of the device is **192.168.1.1**. In order to log into SP912GH, you must first configure the TCP/IP settings of your PC/Notebook.

1. In the control panel, double click Network Connections and then double click on the connection of your Network Interface Card (NIC). You will then see the following screen.



2. Select **Internet Protocol (TCP/IP)** and then click on the **Properties** button. This will allow you to configure the TCP/IP settings of your PC/Notebook.



3. Select **Use the following IP Address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.

For Example: Device IP address: 192.168.1.1

PC IP address: 192.168.1.10

PC subnet mask: 255.255.255.0

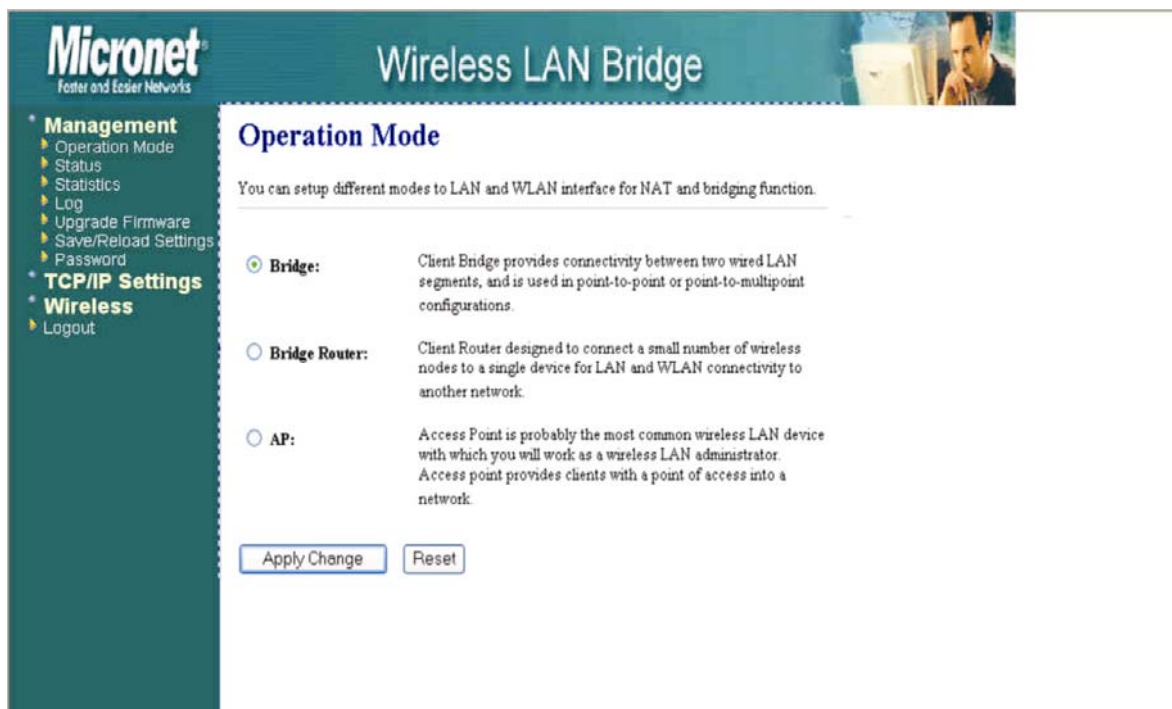
4. Click on the **OK** button to close this window, and once again to close LAN properties window.

3 Configure SP912GH in Bridge/ Bridge Router/ AP

SP912GH can be configured as a Bridge or Access Point. The default IP address of the device is **192.168.1.1** in **Bridge mode**. This chapter will describe the steps to switch from Bridge to Access Point and Access Point to Bridge.

3.1 Bridge/Bridge Router to Access Point

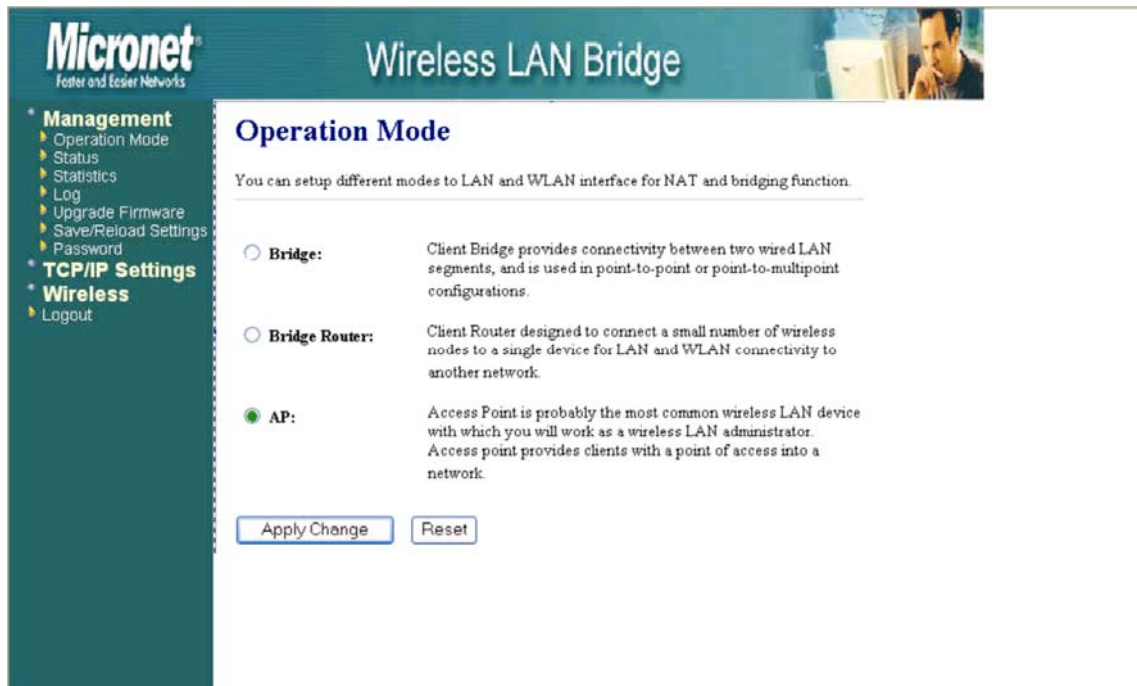
- 1 Enter the default IP address (**192.168.1.1**) of the bridge into the address bar of the web-browser.
- 2 By default, a username and password has not been configured. If you have configured a user name and password, please enter them into the field to continue
- 3 Once you have logged in, click on the **Operation Mode** link under the **Management** menu.



- 4 Since SP912GH is currently in Bridge mode, the **Bridge** radio button will be selected by default.
- 5 Select the **AP** radio button to and then click on the **Apply Change** to switch the operation mode to Access Point.
- 6 Wait for about 1 minute and the device will automatically restart into Access Point mode.

3.2 Access Point to Bridge / Bridge Router

- 1 Enter the default IP address (192.168.1.2) of the bridge into the address bar of the web-browser.
- 2 By default, a user name and password has not been configured. If you have configured a user name and password, please enter them into the field to continue
- 3 Once you have logged in, click on the **Operation Mode** link under the **Management** menu.

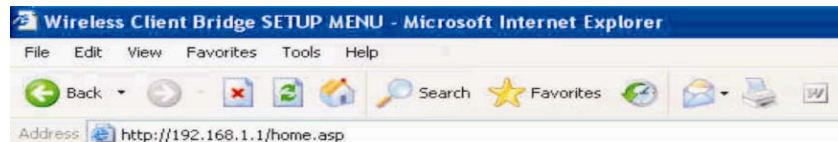


- 4 Since this device is currently in Access Point mode, the **AP** radio button will be selected by default.
- 5 Select the **Bridge** or **Bridge Router** radio button to and then click on the **Apply Change** to switch the operation mode to Bridge.
- 6 Wait for about 1 minute and the device will automatically restart into Bridge mode.

4 Bridge Mode – Web Configuration

4.1 Logging In

- To configure the Bridge through the web-browser, enter the IP address of the Bridge (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.



- Make sure that the Bridge and your computers are on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- Username : **admin**; Password : **admin**
- After logging in you will graphical user interface (GUI) of the bridge. The navigation drop-down menu on left is divided into three main sections:
 - Management**: This includes operation mode, status, statistics, logs, upgrade firmware, save/reload settings, and password.
 - TCP/IP Settings**: This includes the configuration of the LAN port and settings for the LAN IP, subnet mask, DHCP client, spanning tree and MAC cloning.
 - Wireless**: This includes the basic, advanced, security and site-survey settings for the wireless interface.
- The Bridge status page is also displayed once you have logged in. This includes details about the system, wireless, and TCP/IP configuration.

 A screenshot of the Micronet Wireless LAN Bridge web interface. The page title is 'Wireless LAN Bridge'. The left sidebar shows a navigation menu with 'Management', 'TCP/IP Settings', and 'Wireless' sections, along with a 'Logout' link. The main content area is titled 'Client Bridge Status' and contains a table of system and configuration details.

System	
Uptime	0day:0h:45m:47s
Firmware Version	v1.37
Wireless Configuration	
Mode	Infrastructure Client Bridge
Band	2.4 GHz (B+G)
SSID	wireless_g
Channel Number	10
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP	Disabled
MAC Address	00:02:6f:42:ff:b1

- **System**

- **Uptime:** Duration of time since the device was last reset.
- **Firmware version:** Version of the firmware that is currently loaded on the device.

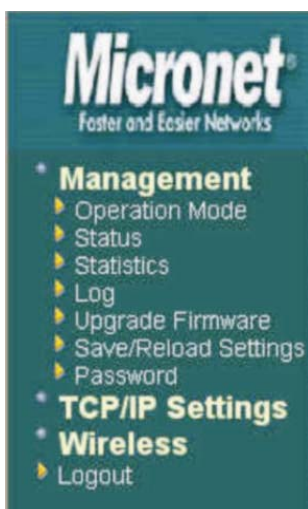
- **Wireless Configuration:**

- **Mode:** Wireless configuration mode such as **Client Bridge, AP, or WDS**.
- **Band:** Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
- **SSID:** The name used to identify the wireless network.
- **Channel Number:** The channel used to communicate on the wireless network.
- **Encryption:** The type of security used on this network. It may be disabled, WEP, WPA, etc.
- **BSSID:** The MAC address of the SSID.
- **State:** The current state of the bridge. It may be scanning or associated or disabled.

- **TCP/IP Configuration:**

- **Attain IP Protocol:** The IP address setting may be fixed or static.
- **IP Address:** Displays the current IP address of the LAN port.
- **Subnet Mask:** Displays the current subnet mask for the IP address.
- **Default Gateway:** Displays the default gateway for the device.
- **DHCP:** Displays the DHCP setting.
- **MAC Address:** Displays the MAC address of the device.

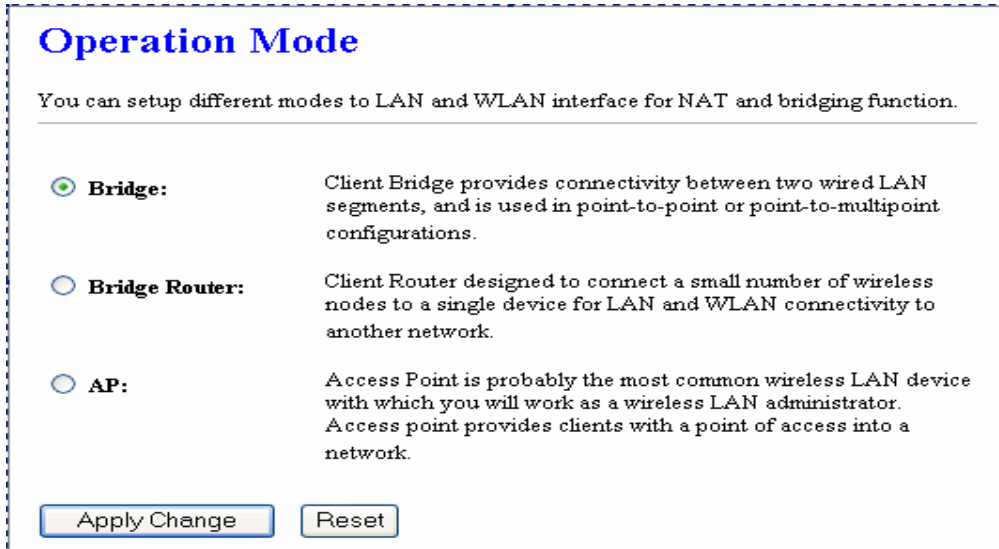
4.2 Management



- Click on the **Management** link on the navigation drop-down menu. You will then see five options: operation mode, status, statistics, log, upgrade firmware, save/reload settings, and password. Each option is described below.

4.2.1 Operation Mode

- Click on the **Operation Mode** link under the **Management** menu. The **Operation Mode** allows you to switch from Client Bridge to Access Point mode.



The screenshot shows a web interface titled "Operation Mode" in blue. Below the title is a subtitle: "You can setup different modes to LAN and WLAN interface for NAT and bridging function." There are three radio button options: "Bridge:" (selected), "Bridge Router:", and "AP:". Each option has a descriptive text block. At the bottom are two buttons: "Apply Change" and "Reset".

Operation Mode

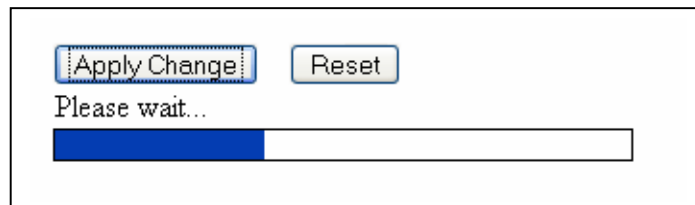
You can setup different modes to LAN and WLAN interface for NAT and bridging function.

☒ **Bridge:** Client Bridge provides connectivity between two wired LAN segments, and is used in point-to-point or point-to-multipoint configurations.

☐ **Bridge Router:** Client Router designed to connect a small number of wireless nodes to a single device for LAN and WLAN connectivity to another network.

☐ **AP:** Access Point is probably the most common wireless LAN device with which you will work as a wireless LAN administrator. Access point provides clients with a point of access into a network.

- Select the **AP**, **Bridge** or **Bridge Router** and then click on the **Apply Change** button.



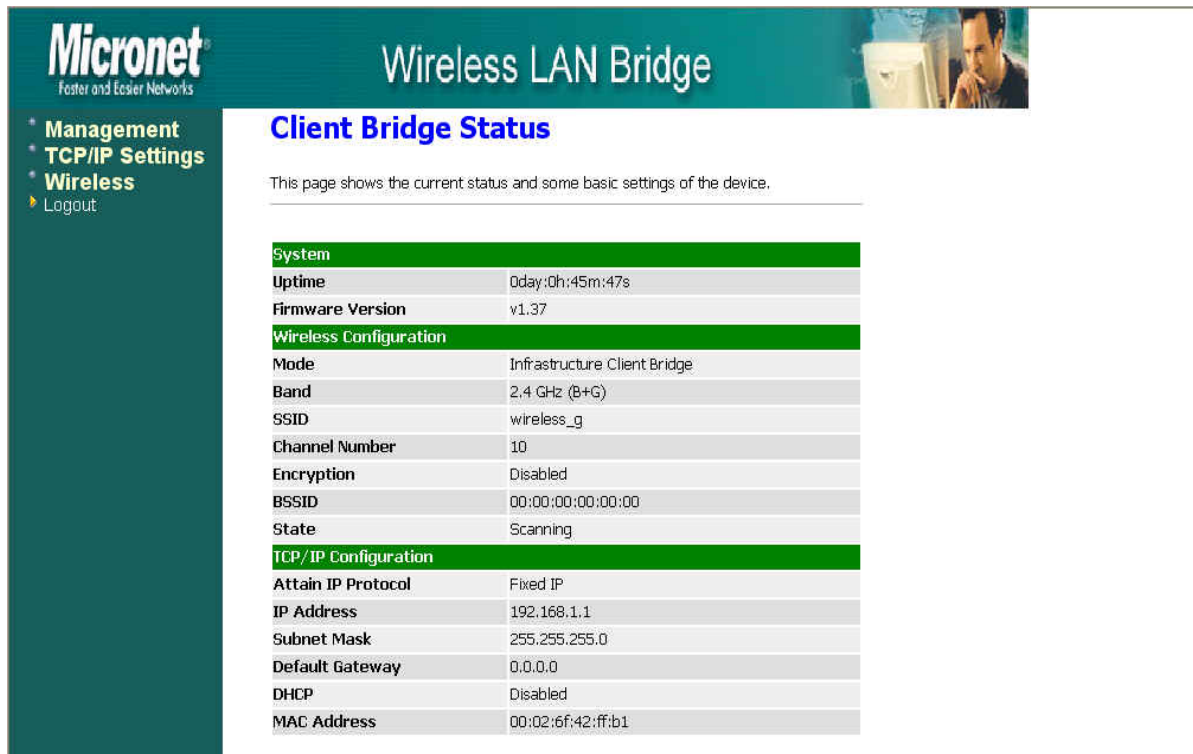
The screenshot shows a pop-up message box with the text "Please wait..." and a progress bar. Above the text are two buttons: "Apply Change" and "Reset". The progress bar is partially filled with blue.

Please wait...

- Wait for about a minute until you see the following Pop-Up message.
 - Click on the **OK** button and then enter the specified IP address into the web-browser.
- **Switch to other mode, the configuration settings will continue using.****
- Refer to **Chapter 5** to learn how to configure this device in Access Point mode.

4.2.2 Status

- Click on the **Status** link under the **Management** menu. The **Status** page is the first page that is displayed once you have logged in. This includes details about the system, wireless, and TCP/IP configuration.



The screenshot shows the Micronet Wireless LAN Bridge web interface. The left sidebar contains the Micronet logo and navigation links: Management, TCP/IP Settings, Wireless, and Logout. The main content area is titled 'Client Bridge Status' and includes a description: 'This page shows the current status and some basic settings of the device.' Below this, there are three sections: System, Wireless Configuration, and TCP/IP Configuration, each with a table of settings.

System	
Uptime	0day:0h:45m:47s
Firmware Version	v1.37

Wireless Configuration	
Mode	Infrastructure Client Bridge
Band	2.4 GHz (B+G)
SSID	wireless_g
Channel Number	10
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning

TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP	Disabled
MAC Address	00:02:6f:42:ff:b1

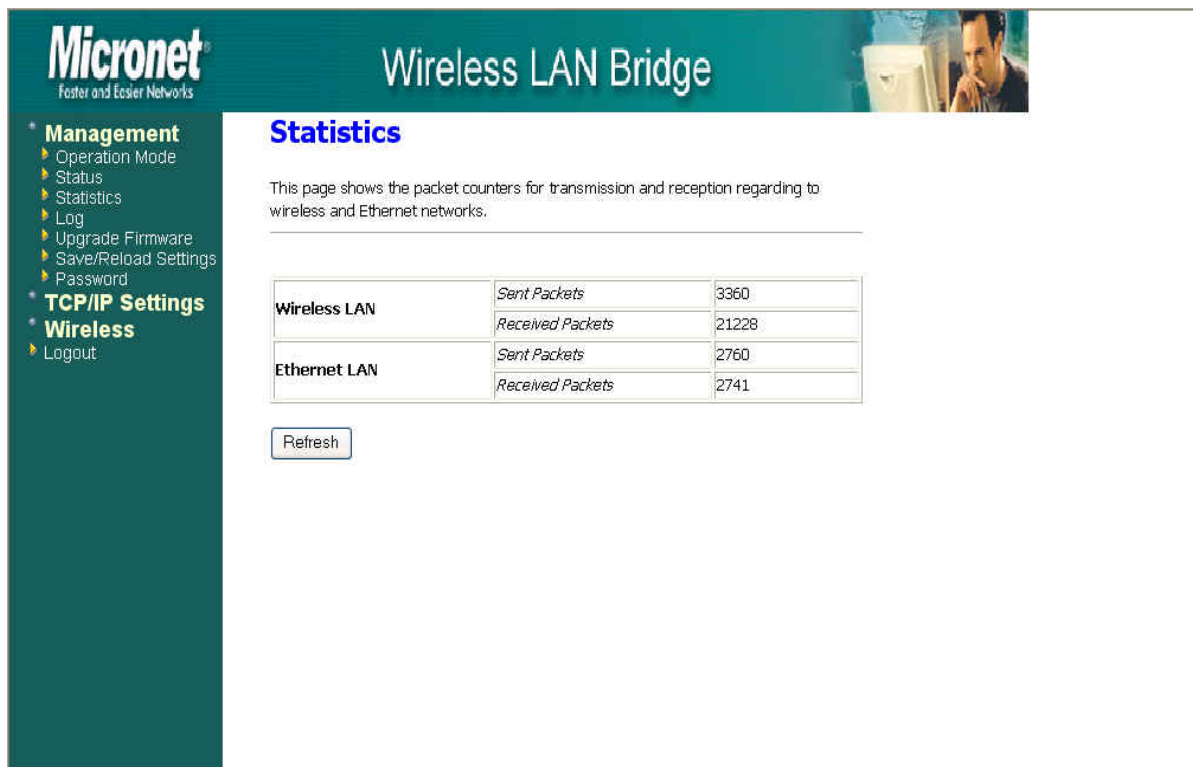
- System**
 - Uptime:** Duration of time since the device was last reset.
 - Firmware version:** Version of the firmware that is currently loaded on the device.
- Wireless Configuration:**
 - Mode:** Wireless configuration mode such as client bridge, AP, or WDS.
 - Band:** Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
 - SSID:** The name used to identify the wireless network.
 - Channel Number:** The channel used to communicate on the wireless network.
 - Encryption:** The type of security used on this network. It may be disabled, WEP, WPA, etc.
 - BSSID:** The MAC address of the SSID.
 - State:** The current state of the bridge. It may be scanning or associated or disabled.

- **TCP/IP Configuration:**

- **Attain IP Protocol:** The IP address setting may be fixed or static.
- **IP Address:** Displays the current IP address of the LAN port.
- **Subnet Mask:** Displays the current subnet mask for the IP address.
- **Default Gateway:** Displays the default gateway for the device.
- **DHCP:** Displays the DHCP setting.
- **MAC Address:** Displays the MAC address of the device.

4.2.3 Statistics

- Click on the **Statistics** link under the **Management** menu. This page displays the number of sent and received packets on the Ethernet and Wireless interface.



Micronet
Faster and Easier Networks

Wireless LAN Bridge

Statistics

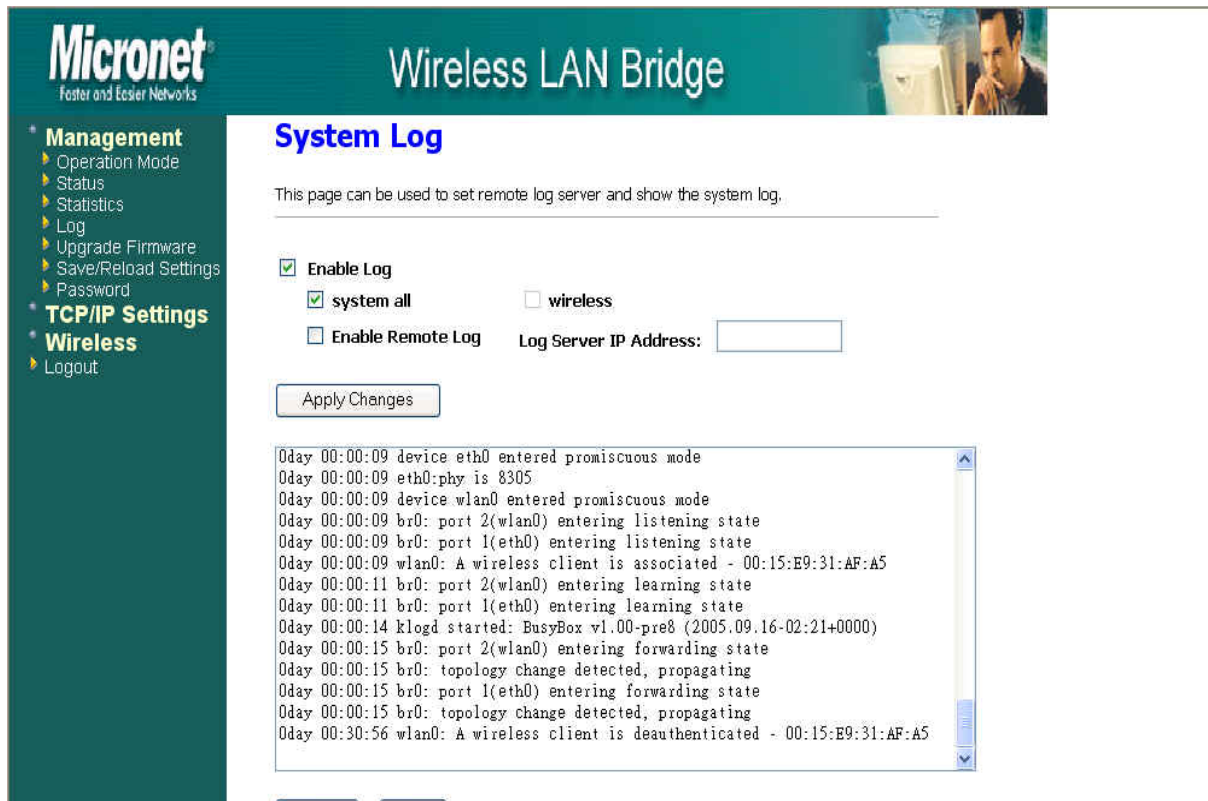
This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	Sent Packets	3360
	Received Packets	21228
Ethernet LAN	Sent Packets	2760
	Received Packets	2741

- Since the packet counter is not dynamic, you must click on the **Refresh** button for the most recent statistics.

4.2.4 Log

- Click on the **Log** link under the **Management** menu. The **Log** page displays a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.



The screenshot shows the Micronet Wireless LAN Bridge web interface. The left sidebar contains a navigation menu with the following items: Management (selected), Operation Mode, Status, Statistics, Log, Upgrade Firmware, Save/Reload Settings, Password, TCP/IP Settings, Wireless, and Logout. The main content area is titled 'System Log' and includes a description: 'This page can be used to set remote log server and show the system log.' Below this, there are configuration options: 'Enable Log' (checked), 'system all' (checked), 'wireless' (unchecked), 'Enable Remote Log' (unchecked), and a 'Log Server IP Address' field. An 'Apply Changes' button is located below these options. A log viewer window displays the following system log entries:

```
Oday 00:00:09 device eth0 entered promiscuous mode
Oday 00:00:09 eth0:phy is 8305
Oday 00:00:09 device wlan0 entered promiscuous mode
Oday 00:00:09 br0: port 2(wlan0) entering listening state
Oday 00:00:09 br0: port 1(eth0) entering listening state
Oday 00:00:09 wlan0: A wireless client is associated - 00:15:E9:31:AF:A5
Oday 00:00:11 br0: port 2(wlan0) entering learning state
Oday 00:00:11 br0: port 1(eth0) entering learning state
Oday 00:00:14 klogd started: BusyBox v1.00-pre8 (2005.09.16-02:21+0000)
Oday 00:00:15 br0: port 2(wlan0) entering forwarding state
Oday 00:00:15 br0: topology change detected, propagating
Oday 00:00:15 br0: port 1(eth0) entering forwarding state
Oday 00:00:15 br0: topology change detected, propagating
Oday 00:30:56 wlan0: A wireless client is deauthenticated - 00:15:E9:31:AF:A5
```

- In order for the log to record all the events, you must first place a check in the **Enable Log** or **Enable Remote Log (Log Server required)** check box.
- Select **system all** or **wireless** depending on the type of events you want recorded.
- Since the log is not dynamic, you must click on the **Refresh** button for the most recent events, or click on the **Clear** button to clear the log.

4.2.5 Upgrade Firmware

- Click on the **Upgrade Firmware** link under the **Management** menu. This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.



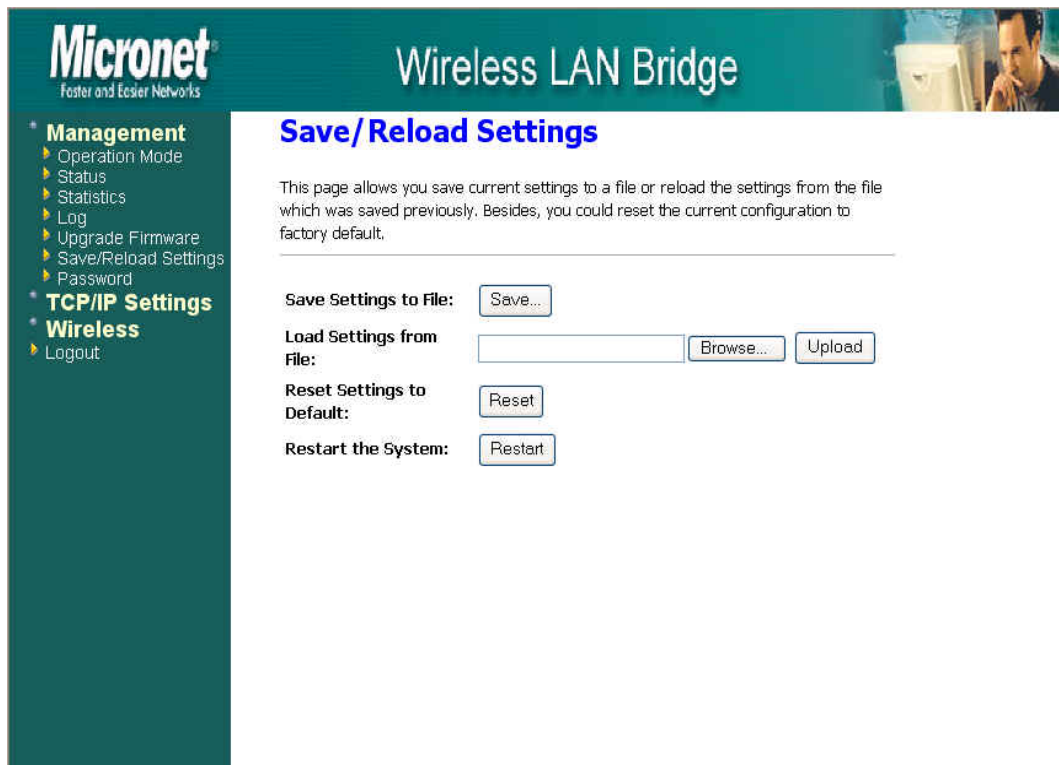
The screenshot shows the web interface of a Micronet Wireless LAN Bridge. The header features the Micronet logo with the tagline 'Faster and Easier Networks' and the title 'Wireless LAN Bridge'. A navigation menu on the left includes 'Management' (with sub-items: Operation Mode, Status, Statistics, Log, Upgrade Firmware, Save/Reload Settings, Password), 'TCP/IP Settings', 'Wireless', and 'Logout'. The main content area is titled 'Upgrade Firmware' and contains a warning: 'This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.' Below this, there is a 'Select File:' label, a text input field, and a 'Browse...' button. At the bottom of the form are 'Upload' and 'Reset' buttons.

- Click on the Browse button and then select the appropriate firmware and then click on the **Upload** button.

Note: The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

4.2.6 Save / Reload Settings, Reset to Default

- Click on the **Save / Reload Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.
- This page also allows you to reset the device to its factory default settings.



The screenshot shows the web interface for a Micronet Wireless LAN Bridge. The header features the Micronet logo with the tagline 'Faster and Easier Networks' and the title 'Wireless LAN Bridge'. A navigation menu on the left includes 'Management' (with sub-items: Operation Mode, Status, Statistics, Log, Upgrade Firmware, Save/Reload Settings, Password), 'TCP/IP Settings', 'Wireless', and 'Logout'. The main content area is titled 'Save/Reload Settings' and contains a descriptive paragraph: 'This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.' Below this text are four action sections: 'Save Settings to File:' with a 'Save...' button; 'Load Settings from File:' with a text input field, a 'Browse...' button, and an 'Upload' button; 'Reset Settings to Default:' with a 'Reset' button; and 'Restart the System:' with a 'Restart' button.

- Click on the **Save** button to save the current settings to a file on the local disk.
- Click on the **Browse** button to select the settings file and then click on the Upload button to load the previously saved settings.
- Click on the **Reset** button to reset the device to its factory default settings. Click **Restart** to reboot the device.

4.2.7 Password

- Click on the **Password** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password. For security reasons it is highly recommended that you create a user name and password.



The screenshot shows the Micronet Wireless LAN Bridge web interface. The header features the Micronet logo with the tagline 'Foster and Easier Networks' and the title 'Wireless LAN Bridge'. A navigation menu on the left includes 'Management' (with sub-items: Operation Mode, Status, Statistics, Log, Upgrade Firmware, Save/Reload Settings, Password), 'TCP/IP Settings', 'Wireless', and 'Logout'. The main content area is titled 'Password Setup' and contains a warning: 'This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.' Below this, there are three input fields: 'User Name:', 'New Password:', and 'Confirmed Password:'. At the bottom of the form are two buttons: 'Apply Changes' and 'Reset'.

- Enter a **user name** into the first field.
- Enter a password into the **New Password** field and then re-type the password into the **Confirmed Password** field. Then click on the **Apply Changes** button.
- By clicking on the **Reset** button, the user name and password fields will become blank indicating that the username and password has been disabled.

4.3 TCP/IP Settings



- Click on the **TCP/IP Settings** link on the navigation drop-down menu. You will then see the **LAN Interface** option. This option is described in detail below.

4.3.1 LAN Interface

- Click on the **LAN Interface** link under the **TCP/IP Settings** menu. Using this option you may change the IP address of the device as well as toggle the **DHCP** and **802.1d** spanning tree feature.

A screenshot of the Micronet web interface's 'Wireless LAN Bridge' section, specifically the 'LAN Interface Setup' page. The page has a teal header with the Micronet logo and the title 'Wireless LAN Bridge'. Below the header, there is a navigation menu on the left with the same structure as the first image. The main content area is titled 'LAN Interface Setup' in blue. Below the title, there is a paragraph explaining the page's purpose: 'This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..'. Below this paragraph, there are several configuration fields: 'IP Address' (text box with '192.168.1.2'), 'Subnet Mask' (text box with '255.255.255.0'), 'Default Gateway' (text box with '0.0.0.0'), 'DHCP' (dropdown menu with 'Server' selected), 'DHCP Client Range' (two text boxes with '192.168.1.100' and '192.168.1.200', and a 'Show Client' button), 'DNS Server' (text box), and '802.1d Spanning Tree' (dropdown menu with 'Enabled' selected). At the bottom of the form, there are two buttons: 'Apply Changes' and 'Reset'.

- **IP Address:** Enter the IP address.
- **Subnet Mask:** Enter the subnet mask for the IP address.
- **Default Gateway:** Enter the IP address for the default gateway.
- **DHCP:** If SP912GH is a DHCP client and will receive its IP settings from a DHCP server, then select **Enabled** from the drop-down list. Enabling the DHCP client will disable the IP address, subnet mask, and default gateway fields. Otherwise the DHCP option is **Disabled**, then the IP address, subnet mask, and default gateway fields must be filled in.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.3.2 SNMP Settings



Micronet
Faster and Easier Networks

Wireless LAN Bridge

SNMP Parameter Setup

This page is used to configure the parameters for simple network management protocol which connects to your Access Point. Here you may change the setting for SNMP demon , read-only and read-write community name, Trap demon, trap IP address, community,etc..

Support WebAdmin Control: ☐ Disable ☒ Enable

Read-Only Community Name:

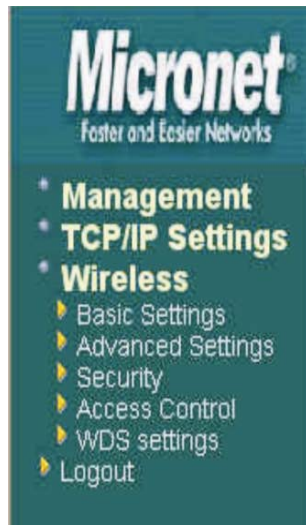
Read-Write Community Name:

Send SNMP Trap: ☒ Disable ☐ Enable

Send Trap To: IP address Community

- Check **Enable** to activate the SNMP and then configure the **Read/Write Community** Strings.
- Enable **Send SNMP Trap** to activate the SNMP Trap Agent and input the IP address of SNMP Trap Host.

4.4 Wireless



- Click on the **Wireless** link on the navigation drop-down menu. You will then see four options: basic settings, advanced settings security and site survey. Each option is described below.

4.4.1 Basic Settings (Infrastructure, Adhoc)

- Click on the **Basic Settings** link under the **Wireless** menu. Using this option you may configure the 802.11b/g settings as well as the frequency, channel, and SSID.

A screenshot of the 'Wireless Basic Settings' page in the Micronet web interface. The page title is 'Wireless LAN Bridge' and 'Wireless Basic Settings'. A description states: 'This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.' The form includes the following fields:


- Network Type:** A dropdown menu set to 'Infrastructure'.
- SSID:** A text input field containing 'wireless_g'.
- Desired BSSID:** A text input field containing '000000000000'.
- Channel:** A dropdown menu set to 'Auto'.
- ☐ **Enable Mac Clone (Single Ethernet Client)**
- Clone MAC Address:** A text input field containing '000000000000'.

At the bottom, there are two buttons: 'Apply Changes' and 'Reset'.

- **Network Type:** Select **Infrastructure** or **Adhoc** from the drop-down list. Infrastructure is a point-to-multipoint (PtMp) topology where as Adhoc is a point-to-point topology (PtP).
- **SSID:** 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. Enter the MAC address of AP Radio IF for **Desired BSSID**.
- **Channel:** Select a channel from the drop-down list. The channels available are based on the country's regulation. When selecting Infrastructure mode, a channel is not required, however, when selecting Adhoc mode, you must select the same channel on all points.
- **Enable MAC cloning:** Change the Bridge's MAC to the connected Client's MAC which is the first client connects with Bridge. This function only allow one Client connect to network.
- **Clone MAC Address:** Bridge's MAC will be defined by the value in blank space.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.4.2 Advanced Settings (Infrastructure, Adhoc)

- Click on the **Advanced Settings** link under the **Wireless** menu. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: **Fragmentation threshold**, **RTS threshold**, **Beacon interval**, **Output power**, **Preamble type**, **Transparent Bridge** and **Turbo Mode**.



Micronet
Faster and Easier Networks

Wireless LAN Bridge

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Fragment Threshold:	<input type="text" value="2346"/> (256-2346)
RTS Threshold:	<input type="text" value="2347"/> (0-2347)
Beacon Interval:	<input type="text" value="100"/> (20-1024 ms)
Output Power Level:	<input type="button" value="High"/>
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Long & Short Preamble
Transparent Bridge:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Turbo Mode:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

- **Authentication Type:** select an authentication method. Options available are **Open System**, **Shared Key** or **Auto**.
 - I. **Open System:** An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption.
 - II. **Shared Key:** Shared Key sends an unencrypted challenge text string to any other device attempting to communicate with SP912GH. It is requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate.
 - III. **Auto:** It is recommended to select Auto if you are not sure which authentication type is used.
- **Fragment Threshold:** Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **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.
- **Beacon Interval:** Beacons will be sent out to devices at the specified intervals. This value is measured in milliseconds (ms).
- **Output Power Level:** You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- You can arrange the different data rate in distance in Bridge mode. Please refer below table.

	6M-24M	36M	48M	54M
High	▼	▼	▼	Great
Ultra High	▼	▼	Great	N/A
Super	▼	Great	N/A	N/A
Extreme	Great	N/A	N/A	N/A

- **Preamble Type:** For best performance, all devices on the wireless network should use the same preamble type. However, the wireless network will still function even though the wrong preamble type is used.
- **Transparent Bridge:** check **Enable** to activate the Transparent Bridging Function.
- **Turbo Mode:** Select “**Enable**” to activate the Turbo mode for better performance. The Default is disabled.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.4.3 Security

- Click on the **Security** link under the **Wireless** menu. On this page you can configure the authentication and encryption settings such as **WEP**, **WPA**, and **802.1x**.

4.4.3.1 Encryption Disabled

Micronet
Foster and Easier Networks

Wireless LAN Bridge

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys your wireless network.

Encryption: None Set WEP Key

☐ Use 802.1x Authentication

WPA Authentication Mode: WEP 64bits WEP 128bits

☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

WPA Cipher Suite: TKIP AES

WPA2 Cipher Suite: TKIP AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

☐ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes Reset

- **Encryption:** Select **None** from the drop-down list if your wireless network does not use any type of encryption.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.4.3.2 WEP 64-bit / 128-bit

The screenshot shows the 'Wireless Security Setup' page of a Micronet Wireless LAN Bridge. The page has a green sidebar with navigation links: Management, TCP/IP Settings, and Wireless (selected). Under 'Wireless', there are links for Basic Settings, Advanced Settings, Security, Access Control, WDS settings, and Logout. The main content area is titled 'Wireless Security Setup' and includes a description: 'This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys on your wireless network.' The settings are organized into two columns. The left column contains: 'Encryption:' with a dropdown menu set to 'WEP'; 'Use 802.1x Authentication' (unchecked); 'WPA Authentication Mode:' with radio buttons for 'Enterprise (RADIUS)' and 'Personal (Pre-Shared Key)' (selected); 'WPA Cipher Suite:' with radio buttons for 'TKIP' and 'AES' (selected); 'WPA2 Cipher Suite:' with radio buttons for 'TKIP' and 'AES' (selected); 'Pre-Shared Key Format:' with a dropdown menu set to 'Passphrase'; 'Pre-Shared Key:' with a text input field; and 'Enable Pre-Authentication' (unchecked). The right column contains: 'Set WEP Key' button; 'WEP 64bits' and 'WEP 128bits' radio buttons (both unselected); 'Authentication RADIUS Server:' with fields for 'Port' (1812), 'IP address', and 'Password'. At the bottom, there are 'Apply Changes' and 'Reset' buttons. A note at the bottom states: 'Note: When encryption WEP is selected, you must set WEP key value.'

- **Encryption:** Select **WEP** from the drop-down list if your wireless network uses WEP encryption. 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.
- **Set WEP Key:** Click on this button to configure the WEP Key.

The screenshot shows the 'Wireless WEP Key Setup' page. The page has a title 'Wireless WEP Key Setup' and a description: 'This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.' The settings are organized into two columns. The left column contains: 'Key Length:' with a dropdown menu set to '64-bit'; 'Key Format:' with a dropdown menu set to 'Hex (10 characters)'; 'Default Tx Key:' with a dropdown menu set to 'Key 1'; 'Encryption Key 1:' with a text input field; 'Encryption Key 2:' with a text input field; 'Encryption Key 3:' with a text input field; and 'Encryption Key 4:' with a text input field. The right column contains: 'Apply Changes', 'Close', and 'Reset' buttons.

- **Key Length:** Select a **64-bit** or **128-bit** from the drop-down list.
- **Key Format:** Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F.
- **Default Tx Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Encryption Key 1-4:** You may enter four different WEP keys.
- Click on the **Apply Changes** button to confirm the changes and then click on the **Close** button to return to the pervious window.

4.4.3.3 WPA / WPA2 Passphrase

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys your wireless network.

Encryption: **WPA2**

☐ Use 802.1x Authentication ☒ WEP 64bits ☐ WEP 128bits

WPA Authentication Mode: ☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

WPA Cipher Suite: ☐ TKIP ☒ AES

WPA2 Cipher Suite: ☒ TKIP ☐ AES

Pre-Shared Key Format: **Passphrase**

Pre-Shared Key: **12345**

☐ Enable Pre-Authentication

Authentication RADIUS Server: Port **1812** IP address **192.168.1.46** Password

Note: When encryption WEP is selected, you must set WEP key value.

- **Encryption:** Select **WPA** or **WPA2** from the drop-down list if your wireless network uses this encryption. **WPA (Wi-Fi Protected Access)** : It 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 Authentication Mode:** Select the **Personal (Pre-Shared Key)** radio button.
- **WPA/WPA2:** Select **TKIP** or **AES** as the cipher suite.
- **Pre-Shared Key Format:** Select **Passphrase** from the drop-down list.
- **Pre-Shared Key:** Enter the pass phrase here; this should be between 8 and 63 characters.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.4.3.4 WPA / WPA2 RADIUS Authentication

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys your wireless network.

Encryption: **WPA**

☐ Use 802.1x Authentication ☒ WEP 64bits ☐ WEP 128bits

WPA Authentication Mode: ☒ Enterprise (RADIUS) ☐ Personal (Pre-Shared Key)

WPA Cipher Suite: ☐ TKIP ☒ AES

WPA2 Cipher Suite: ☐ TKIP ☒ AES

Pre-Shared Key Format: **Passphrase**

Pre-Shared Key:

☐ Enable Pre-Authentication

Authentication RADIUS Server: Port **1812** IP address **192.168.1.46** Password

Note: When encryption WEP is selected, you must set WEP key value.

- **Encryption:** Select **WPA** or **WPA2** from the drop-down list if your wireless network uses this encryption. 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 Authentication Mode:** Select the **Enterprise (RADIUS)** radio button.
- **WPA/WPA2:** Select **TKIP** or **AES** as the cipher suite.
- **RADIUS Port:** Enter the port number of the RADIUS server. The default is usually 1812.

- **RADIUS IP Address:** Enter the IP address of the RADIUS server.
- **RADIUS Password:** Enter the shared password of the RADIUS server.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

4.4.4 Site Survey

- Click on the **Site Survey** link under the **Wireless** menu. This page displays the list of Access Points in the coverage area and allows you to connect to them if you have the required credentials.

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could client mode is enabled.

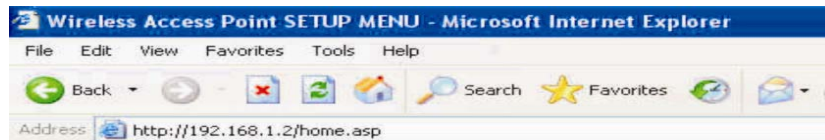
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
DinoNet	00:20:ed:0d:26:96	11 (B)	AP	WEP	69	<input type="radio"/>
TDL-DI-624	00:0f:3d:3d:8e:02	6 (B+G)	AP	WEP	27	<input checked="" type="radio"/>
default	00:90:96:28:24:26	6 (B)	AP	no	26	<input type="radio"/>

- The site survey table lists the following:
 - SSID:** This is the unique name of the wireless network.
 - BSSID:** This is the MAC address of the Access Point.
 - Channel:** This indicates the current channel that the Access Point is operating on, along with the 802.11 network type (B, G, or B+G).
 - Type:** This is the device type.
 - Encrypt:** This indicates the encryption type.
 - Signal:** This indicates the signal strength of the Access Point.
 - Select:** Which device you want to connect?
- You may select the radio button of a specific Access Point and then click on the **Connect** button. If the credentials of this device match that of the Access Point that you will be connected immediately, if not, you must specify the appropriate credentials.
- You may click on the **Refresh** button at any time to re-scan the area or **Connect** to the device what you selected it.

5 Access Point Mode – Web Configuration

5.1 Logging In

- To configure the Access Point through the web-browser, enter the IP address of the Bridge (default: **192.168.1.2**) into the address bar of the web-browser and press **Enter**.



- Make sure that the Access Point and your computers are on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- Log in User name : **admin**; Password : **admin**
- After logging in you will graphical user interface (GUI) of the Access Point. The navigation drop-down menu on left is divided into three main sections:
 4. **Management**: This includes operation mode, status, statistics, logs, upgrade firmware, save/reload settings, and password.
 5. **TCP/IP Settings**: This includes the configuration of the LAN port and settings for the LAN IP, subnet mask, DHCP client, spanning tree and MAC cloning.
 6. **Wireless**: This includes the basic, advanced, security and site-survey settings for the wireless interface.
- The Access Point status page is also displayed once you have logged in. This includes details about the system, wireless, and TCP/IP configuration.

A screenshot of the Micronet Wireless LAN Bridge web interface. The header features the Micronet logo and the text "Wireless LAN Bridge". A left sidebar contains navigation links: Management, TCP/IP Settings, Wireless, and Logout. The main content area is titled "Access Point Status" and includes a description: "This page shows the current status and some basic settings of the device." Below this, there are three sections: System, Wireless Configuration, and TCP/IP Configuration, each containing a table of settings.

System	
Uptime	0day:2h:8m:32s
Firmware Version	v1.31

Wireless Configuration	
Mode	AP+WDS
Band	2.4GHz(B+G)
SSID	RTL8186-VPN-GW
Channel Number	6
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:e0:4c:81:86:21
Associated Clients	0

TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP	Disabled
MAC Address	00:e0:4c:81:86:21

- **System**
 - I. **Uptime:** Duration of time since the device was last reset.
 - II. **Firmware version:** Version of the firmware that is currently loaded on the device.
- **Wireless Configuration:**
 - I. **Mode:** Wireless configuration mode such as client bridge, AP, or WDS.
 - II. **Band:** Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
 - III. **SSID:** The name used to identify the wireless network.
 - IV. **Channel Number:** The channel used to communicate on the wireless network.
 - V. **Encryption:** The type of security used on this network. It may be disabled, WEP, WPA, etc.
 - VI. **BSSID:** The MAC address of the SSID.
 - VII. **Associated Clients:** Displays the number of clients currently associated to the Access Point.
- **TCP/IP Configuration:**
 - I. **Attain IP Protocol:** The IP address setting may be fixed or static.
 - II. **IP Address:** Displays the current IP address of the LAN port.
 - III. **Subnet Mask:** Displays the current subnet mask for the IP address.
 - IV. **Default Gateway:** Displays the default gateway for the device.
 - V. **DHCP:** Displays the DHCP setting.
 - VI. **MAC Address:** Displays the MAC address of the device.

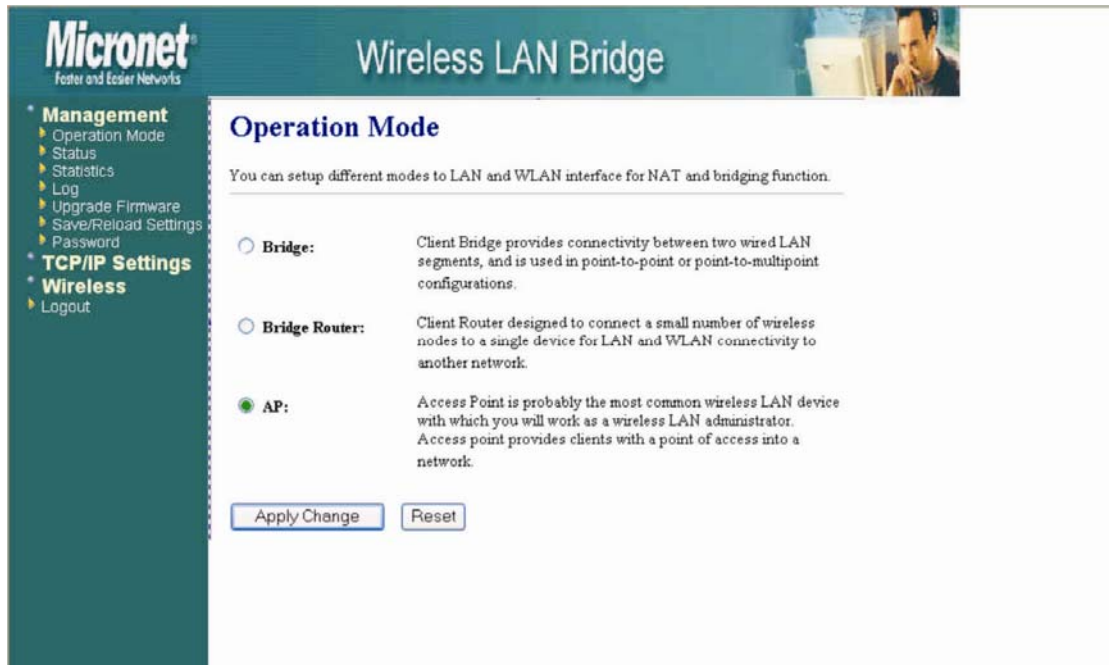
5.2 Management



- Click on the **Management** link on the navigation drop-down menu. You will then see five options: operation mode, status, statistics, log, upgrade firmware, save/reload settings, and password. Each option is described below.

5.2.1 Operation Mode

- Click on the **Operation Mode** link under the **Management** menu. The **Operation Mode** allows you to switch from Access Point to Client Bridge mode.



- Select the **AP**, **Bridge** or **Bridge Router** and then click on the **Apply Change** button.



- Wait for about a minute until you see the Pop-Up message.
- Click on the **OK** button and then enter the specified IP address into the web-browser.
- **Switch to other mode, the configuration settings will continue using. ****
- Switch to other mode, the setting

Refer to Chapter 4 to learn how to configure this device in Bridge/Router mode.

5.2.2 Status

- Click on the **Status** link under the **Management** menu. The **Status** page is the first page that is displayed once you have logged in. This includes details about the system, wireless, and TCP/IP configuration.

Access Point Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:2h:8m:32s
Firmware Version	v1.31
Wireless Configuration	
Mode	AP+WDS
Band	2.4 GHz (B+G)
SSID	RTL8186-VPN-GW
Channel Number	6
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:e0:4c:81:86:21
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP	Disabled
MAC Address	00:e0:4c:81:86:21

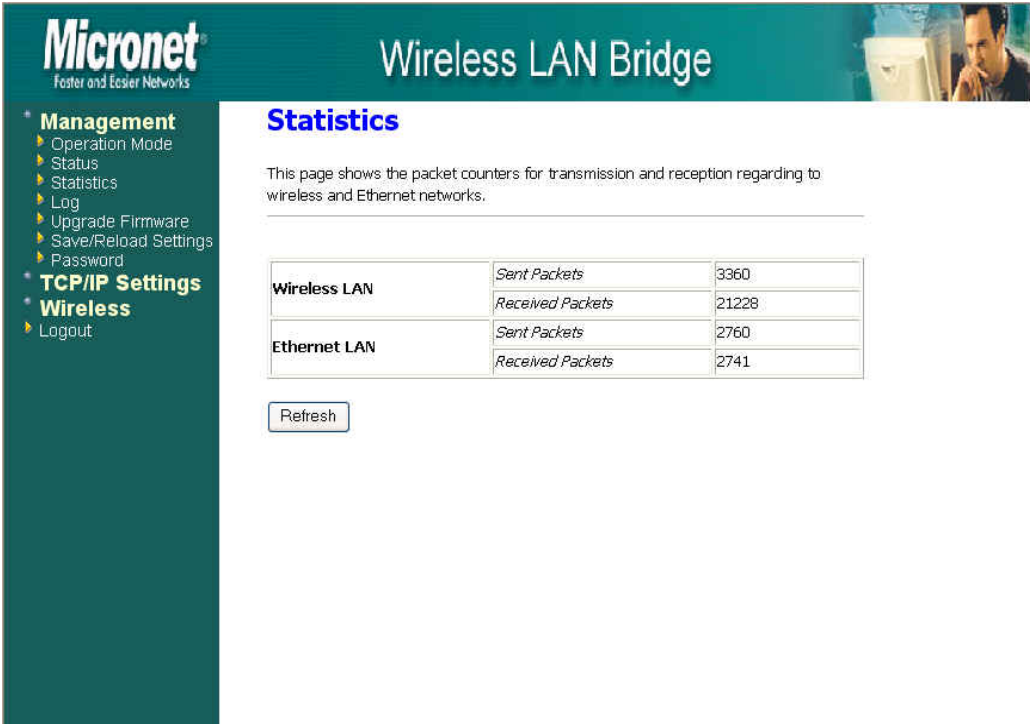
- System**
 - Uptime:** Duration of time since the device was last reset.
 - Firmware version:** Version of the firmware that is currently loaded on the device.
- Wireless Configuration:**
 - Mode:** Wireless configuration mode such as client bridge, AP, or WDS.
 - Band:** Frequency and IEEE 802.11 operation mode (b-only, g-only, or b+g).
 - SSID:** The name used to identify the wireless network.
 - Channel Number:** The channel used to communicate on the wireless network.
 - Encryption:** The type of security used on this network. It may be disabled, WEP, WPA, etc.
 - BSSID:** The MAC address of the SSID.
 - Associated Clients:** Displays the number of clients currently associated to the Access Point.

- **TCP/IP Configuration:**

- I. **Attain IP Protocol:** The IP address setting may be fixed or static.
- II. **IP Address:** Displays the current IP address of the LAN port.
- III. **Subnet Mask:** Displays the current subnet mask for the IP address.
- IV. **Default Gateway:** Displays the default gateway for the device.
- V. **DHCP:** Displays the DHCP setting.
- VI. **MAC Address:** Displays the MAC address of the device.

5.2.3 Statistics

- Click on the **Statistics** link under the **Management** menu. This page displays the number of sent and received packets on the Ethernet and Wireless interface.




The screenshot displays the Micronet Wireless LAN Bridge web interface. The header includes the Micronet logo and the title 'Wireless LAN Bridge'. A left sidebar menu contains options like Management, TCP/IP Settings, and Wireless. The main content area is titled 'Statistics' and includes a descriptive paragraph about packet counters. Below this is a table with two main sections: 'Wireless LAN' and 'Ethernet LAN', each showing 'Sent Packets' and 'Received Packets' counts. A 'Refresh' button is positioned at the bottom of the statistics section.

Interface	Category	Count
Wireless LAN	Sent Packets	3360
	Received Packets	21228
Ethernet LAN	Sent Packets	2760
	Received Packets	2741

- Since the packet counter is not dynamic, you must click on the **Refresh** button for the most recent statistics.

5.2.4 Log

- Click on the **Log** link under the **Management** menu. The **Log** page displays a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.



Wireless LAN Bridge

- Management
 - Operation Mode
 - Status
 - Statistics
 - Log
 - Upgrade Firmware
 - Save/Reload Settings
 - Password
- TCP/IP Settings
- Wireless
- Logout

System Log

This page can be used to set remote log server and show the system log.

☒ **Enable Log**

☒ **system all**
☐ **wireless**

☐ **Enable Remote Log**

Log Server IP Address:

```

0day 00:00:09 device eth0 entered promiscuous mode
0day 00:00:09 eth0:phy is 8305
0day 00:00:09 device wlan0 entered promiscuous mode
0day 00:00:09 br0: port 2(wlan0) entering listening state
0day 00:00:09 br0: port 1(eth0) entering listening state
0day 00:00:09 wlan0: A wireless client is associated - 00:15:E9:31:AF:A5
0day 00:00:11 br0: port 2(wlan0) entering learning state
0day 00:00:11 br0: port 1(eth0) entering learning state
0day 00:00:14 klogd started: BusyBox v1.00-pre8 (2005.09.16-02:21+0000)
0day 00:00:15 br0: port 2(wlan0) entering forwarding state
0day 00:00:15 br0: topology change detected, propagating
0day 00:00:15 br0: port 1(eth0) entering forwarding state
0day 00:00:15 br0: topology change detected, propagating
0day 00:30:56 wlan0: A wireless client is deauthenticated - 00:15:E9:31:AF:A5

```

- In order for the log to record all the events, you must first place a check in the **Enable Log** or **Enable Remote Log (Log Server required)** check box.
- Select **system all** or **wireless** depending on the type of events you want recorded.
- Since the log is not dynamic, you must click on the **Refresh** button for the most recent events, or click on the **Clear** button to clear the log.

5.2.5 Upgrade Firmware

- Click on the **Upgrade Firmware** link under the **Management** menu. This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.

Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File:

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upload** button.

Note: The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

5.2.6 Save / Reload Settings, Reset to Default

- Click on the **Save / Reload Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.
- This page also allows you to reset the device to its factory default settings.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:	<input type="button" value="Save..."/>
Load Settings from File:	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Reset Settings to Default:	<input type="button" value="Reset"/>
Restart the System:	<input type="button" value="Restart"/>

- Click on the **Save** button to save the current settings to a file on the local disk.
- Click on the **Browse** button to select the settings file and then click on the Upload button to load the previously saved settings.
- Click on the **Reset** button to reset the device to its factory default settings. Click **Restart** to reboot the device.

5.2.7 Password

- Click on the **Password** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password. For security reasons it is highly recommended that you create a user name and password.

Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:	<input type="text"/>
New Password:	<input type="text"/>
Confirmed Password:	<input type="text"/>
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

- Enter a **user name** into the first field.
- Enter a password into the **New Password** field and then re-type the password into the **Confirmed Password** field. Then click on the **Apply Changes** button.
- By clicking on the **Reset** button, the user name and password fields will become blank indicating that the username and password has been disabled.

5.3 TCP/IP Settings



- Click on the **TCP/IP Settings** link on the navigation drop-down menu. You will then see the LAN Interface option. This option is described in detail below.

5.3.1 LAN Interface

- Click on the **LAN Interface** link under the **TCP/IP Settings** menu. Using this option you may change the IP address of the device as well as toggle the DHCP and 802.1d spanning tree feature.

5.3.1.1 Static IP Address

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	<input type="text" value="192.168.1.254"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/>
DHCP:	<input type="button" value="Disabled"/> ▾
DHCP Client Range:	<input type="text" value="192.168.1.100"/> - <input type="text" value="192.168.1.200"/> <input type="button" value="Show Client"/>
DNS Server:	<input type="text"/>
802.1d Spanning Tree:	<input type="button" value="Disabled"/> ▾
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

- **IP Address:** Enter the IP address.
- **Subnet Mask:** Enter the subnet mask for the IP address.
- **Default Gateway:** Enter the IP address for the default gateway.
- **DHCP:** Since a static IP address is used, this option must be set to **Disabled**. If this device is a DHCP client and will receive its IP settings from a DHCP server, then select **Enabled** from the drop-down list. Enabling the DHCP client will disable the IP address, subnet mask, and default gateway fields. If the DHCP option is **Disabled**, then the IP address, subnet mask, and default gateway fields must be filled in.
- **802.1d Spanning Tree:** Select **Enabled** from the drop-down list if you if you would like to use the spanning tree feature.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

5.3.1.2 DHCP Client

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	<input type="text" value="192.168.1.254"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/>
DHCP:	<input type="button" value="Client"/> ▾
DHCP Client Range:	<input type="text" value="192.168.1.100"/> - <input type="text" value="192.168.1.200"/> <input type="button" value="Show Client"/>
DNS Server:	<input type="text"/>
802.1d Spanning Tree:	<input type="button" value="Disabled"/> ▾
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

- **DHCP:** If this device is a DHCP client and will receive its IP settings from a DHCP server, then select **Client** from the drop-down list. Enabling the DHCP client will disable the IP address, subnet mask, and default gateway fields. If the DHCP option is **Disabled**, then the IP address, subnet mask, and default gateway fields must be filled in.
- **802.1d Spanning Tree:** Select **Enabled** from the drop-down list if you if you would like to use the spanning tree feature.

- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

5.3.1.3 DHCP Server

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port. change the setting for IP address, subnet mask, DHCP, etc..

IP Address:	<input type="text" value="192.168.1.254"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/>
DHCP:	<input type="text" value="Server"/> ▼
DHCP Client Range:	<input type="text" value="192.168.1.100"/> — <input type="text" value="192.168.1.200"/> <input type="button" value="Show Client"/>
DNS Server:	<input type="text"/>
802.1d Spanning Tree:	<input type="text" value="Disabled"/> ▼

- **IP Address:** Enter the IP address.
- **Subnet Mask:** Enter the subnet mask for the IP address.
- **Default Gateway:** Enter the IP address for the default gateway.
- **DHCP:** Select **Server** from the drop-down list since this device is the DHCP server. This device will distribute the IP addresses to the clients associated.
- **DHCP Client Range:** Enter the first and last IP address of the range. Make sure that the range is on the same subnet as the device. You may click on the Show Client button to view a list of IP addresses that were distributed.
- **DNS Server:** Enter the IP address of the DNS server.
- **802.1d Spanning Tree:** Select **Enabled** from the drop-down list if you if you would like to use the spanning tree feature.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

5.3.2 SNMP Settings

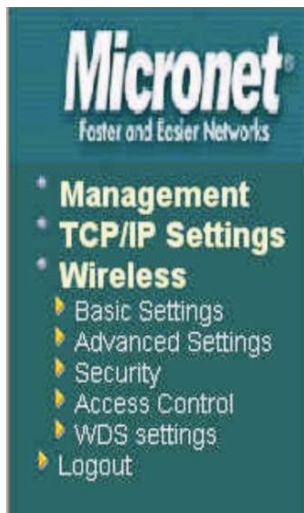
SNMP Parameter Setup

This page is used to configure the parameters for simple network management protocol which connects to your Access Point. Here you may change the setting for SNMP demon, read-only and read-write community name, Trap demon, trap IP addresss, community, etc..

Support WebAdmin Control:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
Read-Only Community Name:	<input type="text" value="public"/>	
Read-Write Community Name:	<input type="text" value="private"/>	
Send SNMP Trap:	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Send Trap To:	IP address <input type="text" value="192.168.1.66"/>	Community <input type="text" value="public"/>

- Check **Enable** to activate the SNMP and then configure the **Read/Write Community** Strings.
- Enable **Send SNMP Trap** to activate the SNMP Trap Agent and input the IP address of SNMP Trap Host.

5.4 Wireless



- Click on the **Wireless** link on the navigation drop-down menu. You will then see five options: basic settings, advanced settings security, access control and WDS. Each option is described below.

5.4.1 Basic Settings

- Click on the **Basic Settings** link under the **Wireless** menu. Using this option you may configure the 802.11b/g settings as well as the frequency, channel, and SSID.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. encryption settings as well as wireless network parameters.

Band:	<input type="text" value="2.4 GHz (B+G)"/>
SSID:	<input type="text" value="RTL8186-VPN-GW"/>
Channel:	<input type="text" value="6"/>
Associated Clients:	<input type="button" value="Show Active Clients"/>

- **Band:** Select the IEEE 802.11 mode from the drop-down list. Options available are **2.4GHz (B)**, **2.4GHz (G)**, or **2.4GHz (B+G)**. Select the appropriate mode based on the type of wireless network. For example, if you are sure that the wireless network will be using only IEEE 802.11g clients, then it is recommended to select 2.4GHz (G) instead of 2.4GHz (B+G) which will reduce the performance of the wireless network.
- **SSID:** 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.
- **Channel:** Select a channel from the drop-down list. The channels available are based on the country's regulation. When selecting Infrastructure mode, a channel is not required, however, when selecting Adhoc mode, you must select the same channel on all points.
- **Show Active Clients:** Click on this button to view a list of associated clients.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

5.4.2 Advanced Settings

- Click on the **Advanced Settings** link under the **Wireless** menu. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: fragmentation threshold, RTS threshold, beacon interval, output power, preamble type, broadcast SSID, IAPP, and 802.11g protection.

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Fragment Threshold:	<input type="text" value="2346"/> (256-2346)
RTS Threshold:	<input type="text" value="2347"/> (0-2347)
Beacon Interval:	<input type="text" value="100"/> (20-1024 ms)
Data Rate:	<input type="button" value="Auto"/>
Output Power Level:	<input type="button" value="High"/>
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Long & Short Preamble
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IAPP:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
802.11g Protection:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
User Isolation:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Turbo Mode:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

- **Authentication Type:** select an authentication method. Options available are **Open System**, **Shared Key** or **Auto**. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- **Fragment Threshold:** Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **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.
- **Beacon Interval:** Beacons will be sent out to devices at the specified intervals. This value is measured in milliseconds (ms).
- **Data Rate:** If you would like to force a data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.

- **Output Power Level:** You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- You can arrange the different data rate in distance in Access Point mode. Please refer below table.

	6M-24M	36M	48M	54M
High	✓	✓	✓	Great
Ultra High	✓	✓	Great	N/A
Super	✓	Great	NA	N/A
Extreme	Great	N/A	N/A	N/A

- **Preamble Type:** For best performance, all devices on the wireless network should use the same preamble type. However, the wireless network will still function even though the wrong preamble type is used.
- **Broadcast SSID:** This is a security feature that is enabled by default. This allows clients on the wireless network to run a site survey and detect this Access Point. Select **Disabled** if you do not want this Access Point detected in a site survey.
- **IAPP:** It is recommended to **Enable** the Inter-Access Point Protocol (IAPP) if you would like the clients on the wireless network to seamlessly roam between Access Points of the same SSID.
- **802.11g Protection:** If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **User Isolation:** Click **“Enabled”** to stop packet transmission between Wireless Clients.
- **Turbo Mode:** Select **“Enable”** to activate the Turbo mode for better performance. The Default is disabled.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

5.4.3 Security

- Click on the **Security** link under the **Wireless** menu. On this page you can configure the authentication and encryption settings such as WEP, WPA, and 802.1x.

5.4.3.1 Encryption Disabled

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys your wireless network.

Encryption:	None ▾	Set WEP Key	
<input type="checkbox"/> Use 802.1x Authentication	<input checked="" type="radio"/> WEP 64bits <input type="radio"/> WEP 128bits		
WPA Authentication Mode:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)		
WPA Cipher Suite:	<input checked="" type="radio"/> TKIP <input type="radio"/> AES		
WPA2 Cipher Suite:	<input type="radio"/> TKIP <input checked="" type="radio"/> AES		
Pre-Shared Key Format:	Passphrase ▾		
Pre-Shared Key:	<input type="text"/>		
<input type="checkbox"/> Enable Pre-Authentication			
Authentication RADIUS Server:	Port <input type="text" value="1812"/>	IP address <input type="text"/>	Password <input type="text"/>

Note: When encryption WEP is selected, you must set WEP key value.

- Encryption:** Select **None** from the drop-down list if your wireless network does not use any type of encryption.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

5.4.3.2 WEP 64-bit / 128-bit

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys in your wireless network.

Encryption:	<input type="button" value="WEP"/>	<input type="button" value="Set WEP Key"/>
<input type="checkbox"/> Use 802.1x Authentication	<input checked="" type="radio"/> WEP 64bits <input type="radio"/> WEP 128bits	
WPA Authentication Mode:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)	
WPA Cipher Suite:	<input checked="" type="radio"/> TKIP <input type="radio"/> AES	
WPA2 Cipher Suite:	<input type="radio"/> TKIP <input checked="" type="radio"/> AES	
Pre-Shared Key Format:	<input type="text" value="Passphrase"/>	
Pre-Shared Key:	<input type="text"/>	
<input type="checkbox"/> Enable Pre-Authentication		
Authentication RADIUS Server:	Port <input type="text" value="1812"/>	IP address <input type="text"/> Password <input type="text"/>

Note: When encryption WEP is selected, you must set WEP key value.

- **Encryption:** Select **WEP** from the drop-down list if your wireless network uses WEP encryption. 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.
- **Set WEP Key:** Click on this button to configure the WEP Key.

Wireless WEP Key Setup

This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

Key Length:	<input type="text" value="64-bit"/>
Key Format:	<input type="text" value="Hex (10 characters)"/>
Default Tx Key:	<input type="text" value="Key 1"/>
Encryption Key 1:	<input type="text" value="xxxxxxxxxx"/>
Encryption Key 2:	<input type="text" value="xxxxxxxxxx"/>
Encryption Key 3:	<input type="text" value="xxxxxxxxxx"/>
Encryption Key 4:	<input type="text" value="xxxxxxxxxx"/>

- **Key Length:** Select a **64-bit** or **128-bit** from the drop-down list.
- **Key Format:** Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F.
- **Default Tx Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Encryption Key 1-4:** You may enter four different WEP keys.
- Click on the **Apply Changes** button to confirm the changes and then click on the **Close** button to return to the pervious window.

5.4.3.3 WPA / WPA2 / WPA2 Mixed Passphrase

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys your wireless network.

Encryption:	WPA2 ▼			Set WEP Key
<input type="checkbox"/> Use 802.1x Authentication	<input checked="" type="radio"/> WEP 64bits <input type="radio"/> WEP 128bits			
WPA Authentication Mode:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)			
WPA Cipher Suite:	<input type="radio"/> TKIP <input checked="" type="radio"/> AES			
WPA2 Cipher Suite:	<input checked="" type="radio"/> TKIP <input type="radio"/> AES			
Pre-Shared Key Format:	Passphrase ▼			
Pre-Shared Key:	<input type="text" value="12345"/>			
<input type="checkbox"/> Enable Pre-Authentication				
Authentication RADIUS Server:	Port <input type="text" value="1812"/>	IP address <input type="text" value="192.168.1.46"/>	Password <input type="text" value="1234567890123456"/>	

Note: When encryption WEP is selected, you must set WEP key value.

- **Encryption:** Select **WPA**, **WPA2** or **WPA2_Mixed** from the drop-down list if your wireless network uses this encryption. 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 Authentication Mode:** Select the **Personal (Pre-Shared Key)** radio button.

- **WPA/WPA2:** Select **TKIP**, **AES** or both as the cipher suite.
- **Pre-Shared Key Format:** Select **Passphrase** from the drop-down list.
- **Pre-Shared Key:** Enter the pass phrase; this should be between 8 and 63 characters.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

5.4.3.4 WPA / WPA2 / WPA2 Mixed RADIUS Authentication

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys your wireless network.

Encryption: WPA

☐ Use 802.1x Authentication
 ☒ WEP 64bits ☐ WEP 128bits

WPA Authentication Mode: ☒ Enterprise (RADIUS) ☐ Personal (Pre-Shared Key)

WPA Cipher Suite: ☐ TKIP ☒ AES

WPA2 Cipher Suite: ☐ TKIP ☒ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

☐ Enable Pre-Authentication

Authentication RADIUS Server:
Port
IP address
Password

Note: When encryption WEP is selected, you must set WEP key value.

- **Encryption:** Select **WPA**, **WPA2** or **WPA2_Mixed** from the drop-down list if your wireless network uses this encryption. 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 Authentication Mode:** Select the **Enterprise (RADIUS)** radio button.
- **WPA/WPA2:** Select **TKIP**, **AES** or both as the cipher suite.
- **RADIUS Port:** Enter the port number of the RADIUS server. The default is usually 1812.
- **RADIUS IP Address:** Enter the IP address of the RADIUS server.

- **RADIUS Password:** Enter the shared password of the RADIUS server.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

5.4.3.5 Access Control

- Click on the **Access Control** link under the **Wireless** menu. On this page you can filter the MAC address by allowing or blocking access the network.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able

Wireless Access Control Mode:

MAC Address:

Current Access Control List:

MAC Address	Comment	Select
<div><input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/></div>		

- **Wireless Access Control Mode:** You may choose to **Disable**, **Allow Listed**, or **Deny Listed** MAC address from associating with the network. By selecting Allow Listed, only the address listed in the table will have access to the network; all other clients will be blocked. On the other hand, selected Deny Listed, only the listed MAC address will be blocked from access the network; all other clients will have access to the network.
- **MAC Address:** Enter the MAC address.
- **Current Access Control list:** This table lists the blocked or allowed MAC addresses; you may delete selected MAC address or delete all the addresses from the table by clicking on the associated buttons.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

5.4.3.6 WDS

- Click on the **WDS** link under the **Wireless** menu. On this page you can configure the WDS (Wireless Distribution System) which allows the Access Point to function as a repeater.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the E the same channel and set MAC address of other APs which you want to communicate with:

☒ **Enable WDS**

Add WDS AP: **MAC Address** **Comment**

Current WDS AP List:

MAC Address	Comment	Select
11:22:33:44:55:66	ap1	<input type="checkbox"/>
22:33:44:55:66:77	ap2	<input type="checkbox"/>

- Enable WDS:** Place a check in this box to enable this feature.
- Add WDS AP:** Enter the MAC address of the Access Point that will join the WDS network along with a comment about the AP.
- Current WDS AP list:** This table lists MAC addresses; you may delete selected MAC address or delete all the addresses from the table by clicking on the associated buttons.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

5.4.3.7 WDS Security Setup

- Click on the **Set Security** button to configure the Security Settings. On this page you can configure the WDS Security which protects your WLAN connection.

WDS Security Setup

This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

Encryption:	<div>None</div>
WEP Key Format:	<div>None</div>
WEP Key:	<div></div>
Pre-Shared Key Format:	<div>WPA2 (AES)</div>
Pre-Shared Key:	<div></div>

Apply Changes

Close

Reset

- **Encryption:** Select **WEP** 64bits, WEP 128bits, WPA (TKIP) or WPA2 (AES) from the drop-down list if your wireless network uses a specific encryption.
- **Key Format:** Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F.
- **Key Length:** Select a **64-bit** or **128-bit** from the drop-down list.
- **Pre-Shared Key Format:** Select **Passphrase** from the drop-down list.
- **Pre-Shared Key:** Enter the pass phrase; this should be between 8 and 63 characters.
- Click on the **Apply Changes** button to confirm the changes. This device will automatically restart once these changes have been applied.

Specifications

Data Rates

1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps

Standards

IEEE802.11b/g, IEEE802.1x, IEEE802.3, IEEE802.3u

Compatibility

IEEE 802.11g/ IEEE 802.11b

Power Requirements

Power Supply: 90 to 240 VDC \pm 10%
(depends on different countries)
Device: 12 V/ 1A

Status LEDs

LAN: Link, WLAN: Link, Power: on/off

Regulation Certifications

FCC Part 15/UL, ETSI 300/328/CE

RF Information**Frequency Band**

2.400~2.4835 GHz (US, EU)
2.400~2.484 GHz (JP)

Media Access Protocol

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Modulation Technology

Orthogonal Frequency Division Multiplexing (OFDM)
DBPSK @ 1Mbps
DQPSK @ 2Mbps
CCK @ 5.5 & 11Mbps
BPSK @ 6 and 9 Mbps
QPSK @ 12 and 18 Mbps
16-QAM @ 24 and 36 Mbps
64-QAM @ 48 and 54 Mbps

Operating Channels

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

Receive Sensitivity (Typical)

-88dBm @ 6Mbps
-70dBm @ 54Mbps

Available Transmit Power (Max.)

26dBm @ 1~24Mbps
23dBm @ 36Mbps
21dBm @ 48Mbps
20dBm @ 54Mbps

RF Connector

TNC Type (Female Reverse)

Networking**Topology**

Ad-Hoc, Infrastructure

Operation Mode

Point-to-Point/ Point-to-Multipoint
Bridge/ AP/ Client Bridge/ WDS

Interface

One 10/100Mbps RJ-45 LAN Port

Security

IEEE802.1x Authenticator / RADIUS
Client (EAP-MD5/TLS/TTLS) Support in AP Mode
WPA2/WPA / Pre-share Key (PSK)/ AES/TKIP
MAC address filtering
Hide SSID in beacons

IP Auto-configuration

DHCP client/server

Management**Configuration**

Web-based configuration (HTTP)

Firmware Upgrade

Upgrade firmware via web-browser

Environmental**Temperature Range**

Operating: 0°C to 45°C (32°F to 113°F)
Storage: -20°C to 70°C (-4°F to 158°F)

Humidity (non-condensing)

5%~95% Typical