

Wireless Broadband Router

GR-124W



User Manual

Version 1.0 / 8, 2009

CATALOG

1	Overview	1
2	Hardware Description and Hardware Installation.....	2
2.1	Front Panel and LED Status	2
2.2	Rear Panel and Interface Description	3
2.3	Hardware Installation.....	4
2.3.1	System Requirements	4
2.3.2	Before You Begin	4
2.3.3	Connecting AP	4
2.4	Operation Range	5
2.5	Roaming	5
3	Network Configuration and Introduction to Network Connection Modes	5
3.1	TCP/IP Settings	6
3.2	Introduction to PPPoE (ADSL) and DHCP (Auto config).....	9
3.3	Connection Introduction for Ethernet User	12
3.4	Connection Introduction for Wireless User.....	12
3.5	Log In to the Web Page.....	15
4	Quick Start.....	17
4.1	Quick Start in the Bridge Mode.....	17
4.2	Quick Start in the Gateway Mode.....	18
4.2.1	System Management.....	19
4.2.2	LAN Settings.....	20
4.2.3	WAN Settings	22
4.2.4	Wireless Settings	22
4.2.5	Wireless Security	23
4.3	Quick Start in the WISP Mode.....	24
5	Web Configuration	28
5.1	Overview.....	28
5.1.1	Status.....	28
5.1.2	Statistic	28
5.1.3	Management.....	29
5.2	Operation Mode.....	30
5.3	Internet Settings	31
5.3.1	LAN.....	32
5.3.2	WAN	35
5.3.3	Advanced Routing	40

5.3.4	DHCP.....	43
5.3.5	QoS.....	43
5.4	Wireless Settings (Gateway Mode).....	51
5.4.1	Basic.....	52
5.4.2	Advanced Settings.....	55
5.4.3	Security.....	63
5.4.4	Station List.....	72
5.4.5	Wireless WDS Setting.....	73
5.5	Wireless Settings (WISP Mode).....	82
5.5.1	Profile.....	83
5.5.2	Link Status.....	89
5.5.3	Site Survey.....	89
5.5.4	Statistics.....	92
5.5.5	Advance.....	92
5.5.6	QoS.....	94
5.5.7	About.....	96
5.6	Firewall.....	96
5.6.1	Filtering.....	96
5.6.2	Virtual Server.....	99
5.6.3	DMZ.....	101
5.6.4	System Security.....	102
5.6.5	Content Filtering.....	103
5.7	Administration.....	106
5.7.1	Management.....	106
5.7.2	Upload Firmware.....	109
5.7.3	Settings Management.....	110
5.7.4	Status.....	110
5.7.5	Statistic.....	111
5.7.6	System Log.....	112
6	Troubleshooting.....	113

About User Manual

This user manual mainly describes how to install and configure the Getnet GR-124W wireless router.

Organization

The GR-124W User Manual is organized as follows:

Chapter	Description
Chapter 1 : Overview	Provides a general overview of the GETNET GR-124W wireless router, and the package list.
Chapter 2 : Hardware Description and Hardware Installation	Mainly describes the front panel and the rear panel of the GETNET GR-124W and the procedure for hardware installation.
Chapter 3 : Network Configuration and Introduction to Network Connection Modes	Describes how to configure network settings and provides the introduction to network connection modes.
Chapter 4 Quick Start	Provides quick start for configuring GETNET GR-124W.
Chapter 5 Web Configuration	Mainly describes how to navigate through the Web pages and how to configure the parameters.
Chapter 6 : Troubleshooting	Describes how to solve some simple problems.

Features

- Support IEEE802.11b, IEEE802.11g, IEEE802.3, IEEE802.3u, IEEE802.11i, and IEEE802.11e
- The transmission data rate is up to 54 Mbps
- Support WEP and WPA for data transmission security
- Support DHCP Server and Client
- Support static and dynamic routing

- Support upgrading firmware version via Web page
- Support restoring factory default settings
- Support virtual server
- Support DMZ (demilitarized zone)
- Support DNS proxy and forwarding
- Support setting QoS bandwidth, and generating rules based on protocol, port, IP, DSCP, or application
- Support wireless security authentication modes, including Open, Shared, WEPAUTO, WPA-Enterprise, WPA-PSK, WPA2-Enterprise, WPA2-PSK, WPA-PSK/WPA2-PSK, WPA/WPA2-Enterprise, and Dynamic WEP 802.1x
- Support 5 types of WAN connection modes, including STATIC (fixed IP), DHCP (Auto config), PPPoE (ADSL), L2TP, and PPTP
- Support remote access control
- Support firewall functions, including IP/MAC/port filter, URL filter, and Web content filter
- Support system status display
- Support backuping and restoring configuration file
- Ethernet provides cross-over cable detection and also provides auto modification and polarity modification function
- Support system log

1 Overview

Thank you for choosing GETNET GR-124W.

GETNET GR-124W is fully compatible with 802.11g standard. Meanwhile, it is also compatible with 802.11 standards and earlier 802.11 b standards. GETNET GR-124W supports CCK and OFDM and its data rate is up to 54 Mbps. It is easy to install and can be applied to AP and router access.

GR-124W provides 64-bit and 128-bit WEP encryption schemes, and WPA encryption, associating with IEEE 802.1X authentication, which insures the security of wireless communication.

Package List

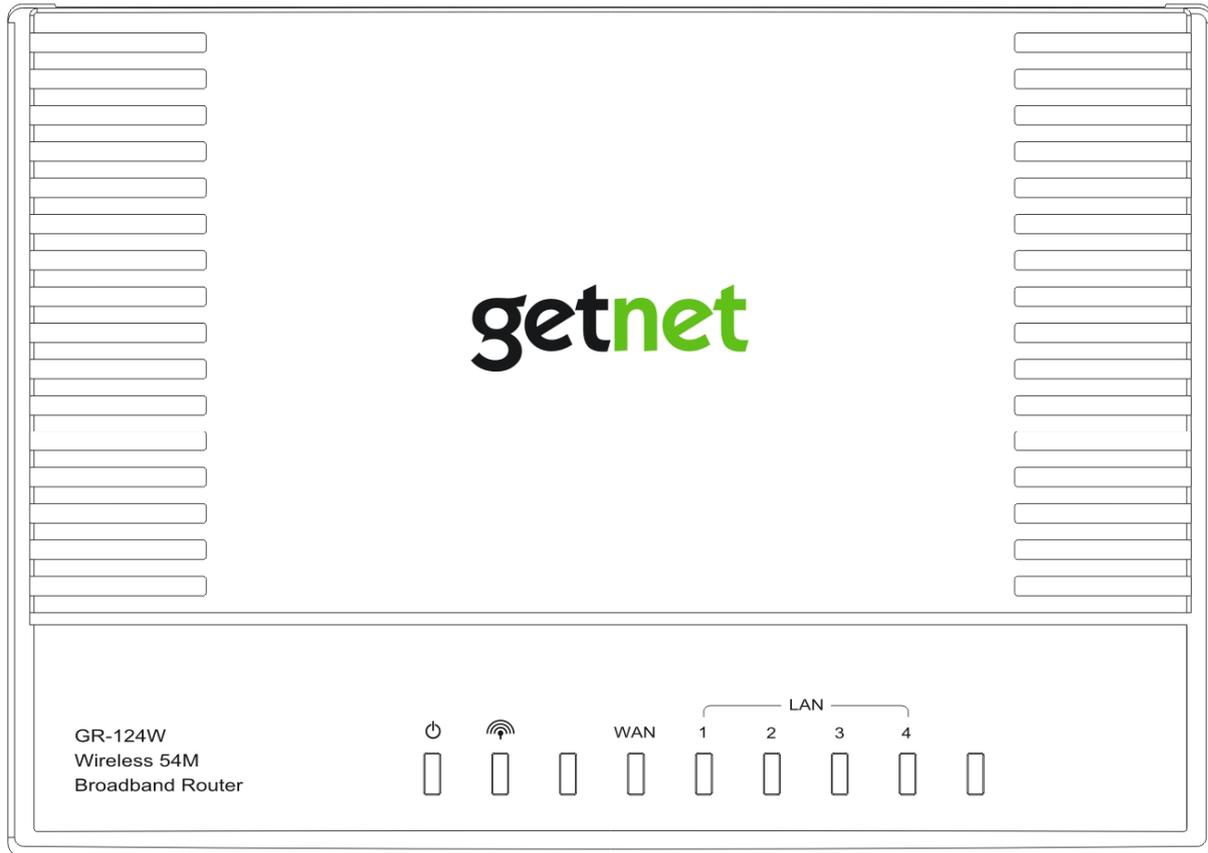
Please check whether your package list includes the following items:

- GR-124W x 1
- Power adapter x 1
- RJ 45 cable x 1

2 Hardware Description and Hardware Installation

2.1 Front Panel and LED Status

There are 8 LED indicators on the front panel of GR-124W. By observing their status, you can judge whether the device runs normally.

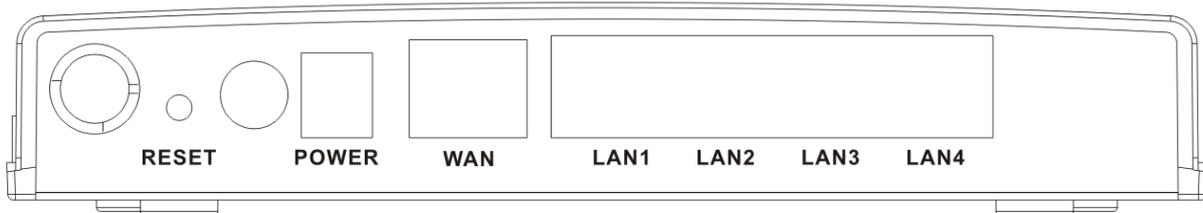


The following table describes the LED indicators on the front panel.

LED Indicator	Color	Status	Description
Power	Red	On	Power is on.
	Green	On	The device runs normally.
	-	Off	Power is off or the device is down.
WLAN	Green	On	Radio switch is turned on.
	Green	Blink	Data is being transmitted.
	-	Off	Radio switch is shut off.
WAN	Green	On	Connection succeeds.
	Green	Blink	Data is being transmitted.

	-	Off	No WAN connection.
LAN 1/2/3/4	Green	On	LAN connection succeeds.
	Green	Blink	Data is being transmitted.
	-	Off	No LAN connection.

2.2 Rear Panel and Interface Description



The following table describes the interfaces or the buttons on the rear panel:

Interface/Button	Description
Reset	Press the button for 3 seconds and then release it. System restores the factory default settings.
ON/OFF	By pressing the button, the power is on. Press the button again, and then the power is off.
POWER	Power socket, for connecting the power adapter.
WAN	WAN interface, for connecting WAN or the uplink network devices.
LAN1~LAN4	LAN interface, for connecting hub, switch, or computer on LAN.

Note:

Do not press the **Reset** button unless you want to clear the current settings. The **Reset** button is in a small circular hole on the rear panel. If you want to restore the default settings, please press the **Reset** button gently for 3 seconds with a fine needle inserted into the hole and then release the button. The system reboots and returns to the factory defaults.

Warning:

The power specification is 12V, 500 mA. If the power adapter does not match the specification, it may damage the device.

2.3 Hardware Installation

2.3.1 System Requirements

Before installing the device, please make sure that the following items are ready.

- At least one Ethernet RJ45 cable (10Base-T/100Base-T)
- GR-124W x 1
- A PC has been installed TCP/IP protocol and it can access the Internet.

2.3.2 Before You Begin

Before you install the device, please pay attention to the following items:

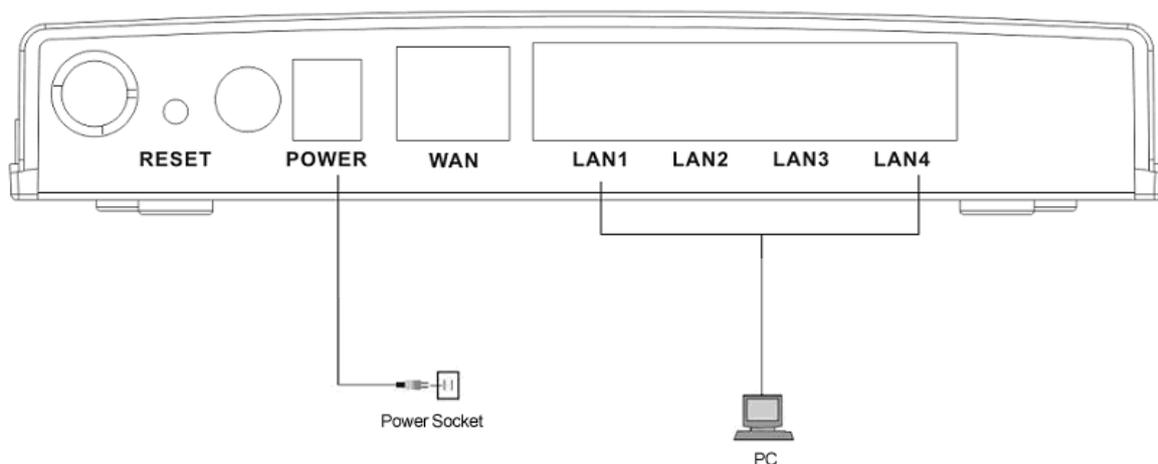
- When connecting the device to the computer, hub, router or switch, the Ethernet cable should be less than 100 meters.
- Do not place this device on an unstable surface or support. Do not put this device on the ground.
- Keep the device clean. Avoid the device from direct sunshine. Avoid any metal in the device.
- Place the device in the center of the area, and try to optimize the wireless coverage.

2.3.3 Connecting AP

Step 1 Connect one end of the RJ45 cable to the LAN interface of the GR-124W.

Step 2 Connect the other end of the RJ45 cable to your PC.

Step 3 Connect the power adapter to the power socket of the GR-124W.



2.4 Operation Range

The operation range of GR-124W depends on the actual environment. When the device is placed in the house or in the office, the overall arrangements are different. So the path and effect for the signal transmission are different. For example, the outdoor straight transmission distance for some devices in the open air is up to 300 meters, and the indoor straight transmission distance is up to 100 meters.

2.5 Roaming

Suppose that several GR-124Ws run in the same network. Each GR-124W acts as one BSS, and has its coverage. One wireless client terminal (e.g. notebook PC or PDA) can realize roaming from one AP to another AP correctly. In that case, the wireless client terminal can communicate with the other devices within the GR-124Ws' coverage.

In order to realize the wireless client roaming among different GR-124Ws, you need to set the GR-124W properly. Do as follows:

- Set the same SSID for different GR-124Ws.
- The SSIDs of all the computers and PDAs should be consistent with that of the GR-124Ws.
- All the BSSs must use the same wireless channel.
- If the encryption function is enabled, all the GR-124Ws should configure the same encryption mode and the encryption key for establishing connection.
- GR-124W must keep the wireless signal cover the whole operation environment and the wireless signal should be continuous. Please put the GR-124Ws to the appropriate places for a better network coverage.

3 Network Configuration and Introduction to Network Connection Modes

Web management tool allows you to configure GR-124W. The recommended browser is Internet Explorer 5.0 version or above.

The following sections describe how to set the Internet connection, local Ethernet connection, and wireless connection, and how to access the Web page of the GR-124W.

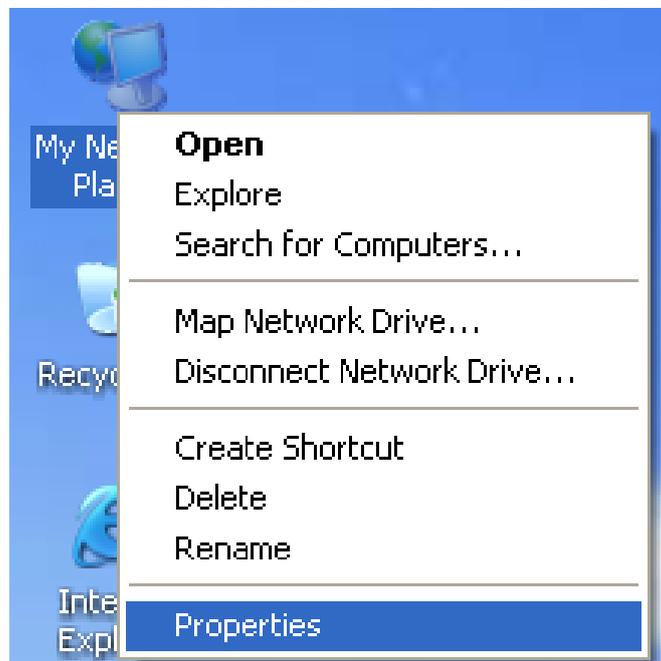
3.1 TCP/IP Settings

By default, the IP address of LAN interface of the GR-124W is 192.168.1.1. The subnet mask is 255.255.255.0. The DHCP Server is enabled.

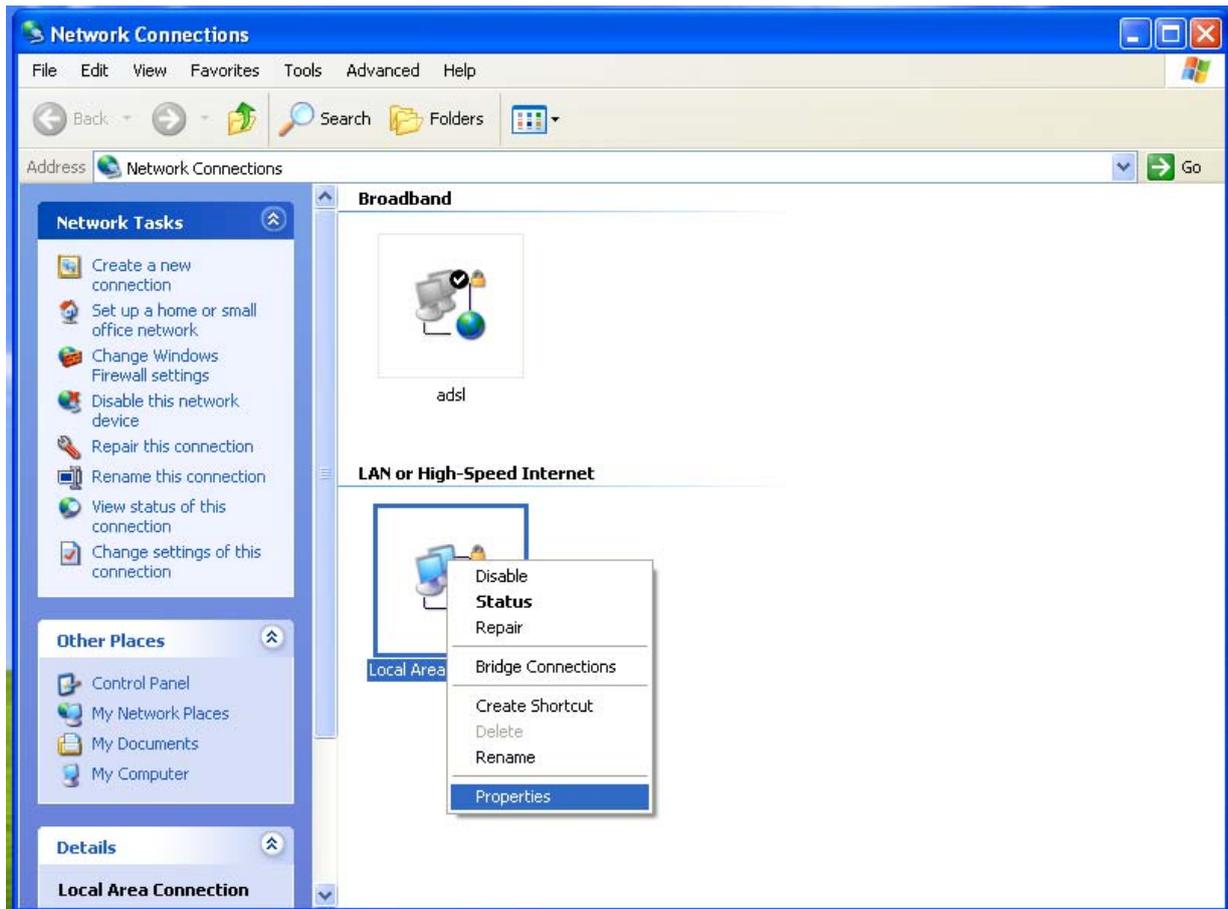
It is recommended you set the network adapter to be **Obtain an IP address automatically**. Your PC automatically acquires IP address, subnet mask, gateway, and DNS address via the GR-124W. If you know the setting of the current LAN interface, you can manually set the TCP/IP properties of the network adapter, so that your PC can communicate with the GR-124W.

You may manually set the network adapter by following the steps below:

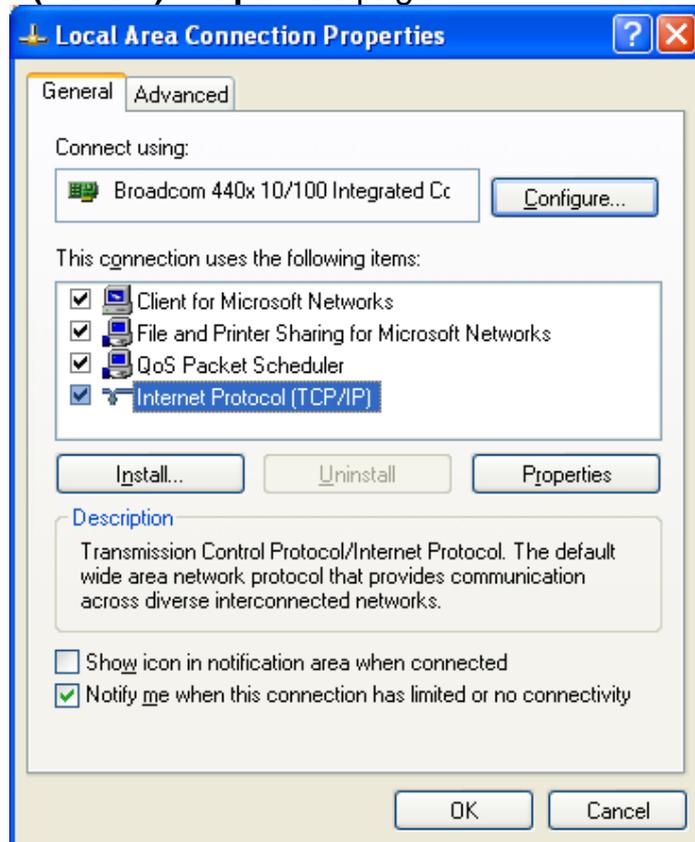
- Step1** Right click the icon of **My Network Places** (e.g., Windows XP) and select **Properties** in the menu. The **Network Connections** page appears.



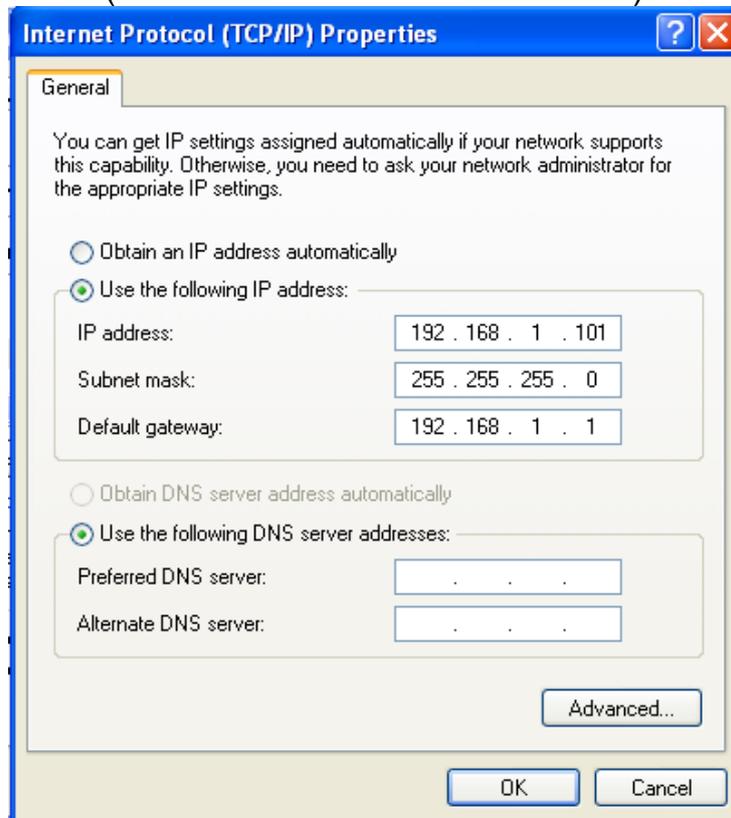
- Step2** Right click the network adapter icon and select **Properties** in the menu. The **Local Area Connections Properties** appears. (**Note:** *If there are several network cards on your PC, it may not display the **Local Area Connections Properties** page. It may display other dialog boxes.*)



Step3 Double click the **Internet Protocol (TCP/IP)** to display the **Internet Protocol (TCP/IP) Properties** page.

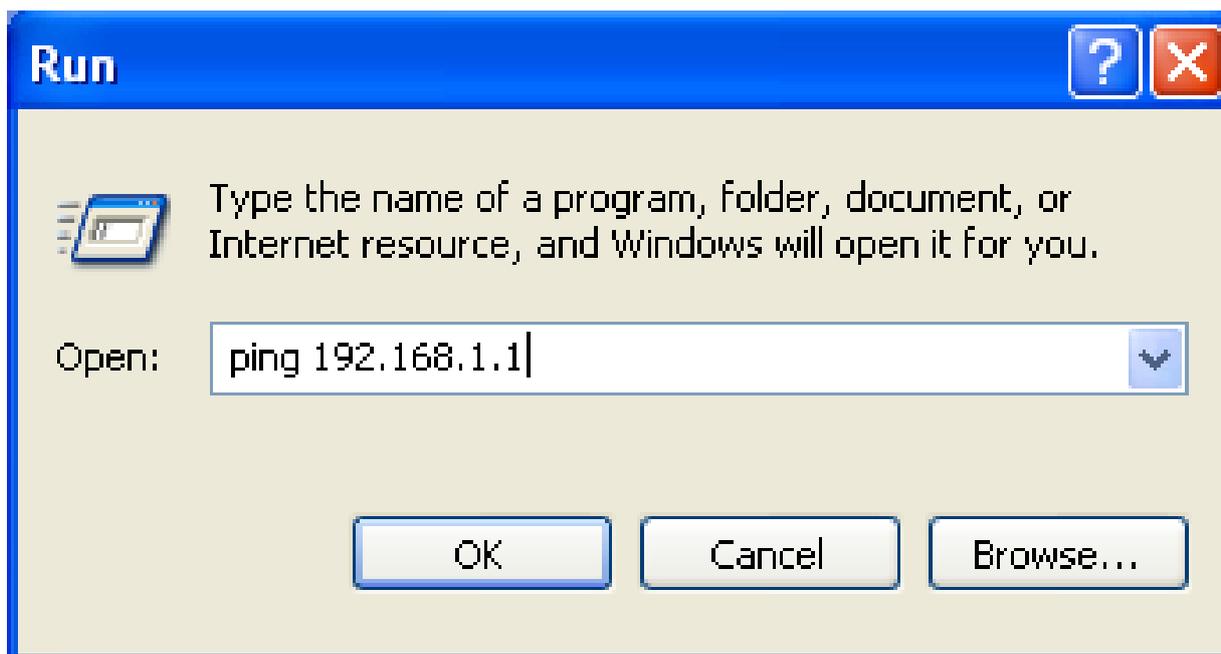


Step4 Select **Use the following IP address** and enter the IP address of the network adapter. The IP address should belong to the IP network segment 192.168. 1.X (X is a number between 2 and 254).



Step5 Set subnet mask and then click the **OK** button to finish manual setting.

Step6 After finishing setting, you may ping the default IP address of the GR-124W, to check whether the current connection between PC and the GR-124W is normal. Click **RUN...** in the lower left corner on the desktop, and then enter **ping 192.168.1.1** in the dialog box. See the following figure:



Note:

192.168.1.1 is the default IP address of the LAN interface. If this IP address is changed and you need to ping the IP address of the GR-124W, you should enter the current IP address in the dialog box above.

Step7 If PC can ping through the default IP address of the GR-124W and the following page appears, it indicates that the connection between PC and the GR-124W is normal.

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

3.2 Introduction to PPPoE (ADSL) and DHCP (Auto config)

If you want to access the Internet via the GR-124W, there are two common access ways, including PPPoE and DHCP (Auto config). The following sections describe the common network connection modes of these two ways.

Note:

In the gateway mode, GR-124W provides 5 types uplink access modes, including STATIC (fixed IP), DHCP (Auto config), PPPoE (ADSL), L2TP, and PPTP. For more details, please refer to 5.3.2 WAN.

- **The Network Connection Mode of PPPoE**



If you access the Internet by PPPoE, please do as follows:

- Step1** Connect the uplink interface of ADSL or cable modem to the ISP office end, and make sure that the communication between both sides is normal. Set your ADSL or Cable modem to be bridge mode. For more details, please refer to ADSL or Cable modem user manual, or consult ISP, and the manufactures of the ADSL or cable modem.
- Step2** Use one Ethernet cable connects the LAN interface of the ADSL or cable modem to the WAN interface of the GR-124W.
- Step3** Use one Ethernet cable connects your PC to the LAN interface of the GR-124W. Set the TCP/IP properties of the network adapter. By default, it is recommended you set the network adapter to be **Obtain an IP address automatically**. If you want to manually set the TCP/IP properties, please refer to 3.1 TCP/IP Settings.
- Step4** Log in to the Web page of the GR-124W. Click **Internet > WAN** to display the **Wide Area Network (WAN) Settings** page.

Internet	Operation Mode	Internet	Wireless	Firewall																		
		Lan Wan Advanced Routing DHCP QoS																				
Wan Setting	<h3>Wide Area Network (WAN) Settings</h3> <p>You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.</p> <p>WAN Connection Type: PPPoE (ADSL) ▾</p> <table border="1"> <thead> <tr> <th colspan="2">PPPoE Mode</th> </tr> </thead> <tbody> <tr> <td>User Name</td> <td>pppoe_user</td> </tr> <tr> <td>Password</td> <td>••••••••</td> </tr> <tr> <td>Verify Password</td> <td>••••••••</td> </tr> <tr> <td>Operation Mode</td> <td>Keep Alive ▾</td> </tr> <tr> <td></td> <td>Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds</td> </tr> <tr> <td></td> <td>On demand Mode: Idle Time <input type="text" value="5"/> minutes</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="2">MAC Clone</th> </tr> </thead> <tbody> <tr> <td>Enabled</td> <td>Disable ▾</td> </tr> </tbody> </table> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>				PPPoE Mode		User Name	pppoe_user	Password	••••••••	Verify Password	••••••••	Operation Mode	Keep Alive ▾		Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds		On demand Mode: Idle Time <input type="text" value="5"/> minutes	MAC Clone		Enabled	Disable ▾
PPPoE Mode																						
User Name	pppoe_user																					
Password	••••••••																					
Verify Password	••••••••																					
Operation Mode	Keep Alive ▾																					
	Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds																					
	On demand Mode: Idle Time <input type="text" value="5"/> minutes																					
MAC Clone																						
Enabled	Disable ▾																					

Step5 On the **Wide Area Network (WAN) Settings** page, set the **WAN Connection Type** to be **PPPoE (ADSL)** and enter the correct PPPoE username and password. After finishing setting, click the **Apply** button to start dial-up.

- **The Network Connection Mode of DHCP (Auto config)**



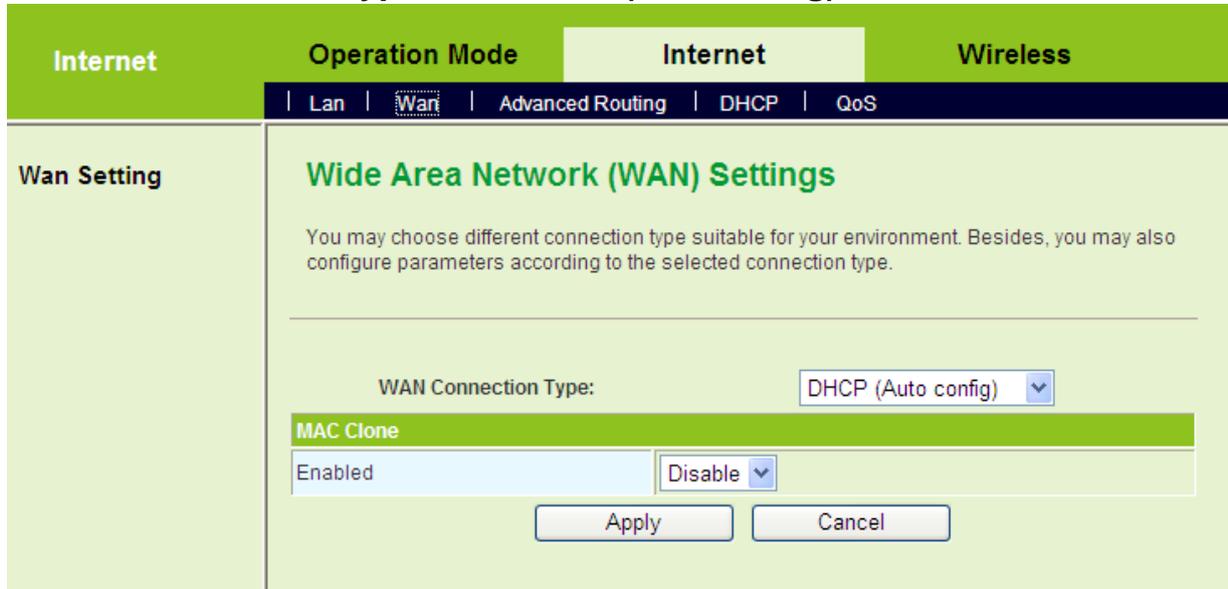
If you can access the Internet without dial-up, and ISP provides DHCP service, please follow the steps below to finish setting.

Step1 Use one Ethernet cable to connect the uplink interface of router or gateway to the WAN interface of the GR-124W.

Step2 Use one Ethernet cable connects your PC to the LAN interface of the GR-124W. Set the TCP/IP properties of the network adapter. By default, it is recommended you set the network adapter to be **Obtain an IP address**

automatically. If you want to manually set the TCP/IP properties, please refer to 3.1 TCP/IP Settings.

Step3 Log in to the Web page of the GR-124W. Click **Internet > WAN** to display the **Wide Area Network (WAN) Settings** page. On this page, set **WAN Connection Type** to be **DHCP (Auto config)**.



Step4 After finishing settings, click the **Apply** button, and then GR-124W starts to acquire the parameters assigned by the DHCP server, such as the IP address, and the DNS address.

3.3 Connection Introduction for Ethernet User

In the gateway mode, by default, the NAT function of the GR-124W is enabled. Users using the LAN interfaces of the GR-124W will use the same IP address of the WAN interface to access the Internet.

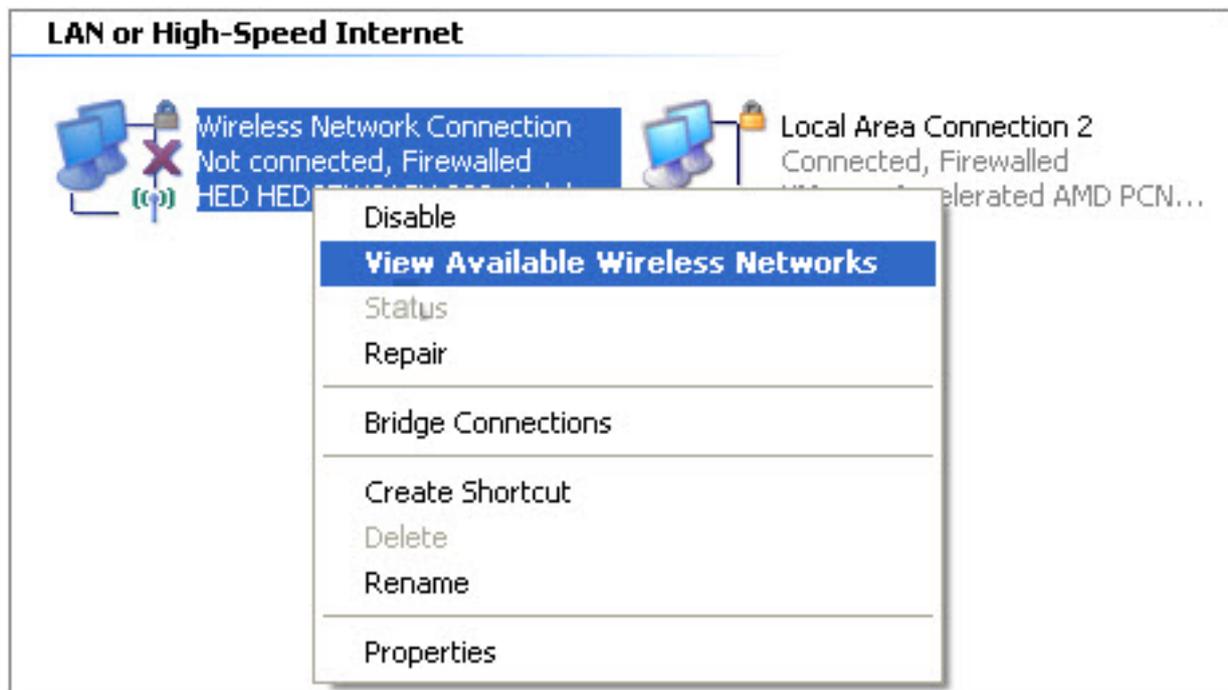
Usually, users using the LAN interfaces of the GR-124W need to set the network adapter to be **Obtain an IP address automatically**. If any user wants to manually set the TCP/IP properties, please refer to 3.1 TCP/IP Settings.

3.4 Connection Introduction for Wireless User

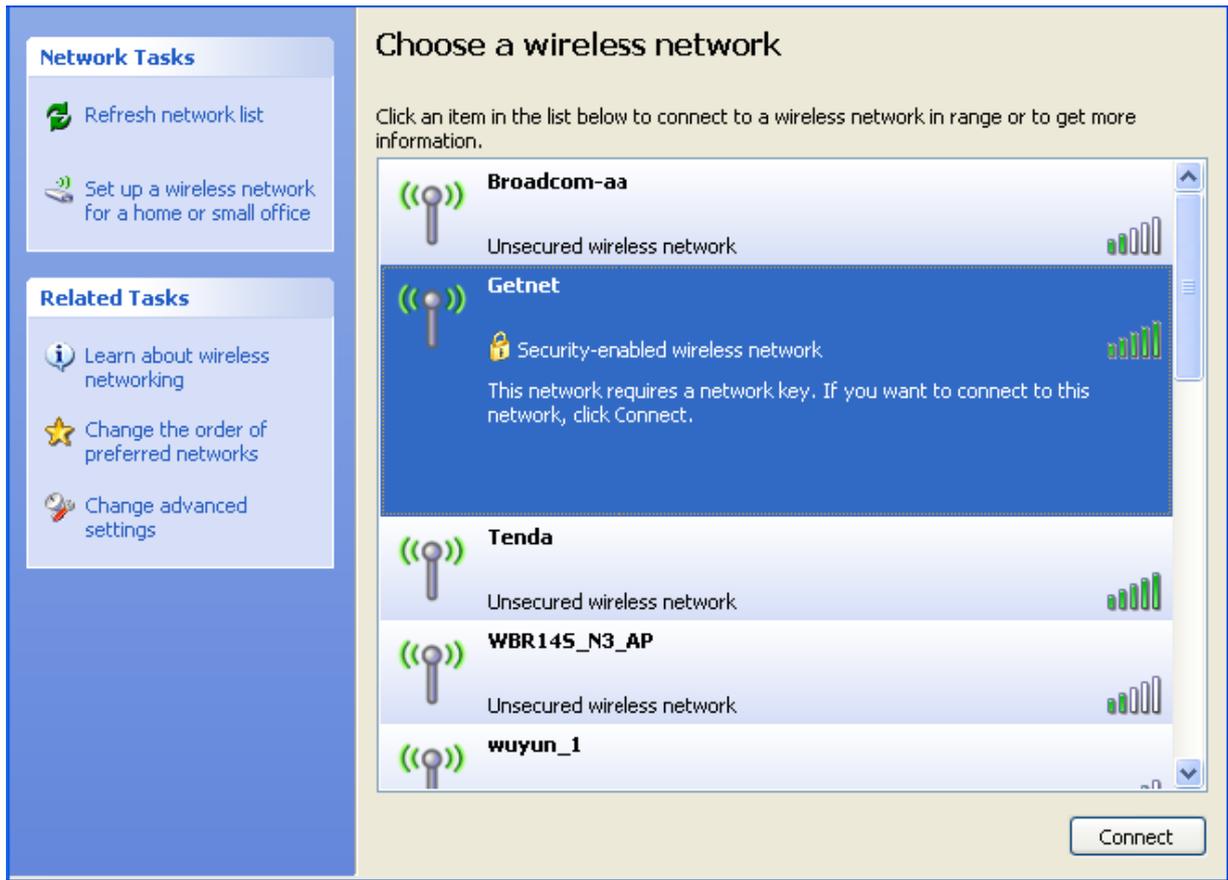
By default, the AP function of the GR-124W is enabled. User that uses the wireless network adapter can follow the steps below to finish setting.

Step1 Enable your wireless network adapter on your PC, and make sure that **Wireless Zero Configuration** tool is available. Right click the **Wireless**

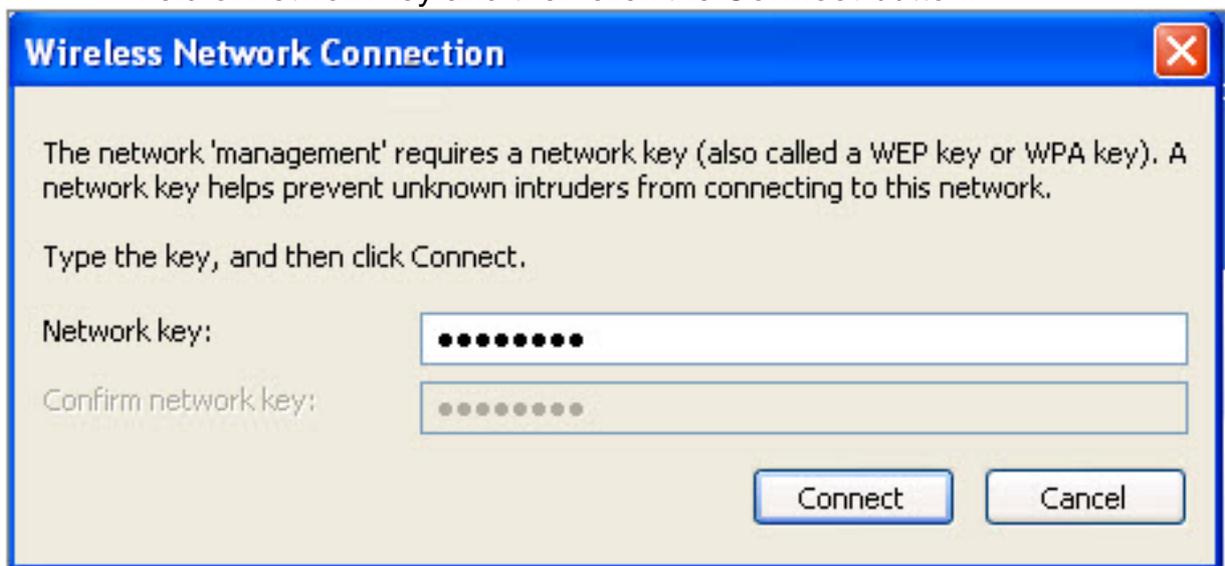
Network Connection icon and select **View Available Wireless Networks**.



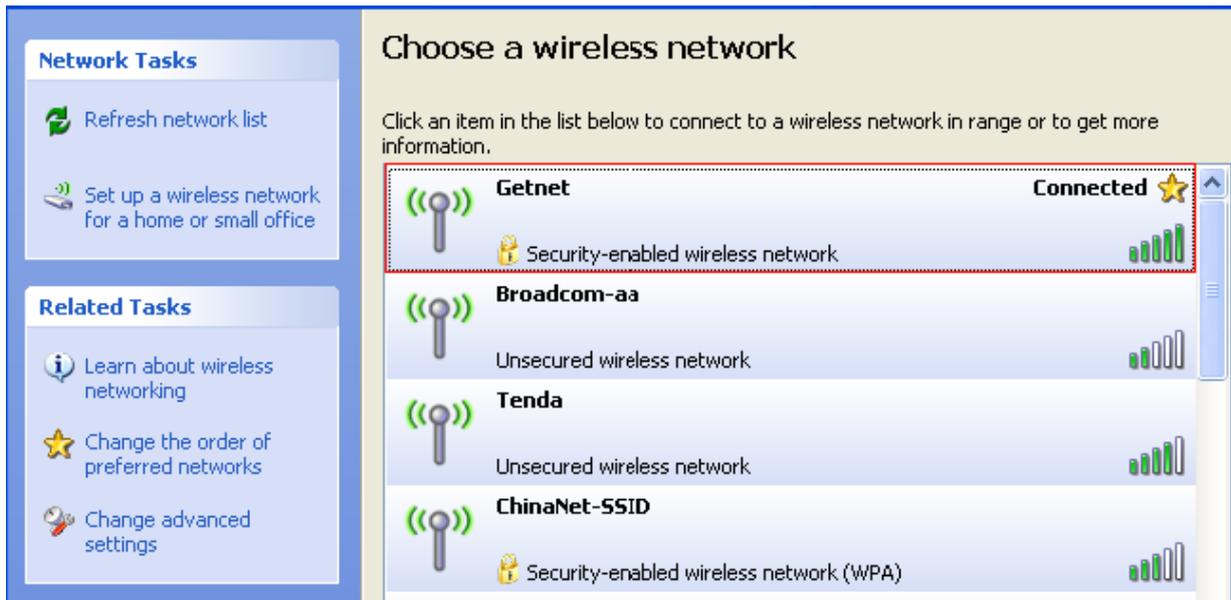
Step2 On the **Wireless Network Connection** page, click **Refresh network list** and the network list will be refreshed. The default SSID of the GR-124W is **Getnet**. Choose the AP that you want to connect, and then click the **Connect** button. The default wireless security mode is **Disable**, and you can connect AP directly without the encryption key. If the GR-124W is encrypted, this AP is marked with a lock icon.



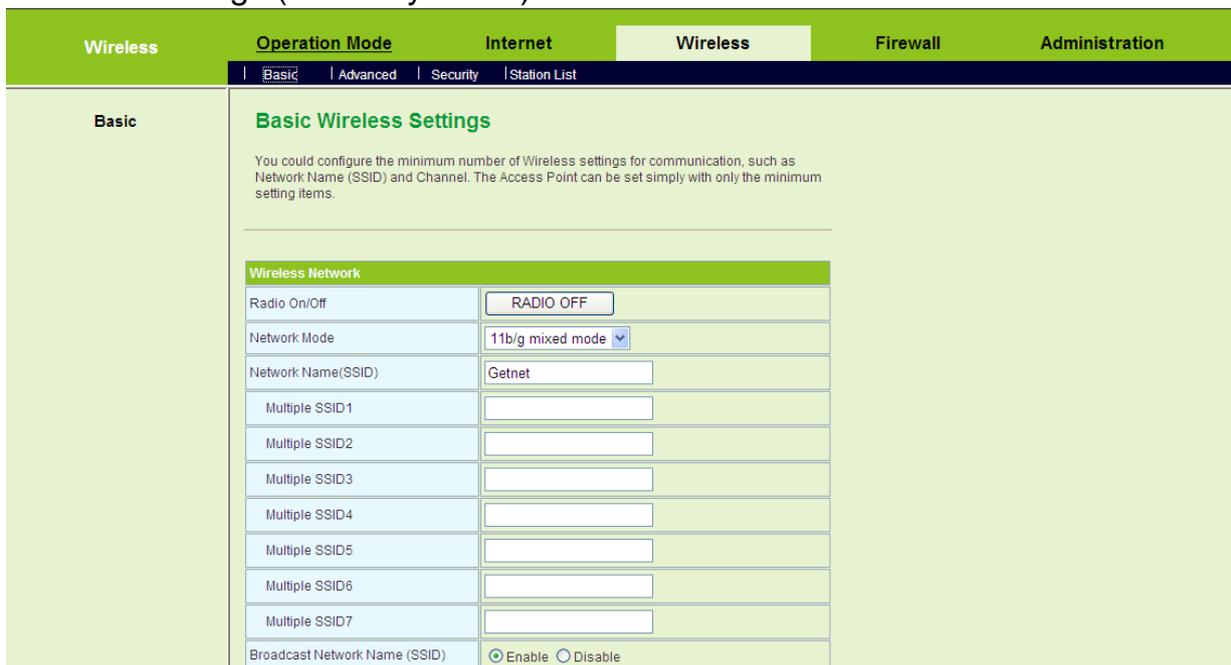
Step3 If the GR-124W is encrypted, you need to enter the encryption key in the field of network key and then click the **Connect** button.



Step4 If the wireless network card connects to GR-124W successfully, the character **Connected** will appear in the AP's upper right corner.



Step5 If you are not sure of the SSID available, please log in to the Web page of AP, and view the SSID on the **Basic Wireless Settings** page. For more information about the wireless settings, please refer to 5.4 Wireless Settings (Gateway Mode).



Note:

*After your wireless network card connects to AP successfully, usually, you should set the network adapter to be **Obtain an IP address automatically**.*

3.5 Log In to the Web Page

Open the browser, and enter **http://192.168.1.1/** in the IE address bar.



Enter the user name (**admin**, by default) and the password (**admin**, by default) on the login page.

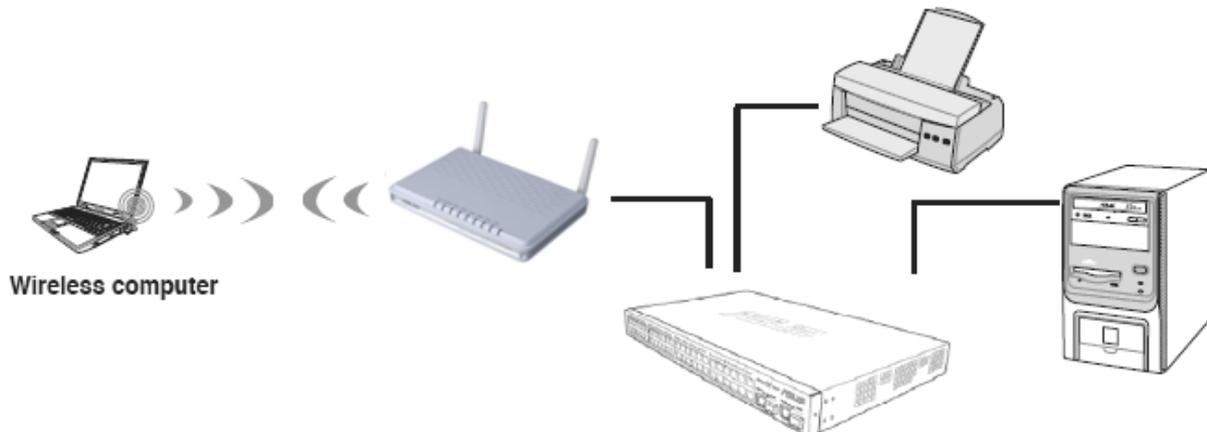


After clicking the **OK** button on the login page, you can log in to the Web page

4 Quick Start

4.1 Quick Start in the Bridge Mode

In the bridge mode, you may connect the LAN interfaces of the GR-124W or other wireless devices to a LAN.



Click **Operation Mode** to display the **Operation Mode Configuration** page.

Operation Mode	Operation Mode	Internet	Wireless	Firewall
	Operation Mode Setting			
Operation Mode	<h3>Operation Mode Configuration</h3> <p>You may configure the operation mode suitable for you environment.</p> <p><input checked="" type="radio"/> Bridge: In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.</p> <p><input type="radio"/> Gateway: In this mode, the device is supposed to connect to Internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP/L2TP client or static IP.</p> <p><input type="radio"/> WISP: In this mode, all Ethernet ports are bridged together and the wireless interface of this router will connect to ISP's Access Point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP/L2TP client or static IP.</p> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>			

On the **Operation Mode Configuration** page, choose the **Bridge** mode, and then click the **Apply** button.

Wireless Settings

Click **Wireless > Basic** to display the **Basic Wireless Settings** page.

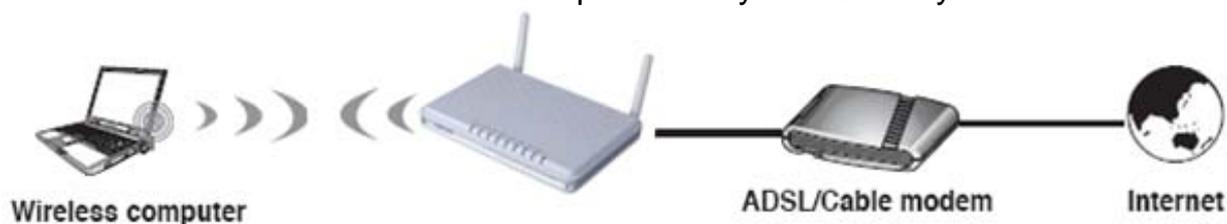
Wireless	Operation Mode	Internet	Wireless	Firewall	Administration
Basic Advanced Security Station List					
Basic					
Wireless Network					
Radio On/Off	<input type="button" value="RADIO OFF"/>				
Network Mode	11b/g mixed mode				
Network Name(SSID)	Getnet				
Multiple SSID1	<input type="text"/>				
Multiple SSID2	<input type="text"/>				
Multiple SSID3	<input type="text"/>				
Multiple SSID4	<input type="text"/>				
Multiple SSID5	<input type="text"/>				
Multiple SSID6	<input type="text"/>				
Multiple SSID7	<input type="text"/>				
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
BSSID	00:0C:43:30:52:F0				
Frequency (Channel)	2462MHz (Channel 11)				
Rate	Auto				
Wireless Distribution System(WDS)					
WDS Mode	Disable				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

On this page, enable the radio switch and set at least one legal SSID. Make sure that the wireless devices can connect to the AP.

After finish the settings, click the **Apply** button to apply the settings.

4.2 Quick Start in the Gateway Mode

In the gateway mode, the GR-124W accesses the Internet by ADSL or cable modem, and several users share the IP address provided by the ISP on your network.



In the gateway mode:

- NAT is enabled.
- WAN interface can be connected to the Internet by STATIC (fixed IP), DHCP (Auto config), PPPoE (ADSL), L2TP, and PPTP.

If you want to configure GR-124W working in gateway mode, do as follows:
Click **Operation Mode** to display the **Operation Mode Configuration** page.

Operation Mode | **Operation Mode** | **Internet** | **Wireless**

Operation Mode Setting

Operation Mode

Operation Mode Configuration

You may configure the operation mode suitable for you environment.

Bridge:
In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

Gateway:
In this mode, the device is supposed to connect to Internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP/L2TP client or static IP.

WISP:
In this mode, all Ethernet ports are bridged together and the wireless interface of this router will connect to ISP's Access Point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP/L2TP client or static IP.

NAT Enabled

On the **Operation Mode Configuration** page, choose the **Gateway** mode, and then click the **Apply** button.

4.2.1 System Management

If you want to set the network time, click **Administration > Management** to display the **System Management** page.

Administration	Operation Mode	Internet	Wireless	Firewall	Administration
Management Upload Settings Status Statistics Log					
Management	You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.				
	Administrator Settings				
	Account	<input type="text" value="admin"/>			
	Password	<input type="password" value="••••"/>			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					
NTP Settings					
Current Time	<input type="text" value="Sat Jan 1 00:03:05 UTC 2000"/>		<input type="button" value="Sync with host"/>		
Time Zone:	<input type="text" value="(GMT+08:00) China Coast, Hong Kong"/>				
NTP Server	<input type="text"/> <small>ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw</small>				
NTP synchronization(hours)	<input type="text"/>				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					
DDNS Settings					
Dynamic DNS Provider	<input type="text" value="None"/>				
Account	<input type="text"/>				
Password	<input type="text"/>				
DDNS	<input type="text"/>				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

In the table of **NTP Settings**, choose your time zone, enter the NTP server address, and set the NTP synchronization time. After finish setting, click the **Apply** button to apply the settings, and then AP can synchronize its time with the network time server.

4.2.2 LAN Settings

If you want to change the default IP address of the GR-124W, click the **Internet > LAN** to display the **Local Area Network (LAN) Settings** page.

Internet	Operation Mode	Internet	Wireless	Firewall
	Lan Wan Advanced Routing DHCP QoS			
Internet	<h2>Local Area Network (LAN) Settings</h2> <p>You may enable/disable networking functions and configure their parameters as your wish.</p>			
LAN Setup				
IP Address	<input type="text" value="192.168.1.1"/>			
Subnet Mask	<input type="text" value="255.255.255.0"/>			
LAN 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
LAN2 IP Address	<input type="text"/>			
LAN2 Subnet Mask	<input type="text"/>			
MAC Address	<input type="text" value="00:0C:43:30:52:77"/>			
DHCP Type	Server ▾			
Start IP Address	<input type="text" value="192.168.1.2"/>			
End IP Address	<input type="text" value="192.168.1.254"/>			
Subnet Mask	<input type="text" value="255.255.255.0"/>			
Primary DNS Server	<input type="text" value="192.168.1.1"/>			
Secondary DNS Server	<input type="text" value="192.168.1.1"/>			
Default Gateway	<input type="text" value="192.168.1.1"/>			
Lease Time	<input type="text" value="86400"/>			
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>			
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>			
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>			
802.1d Spanning Tree	Disable ▾			
IGMP Proxy	Disable ▾			
IGMP Snooping	Disable ▾			
UPNP	Disable ▾			
Router Advertisement	Disable ▾			
PPPoE Relay	Disable ▾			
DNS Proxy	Enable ▾			
		Apply		Cancel

On this page, you may manually enter the IP address. It is recommended you keep

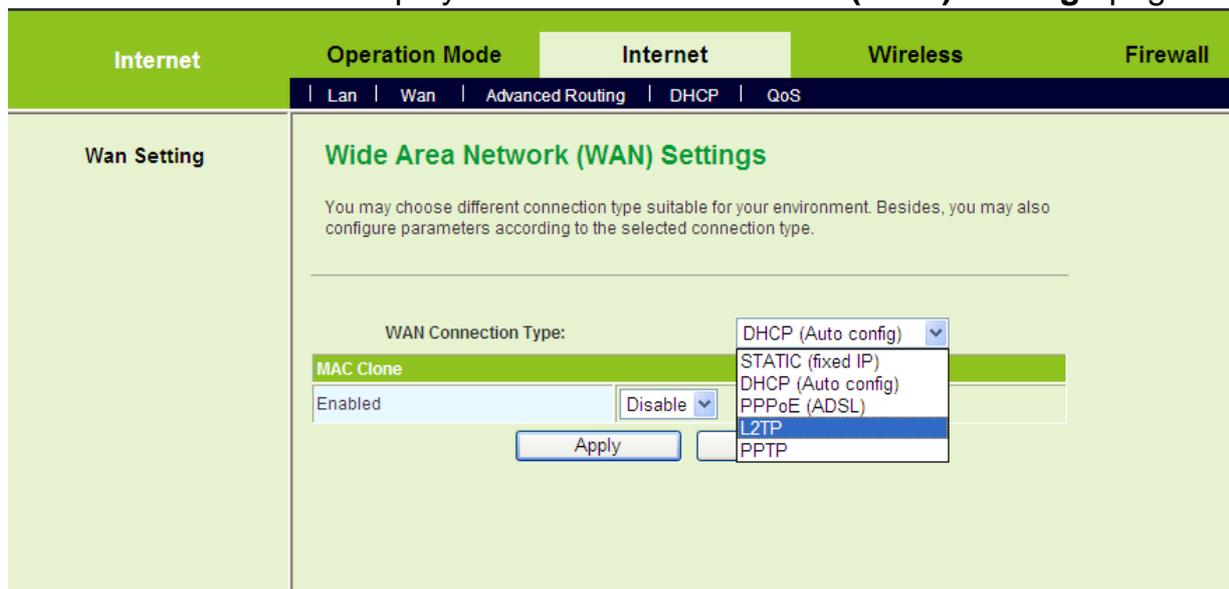
the default setting.

If you do not know the IP address of the DNS server provided by the ISP, please enable DNS Proxy and change your network setting. Assign the IP address of current DNS server to be the LAN IP address of the GR-124W. If you use P2P software, the UPnP function needs to be enabled.

After finishing setting, click the **Apply** button to apply the settings.

4.2.3 WAN Settings

Click **Internet > WAN** to display the **Wide Area Network (WAN) Settings** page.



This page provides 5 types of WAN connection modes, including STATIC (fixed IP), DHCP (Auto config), PPPoE (ADSL), L2TP, and PPTP. On this page, select the proper WAN connection type according to the connection types provided by your ISP, and configure its parameters.

After finishing setting, click the **Apply** button to apply the settings.

4.2.4 Wireless Settings

Click **Wireless > Basic** to display the **Basic Wireless Settings** page.

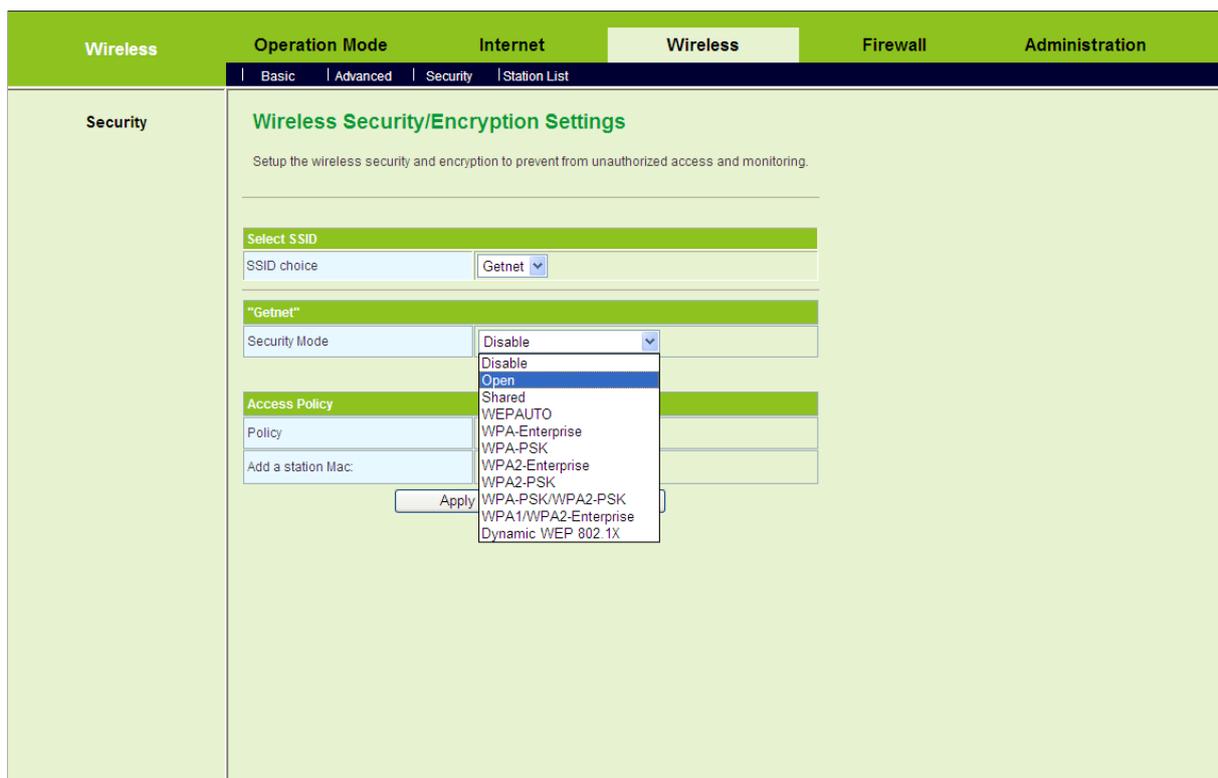
Wireless		Operation Mode		Internet		Wireless		Firewall	
		Basic		Advanced		Security		Station List	
Basic									
Wireless Network									
Radio On/Off		RADIO OFF							
Network Mode		11b/g mixed mode							
Network Name(SSID)		11b/g mixed mode							
Multiple SSID1		11b only							
Multiple SSID2		11g only							
Multiple SSID3									
Multiple SSID4									
Multiple SSID5									
Multiple SSID6									
Multiple SSID7									
Broadcast Network Name (SSID)		<input checked="" type="radio"/> Enable <input type="radio"/> Disable							
AP Isolation		<input type="radio"/> Enable <input checked="" type="radio"/> Disable							
MBSSID AP Isolation		<input type="radio"/> Enable <input checked="" type="radio"/> Disable							
BSSID		00:0C:43:30:52:F0							
Frequency (Channel)		2462MHz (Channel 11)							
Rate		Auto							
Wireless Distribution System(WDS)									
WDS Mode		Disable							
Apply					Cancel				

On this page, it provides 3 types of network modes, including 11 b/g mixed, 11 b only, and 11 g only modes. The default network mode is 11 b/g mixed mode. You can set the SSID according to your actual application. The maximum character length is up to 32 characters. The default channel is channel11.

After finishing setting, click the **Apply** button to apply the settings.

4.2.5 Wireless Security

Click **Wireless > Security** to display the **Wireless Security/Encryption Settings** page.



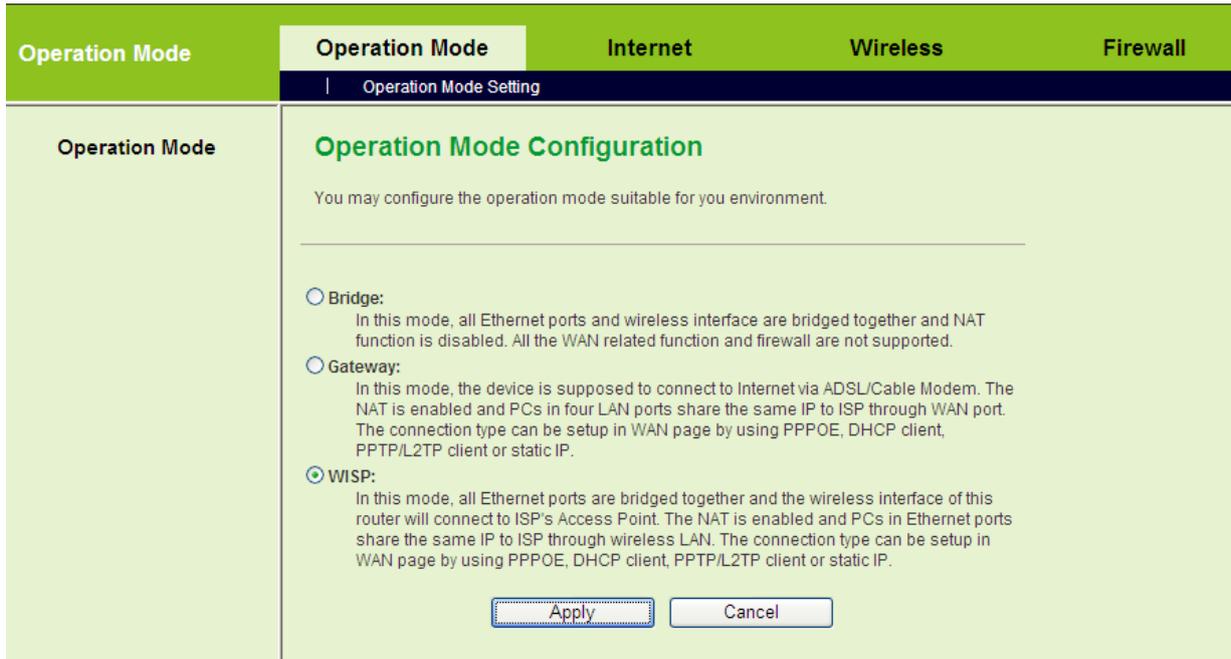
On this page, you can set the security mode. The security modes include Open, Shared, WEPAUTO, WPA-Enterprise, WPA-PSK, WPA2-Enterprise, WPA2-PSK, WPA-PSK/WPA2-PSK, WPA1/WPA2-Enterprise, and Dynamic WEP 802.1X. After finishing setting, click the **Apply** button to apply the settings.

4.3 Quick Start in the WISP Mode

In the WISP (Wireless Internet Service Provider) mode, GR-124W works as a station, and it can connect to another AP. All the Ethernet interfaces can access the Internet by wireless routing. Several GR-124Ws can realize more flexible network structure.

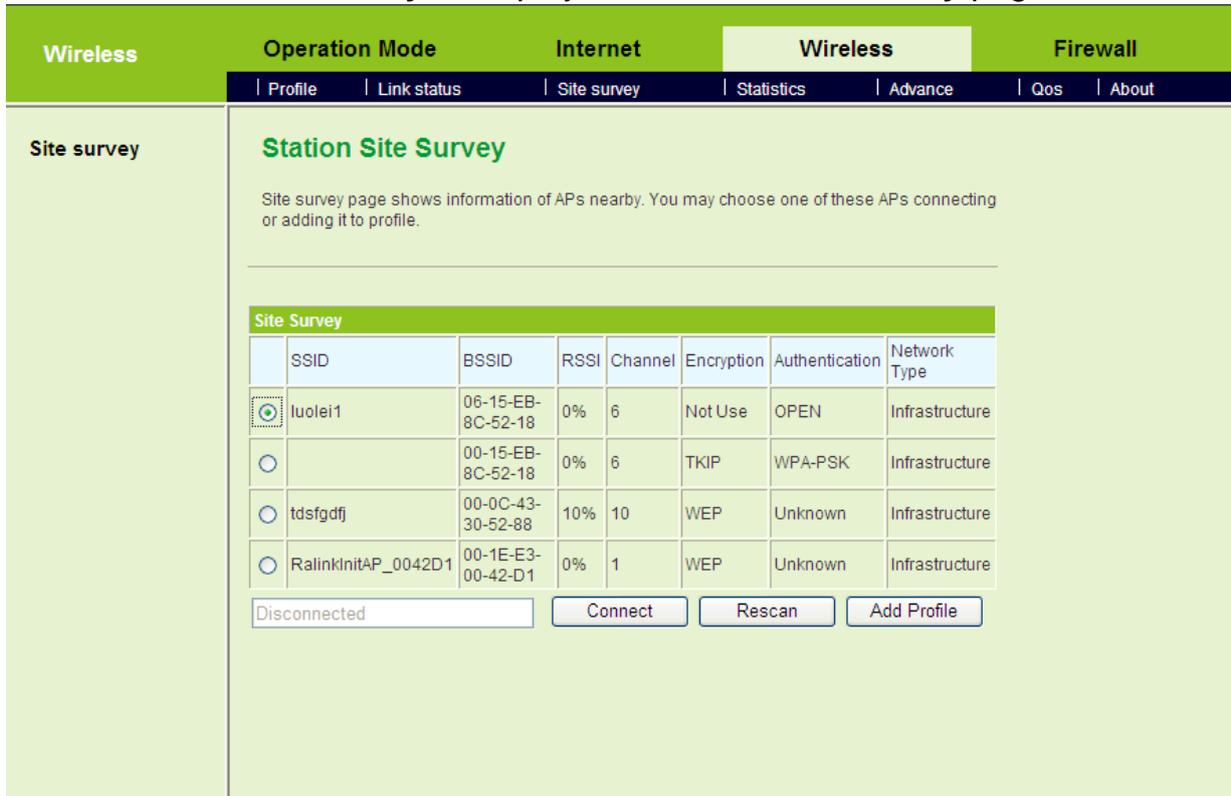


Click **Operation Mode** to display the **Operation Mode Configuration** page.



On the **Operation Mode Configuration** page, choose the **WISP** mode, and then click the **Apply** button.

Click **Wireless > Site Survey** to display the **Station Site Survey** page.



On this page, choose an AP in the **Site Survey** list, and then click the **Connect** button. After clicking the **Connect** button, the following page appears.

SSID

Security Policy

Security Mode

This is no any security. Are you sure to connect AP?

If this AP is not encrypted, you can click the **Apply** button on the pop-up page to confirm the connection.

If the AP that you want to connect is encrypted, you need to enter the key on the pop-up page.

If the connection succeeds, the SSID of the AP in the **Site Survey** list will be marked with an icon .

Wireless | Operation Mode | Internet | **Wireless** | Firewall

Profile | Link status | Site survey | Statistics | Advance | Qos | About

Site survey

Station Site Survey

Site survey page shows information of APs nearby. You may choose one of these APs connecting or adding it to profile.

Site Survey							
	SSID	BSSID	RSSI	Channel	Encryption	Authentication	Network Type
<input checked="" type="radio"/>	luolei1	06-15-EB-8C-52-18	0%	6	Not Use	OPEN	Infrastructure
<input type="radio"/>	tdsfgdfj	00-0C-43-30-52-88	20%	10	WEP	Unknown	Infrastructure

Connected <--> luolei1

After finishing the connection, you may establish PPPoE, L2TP, PPTP, DHCP, and Static connections. For more details, please refer to 5.3.2 WAN.

5 Web Configuration

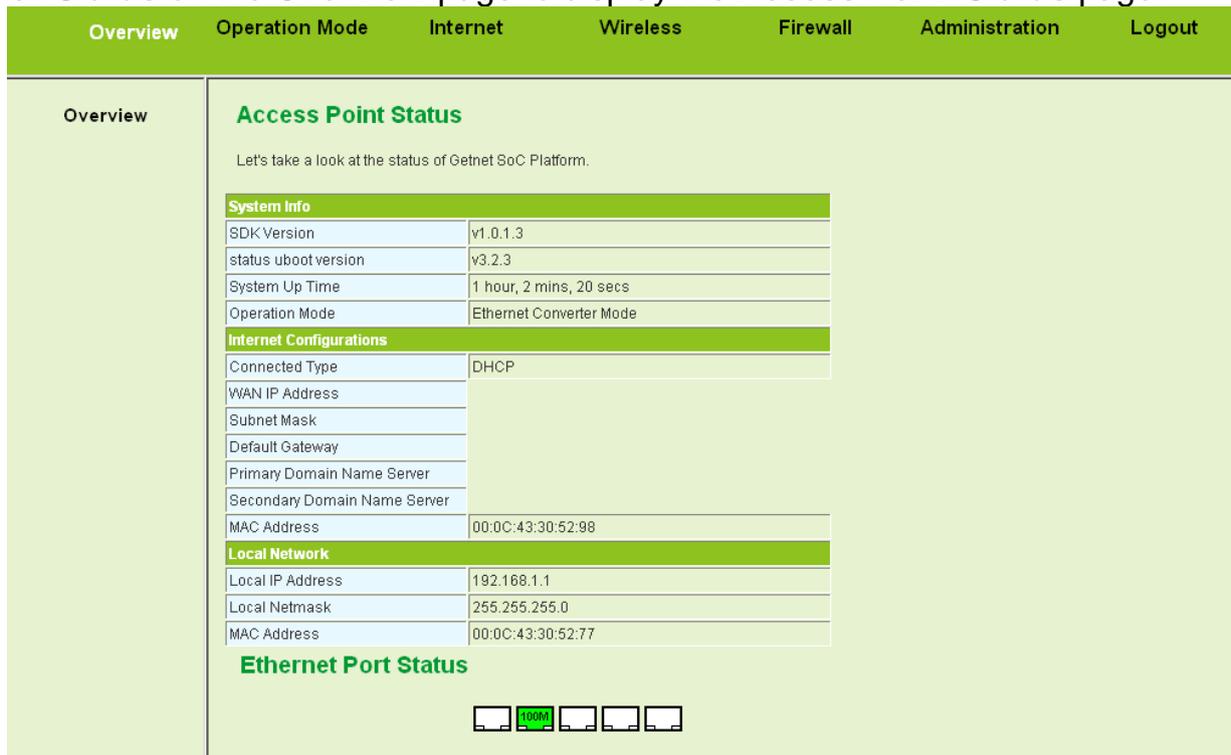
5.1 Overview

After finishing login, system displays the **Overview** page. The **Overview** page includes **Status**, **Statistic**, and **Management** submenus



5.1.1 Status

Click **Status** on the **Overview** page to display the **Access Point Status** page.



This page displays system information, Internet configuration, and local network settings.

5.1.2 Statistic

Click **Statistic** on the **Overview** page to display the **Statistic** page.

Overview	Operation Mode	Internet	Wireless	Firewall																																		
Overview	<h3>Statistic</h3> <p>Take a look at the Getnet SoC statistics</p> <table border="1"> <thead> <tr> <th colspan="2">Memory</th> </tr> </thead> <tbody> <tr> <td>Memory total:</td> <td>13892 kB</td> </tr> <tr> <td>Memory left:</td> <td>2428 kB</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="2">WAN/LAN</th> </tr> </thead> <tbody> <tr> <td>WAN Rx packets:</td> <td>262</td> </tr> <tr> <td>WAN Rx bytes:</td> <td>20406</td> </tr> <tr> <td>WAN Tx packets:</td> <td>2097</td> </tr> <tr> <td>WAN Tx bytes:</td> <td>0</td> </tr> <tr> <td>LAN Rx packets:</td> <td>2871</td> </tr> <tr> <td>LAN Rx bytes:</td> <td>372753</td> </tr> <tr> <td>LAN Tx packets:</td> <td>7211</td> </tr> <tr> <td>LAN Tx bytes:</td> <td>3451217</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="2">All interfaces</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td>lo</td> </tr> <tr> <td>Rx Packet</td> <td>15</td> </tr> <tr> <td>Rx Byte</td> <td>2263</td> </tr> <tr> <td>Tx Packet</td> <td>15</td> </tr> </tbody> </table>				Memory		Memory total:	13892 kB	Memory left:	2428 kB	WAN/LAN		WAN Rx packets:	262	WAN Rx bytes:	20406	WAN Tx packets:	2097	WAN Tx bytes:	0	LAN Rx packets:	2871	LAN Rx bytes:	372753	LAN Tx packets:	7211	LAN Tx bytes:	3451217	All interfaces		Name	lo	Rx Packet	15	Rx Byte	2263	Tx Packet	15
Memory																																						
Memory total:	13892 kB																																					
Memory left:	2428 kB																																					
WAN/LAN																																						
WAN Rx packets:	262																																					
WAN Rx bytes:	20406																																					
WAN Tx packets:	2097																																					
WAN Tx bytes:	0																																					
LAN Rx packets:	2871																																					
LAN Rx bytes:	372753																																					
LAN Tx packets:	7211																																					
LAN Tx bytes:	3451217																																					
All interfaces																																						
Name	lo																																					
Rx Packet	15																																					
Rx Byte	2263																																					
Tx Packet	15																																					

This page displays the memory status, the numbers of transmitted and received data packets of the WLAN, LAN, and WAN.

5.1.3 Management

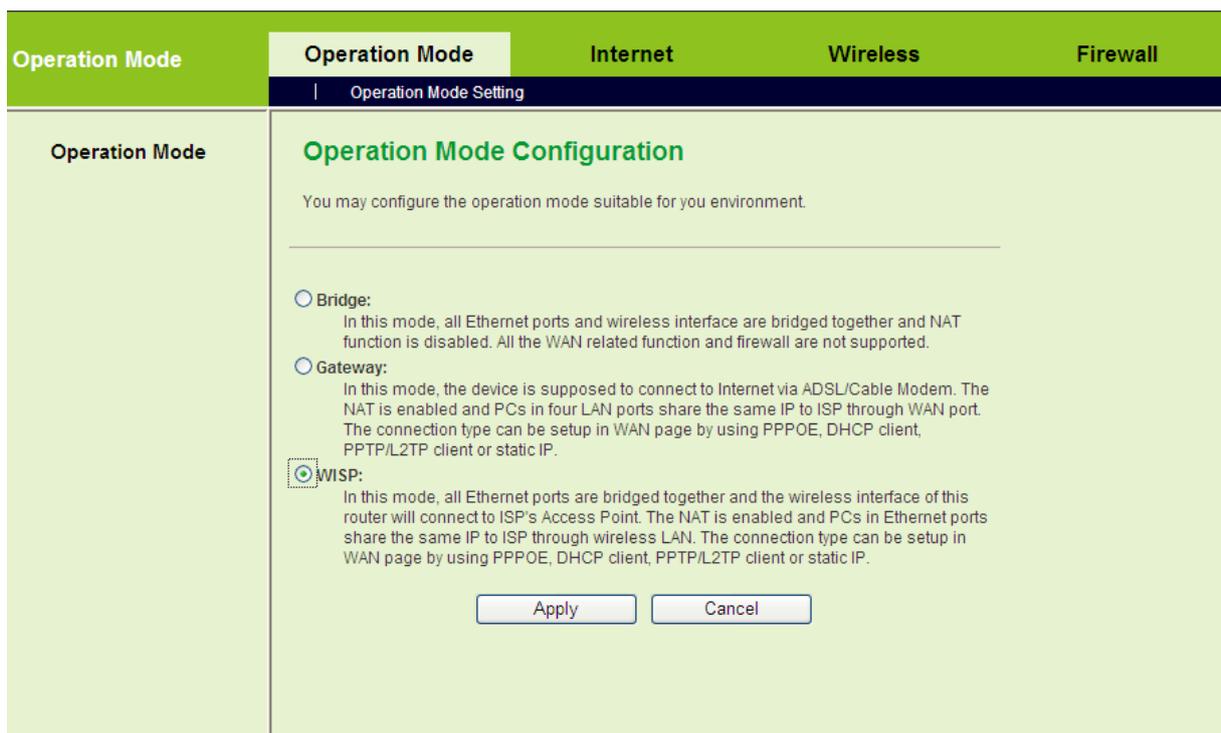
Click **Management** on the **Overview** page to display the **System Management** page.

Overview	Operation Mode	Internet	Wireless	Firewall	Administration	Logout																				
Overview	<h3>System Management</h3> <p>You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.</p> <hr/> <div style="border: 1px solid #ccc; padding: 5px;"> <h4>Administrator Settings</h4> <table border="1"> <tr> <td>Account</td> <td><input type="text" value="admin"/></td> </tr> <tr> <td>Password</td> <td><input type="password" value="•••••"/></td> </tr> </table> <p style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> </div> <hr/> <div style="border: 1px solid #ccc; padding: 5px;"> <h4>NTP Settings</h4> <table border="1"> <tr> <td>Current Time</td> <td><input type="text" value="Sat Jan 1 01:08:14 UTC 2000"/> <input type="button" value="Sync with host"/></td> </tr> <tr> <td>Time Zone:</td> <td><input type="text" value="(GMT+08:00) China Coast, Hong Kong"/></td> </tr> <tr> <td>NTP Server</td> <td> <input type="text"/> <p><small>ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw</small></p> </td> </tr> <tr> <td>NTP synchronization(hours)</td> <td><input type="text"/></td> </tr> </table> <p style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> </div> <hr/> <div style="border: 1px solid #ccc; padding: 5px;"> <h4>DDNS Settings</h4> <table border="1"> <tr> <td>Dynamic DNS Provider</td> <td><input type="text" value="None"/></td> </tr> <tr> <td>Account</td> <td><input type="text"/></td> </tr> <tr> <td>Password</td> <td><input type="text"/></td> </tr> <tr> <td>DDNS</td> <td><input type="text"/></td> </tr> </table> <p style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> </div>					Account	<input type="text" value="admin"/>	Password	<input type="password" value="•••••"/>	Current Time	<input type="text" value="Sat Jan 1 01:08:14 UTC 2000"/> <input type="button" value="Sync with host"/>	Time Zone:	<input type="text" value="(GMT+08:00) China Coast, Hong Kong"/>	NTP Server	<input type="text"/> <p><small>ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw</small></p>	NTP synchronization(hours)	<input type="text"/>	Dynamic DNS Provider	<input type="text" value="None"/>	Account	<input type="text"/>	Password	<input type="text"/>	DDNS	<input type="text"/>	
Account	<input type="text" value="admin"/>																									
Password	<input type="password" value="•••••"/>																									
Current Time	<input type="text" value="Sat Jan 1 01:08:14 UTC 2000"/> <input type="button" value="Sync with host"/>																									
Time Zone:	<input type="text" value="(GMT+08:00) China Coast, Hong Kong"/>																									
NTP Server	<input type="text"/> <p><small>ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw</small></p>																									
NTP synchronization(hours)	<input type="text"/>																									
Dynamic DNS Provider	<input type="text" value="None"/>																									
Account	<input type="text"/>																									
Password	<input type="text"/>																									
DDNS	<input type="text"/>																									

This page provides administration settings, NTP settings, and DDNS settings. For more details, please refer to 5.7.1 Management.

5.2 Operation Mode

Click the **Operation Mode** to display the **Operation Mode Configuration** page.



GETNET GR-124W provides three types of operation modes, including Bridge, Gateway, and WISP modes.

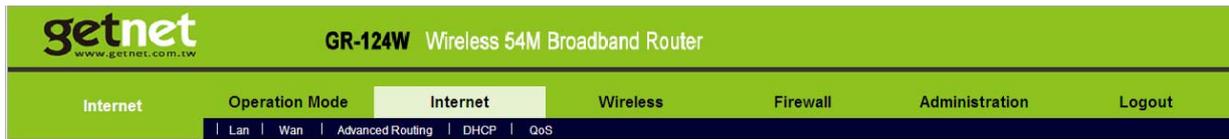
The parameters on this page are described as follows:

Mode	Description
Bridge	In the bridge mode, AP acts as a hub.
Gateway	In the gateway mode, GR-124W allows routing between WAN and LAN, or WAN and wireless network.
WISP	In the WISP mode, all the Ethernet interfaces can access the Internet by wireless routing.
NAT Enabled	Only in the gateway mode can this function be used. After enabling NAT, it can provide address translation between the interior network and the exterior network for LAN and wireless network.

After finishing setting, click the **Apply** button to apply the settings.

5.3 Internet Settings

In the gateway mode, the following figure shows the navigation menu of the **Internet** settings:



The sub-menus of the **Internet** include **LAN**, **WAN**, **Advanced Routing**, **DHCP**, and **QoS**.

5.3.1 LAN

Click **Internet > LAN** to display the **Local Area Network (LAN) Settings** page.

Internet	Operation Mode	Internet	Wireless	Firewall	
	Lan	Wan	Advanced Routing	DHCP	QoS
Internet	<h2>Local Area Network (LAN) Settings</h2> <p>You may enable/disable networking functions and configure their parameters as your wish.</p>				
LAN Setup					
IP Address	<input type="text" value="192.168.1.1"/>				
Subnet Mask	<input type="text" value="255.255.255.0"/>				
LAN 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
LAN2 IP Address	<input type="text"/>				
LAN2 Subnet Mask	<input type="text"/>				
MAC Address	00:0C:43:30:52:77				
DHCP Type	Server ▾				
Start IP Address	<input type="text" value="192.168.1.2"/>				
End IP Address	<input type="text" value="192.168.1.254"/>				
Subnet Mask	<input type="text" value="255.255.255.0"/>				
Primary DNS Server	<input type="text" value="192.168.1.1"/>				
Secondary DNS Server	<input type="text" value="192.168.1.1"/>				
Default Gateway	<input type="text" value="192.168.1.1"/>				
Lease Time	<input type="text" value="86400"/>				
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>				
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>				
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>				
802.1d Spanning Tree	Disable ▾				
IGMP Proxy	Disable ▾				
IGMP Snooping	Disable ▾				
UPNP	Disable ▾				
Router Advertisement	Disable ▾				
PPPoE Relay	Disable ▾				
DNS Proxy	Enable ▾				
		Apply		Cancel	

This page is used to configure the LAN parameters. This page allows you to

configure LAN interface properties, DHCP server properties, and other parameters related to LAN.

The parameters on this page are described as follows:

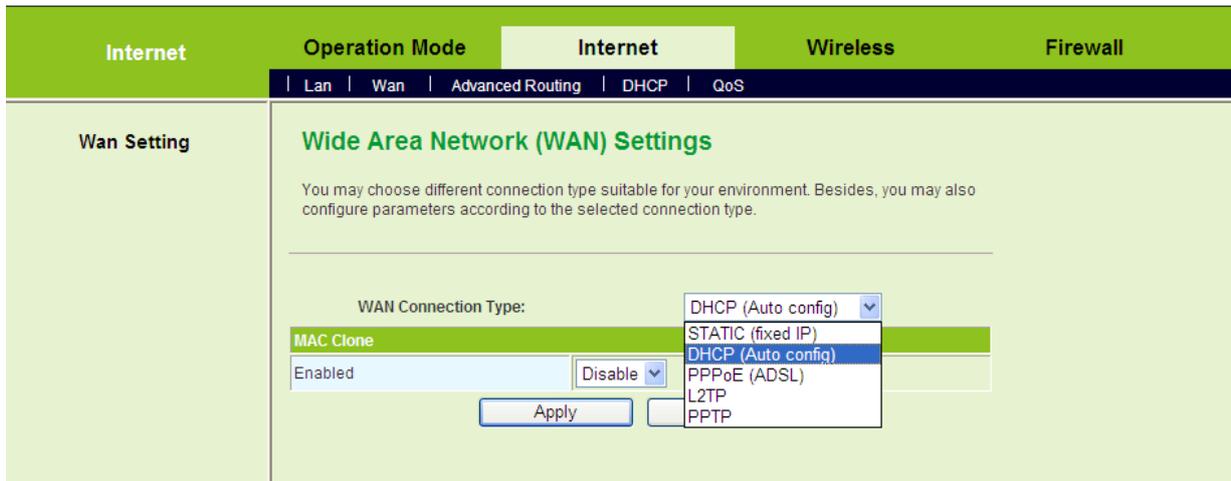
Field	Description
IP Address	The IP address of the LAN interface. The default IP address is 192.168.1.1.
Subnet Mask	The subnet mask of the IP address of the LAN interface. The default subnet mask is 255.255.255.0.
LAN 2	Enable or disable the second IP address of the LAN interface. The default setting is Disable .
LAN 2 IP Address	The second IP address of the LAN interface. This IP address should not collide with the IP address of the interior network.
LAN 2 Subnet Mask	The subnet mask of the second IP address of the LAN interface.
MAC Address	Display the current MAC address that LAN interface uses.
DHCP Type	<p>Enable or disable DHCP service. You can select Server or Disable in the drop down list. The default setting is Server, it indicates DHCP service is enabled. After enabling DHCP service, you can configure the following parameters of the DHCP server:</p> <ul style="list-style-type: none"> ● Start IP Address: The start IP address of the DHCP address pool. ● End IP Address: The end IP address of the DHCP address pool. ● Subnet Mask: The subnet mask that DHCP server assigns. ● Primary DNS Server: The primary DNS server that DHCP server assigns. ● Secondary DNS Server: The secondary DNS server that DHCP server assigns. ● Default Gateway: The gateway that DHCP server assigns. ● Lease Time: The lease time of the IP address. ● Statically Assigned: For binding MAC and IP.
802.1d	It provides redundant link and prevents network from

Field	Description
Spanning Tree	generating loop. You may select Enable or Disable .
LLTD	After enabling LLTD (Link Layer Topology Discovery), Windows Vista automatically discovers other devices' link topologies, and these devices are also compatible with LLTD. You may select Enable or Disable .
IGMP Proxy	Enable or disable IGMP Proxy.
IGMP Snooping	Enable or disable IGMP Snooping. After enabling this function, the packets of the IGMP broadcast will not be sent to the LAN interface that does not belong to the group.
UPNP	Enable or disable the UPnP function. After enabling this function, AP will provide automatic port-mapping for P2P software on the interior network.
Router Advertisement	Enable or disable router advertisement. After enabling this function, APs will send broadcast message or send back message to show their existence.
PPPoE Relay	Enable or disable PPPoE Relay. After enabling this function, the local PC can directly make PPPoE dial-up in the gateway mode.
DNS Proxy	Enable or disable DNS Proxy. After enabling this function, the devices on the LAN where AP acts as a proxy can send domain resolution request to AP.

After finishing the settings, click the **Apply** button to apply the settings.

5.3.2 WAN

Click **Internet > WAN** to display the **Wide Area Network (WAN) Settings** page.



This page is used to configure the WAN connection parameters. On this page, you may choose the proper WAN connection type and configure the parameters related to the connection type.

The parameters on this page are described as follows:

Field	Description
WAN Connection Type	The WAN connection types include STATIC (fixed IP), DHCP (Auto config), PPPoE (ADSL), L2TP, and PPTP. The default WAN connection type is DHCP (Auto config) .
MAC Clone	Enable or disable MAC Clone. After enabling this function, click the Fill my MAC button, and then AP will use this MAC address to communicate with the device that connects to the AP's WAN interface. The default setting is Disable .

- **STATIC (fixed IP)**

On the **Wide Area Network (WAN) Settings** page, select **STATIC (fixed IP)** as the WAN connection type, and the following page appears.

The screenshot shows the 'Wide Area Network (WAN) Settings' page. The 'WAN Connection Type' is set to 'STATIC (fixed IP)'. The 'Static Mode' section contains the following fields:

IP Address	172.16.38.12
Subnet Mask	255.255.254.0
Default Gateway	172.16.38.1
Primary DNS Server	10.28.100.2
Secondary DNS Server	

The 'MAC Clone' section has 'Enabled' set to 'Disable'. 'Apply' and 'Cancel' buttons are at the bottom.

On this page, enter the IP address, the subnet mask, the default gateway, and the DNS server provided by the ISP.

After finishing setting, click the **Apply** button to apply the settings.

- **DHCP (Auto config)**

On the **Wide Area Network (WAN) Settings** page, select **DHCP (Auto config)** as the WAN connection type, and the following page appears.

The screenshot shows the 'Wide Area Network (WAN) Settings' page. The 'WAN Connection Type' is set to 'DHCP (Auto config)'. The 'MAC Clone' section has 'Enabled' set to 'Disable'. 'Apply' and 'Cancel' buttons are at the bottom.

If you select DHCP (Auto config), AP acquires the network parameters via WAN interface, such as the IP address, the subnet mask, the gateway, and the DNS server address.

After finishing the settings, click the **Apply** button to apply the settings.

- **PPPoE (ADSL)**

If you want to use PPPoE service, please select **PPPoE (ADSL)** connection type. On the **Wide Area Network (WAN) Settings** page, select **PPPoE (ADSL)** as the WAN connection type, and the following page appears.

The screenshot shows the 'Wide Area Network (WAN) Settings' page. At the top, there are navigation tabs: 'Internet', 'Operation Mode', 'Internet', 'Wireless', and 'Firewall'. Below these are sub-tabs: 'Lan', 'Wan', 'Advanced Routing', 'DHCP', and 'QoS'. The main content area is titled 'Wide Area Network (WAN) Settings' and includes a sub-header 'WAN Setting'. The page contains the following configuration fields:

- WAN Connection Type:** A dropdown menu set to 'PPPoE (ADSL)'.
- PPPoE Mode:** A section containing:
 - User Name:** A text input field with 'pppoe_user' entered.
 - Password:** A password input field with masked characters.
 - Verify Password:** A password input field with masked characters.
 - Operation Mode:** A dropdown menu set to 'Keep Alive'. Below it, 'Keep Alive Mode: Redial Period' is set to '60' seconds, and 'On demand Mode: Idle Time' is set to '5' minutes.
- MAC Clone:** A section containing:
 - Enabled:** A dropdown menu set to 'Disable'.

At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

On this page, enter the username and the password provided by the ISP, and set the value of the **Keep Alive** mode. You can also use the default value of the **Keep Alive** mode.

After finishing the settings, click the **Apply** button to apply the settings.

- **L2TP**

If you want to use L2TP service, please select **L2TP** connection type. On the **Wide Area Network (WAN) Settings** page, select **L2TP** as the WAN connection type, and the following page appears.

The screenshot shows the 'Wide Area Network (WAN) Settings' page. At the top, there are tabs for 'Internet', 'Wireless', and 'Firewall'. Below these are sub-tabs for 'Lan', 'Wan', 'Advanced Routing', 'DHCP', and 'QoS'. The 'Wan Setting' sidebar is active. The main content area is titled 'Wide Area Network (WAN) Settings' and includes a note: 'You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.'

The 'WAN Connection Type' is set to 'L2TP'. Below this, the 'L2TP Mode' section contains the following fields:

- Server IP: 10.10.10.123
- User Name: l2tp_user
- Password: [Redacted]
- Address Mode: Static
- IP Address: 10.10.10.254
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.10.10.253
- Keep Alive: [Dropdown]
- Operation Mode: Keep Alive Mode: Redial Period 60 seconds; On demand Mode: Idle Time 5 minutes

The 'MAC Clone' section is also visible, with 'Enabled' set to 'Disable'. At the bottom, there are 'Apply' and 'Cancel' buttons.

On this page, enter the server IP, the username, and the password provided by the ISP. Set the IP address, the subnet mask, and the default gateway. When the **Address Mode** is **Dynamic**, the IP address, the subnet mask, and the default gateway of the WAN interface are automatically assigned by the DHCP server. Set the value of **Keep Alive** mode. You can also use the default value of the **Keep Alive** mode.

After finishing the settings, click the **Apply** button to apply the settings.

- **PPTP**

If you want to use PPTP service, please select **PPTP** connection type. On the **Wide Area Network (WAN) Settings** page, select **PPTP** as the WAN connection type, and the following page appears.

Internet	Operation Mode	Internet	Wireless	Firewall
		Lan Wan Advanced Routing DHCP QoS		
Wan Setting	<h3>Wide Area Network (WAN) Settings</h3> <p>You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.</p>			
	WAN Connection Type: <input type="text" value="PPTP"/>			
	PPTP Mode			
	Server IP	<input type="text" value="10.10.10.123"/>		
	User Name	<input type="text" value="pptp_user"/>		
	Password	<input type="password" value="....."/>		
	Address Mode	<input type="text" value="Static"/>		
	IP Address	<input type="text" value="10.10.10.254"/>		
	Subnet Mask	<input type="text" value="255.255.255.0"/>		
	Default Gateway	<input type="text" value="10.10.10.253"/>		
	Operation Mode	<input type="text" value="Keep Alive"/> Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds On demand Mode: Idle Time <input type="text" value="5"/> minutes		
	MAC Clone			
	Enabled	<input type="text" value="Disable"/>		
	<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>	

On this page, enter the server IP, the username, and the password provided by the ISP. Set the IP address, the subnet mask, and the default gateway. When the **Address Mode** is **Dynamic**, the IP address, the subnet mask, and the default gateway of the WAN interface are automatically assigned by the DHCP server. Set the value of **Keep Alive** mode. You can also use the default value of the **Keep Alive** mode.

After finishing the settings, click the **Apply** button to apply the settings.

5.3.3 Advanced Routing

Click **Internet > Advanced Routing** to display the **Static Routing Settings** page.

Internet | Operation Mode | **Internet** | Wireless | Firewall

| Lan | Wan | **Advanced Routing** | DHCP | QoS

Advanced Routing

Static Routing Settings

You may add and remote custom Internet routing rules, and/or enable dynamic routing exchange protocol here.

Add a routing rule

Destination	<input type="text"/>
Range	Host <input type="button" value="v"/>
Gateway	<input type="text"/>
Interface	LAN <input type="button" value="v"/> <input type="text"/>
Comment	<input type="text"/>

Current Routing table in the system:

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
2	192.168.1.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	

Dynamic Routing Settings

Dynamic Routing Protocol

RIP	Disable <input type="button" value="v"/>
-----	--

This page is used to manage the routing rules, view the routing table, and set the routing RIP function.

- **Add a Routing Rule**

Add a routing rule

Destination	<input style="width: 90%;" type="text"/>
Range	Host <input style="width: 20px;" type="button" value="v"/>
Gateway	<input style="width: 90%;" type="text"/>
Interface	LAN <input style="width: 20px;" type="button" value="v"/> <input style="width: 80%;" type="text"/>
Comment	<input style="width: 90%;" type="text"/>

The parameters for adding a routing rule are described as follows:

Field	Description
Destination	The destination address of the routing rule.
Range	You may select Host or Net .
Gateway	The IP address that the routing rule passes.
Netmask	When the range is Net , you can set this option.
Interface	The local legal interface that the routing rule passes. You may select LAN , WAN , or Custom .
Comment	Comment about the rule.

- **Current Routing Table in the System**

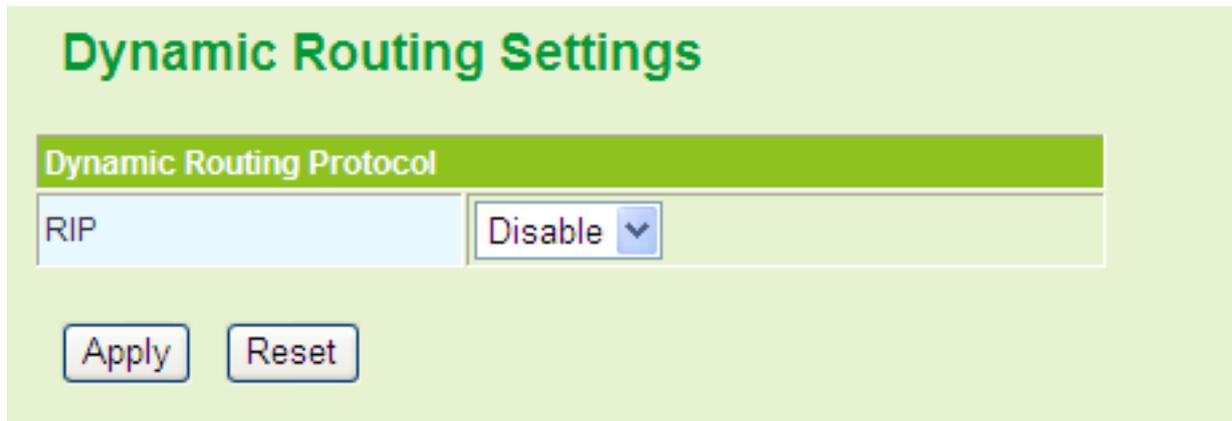
Current Routing table in the system:

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
2	192.168.1.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	

The routing table above displays the preset rules in the system. The numbers of self-defined rules are marked with . If you want to delete one rule, choose the rule

and then click the **Delete** button.

- **Dynamic Routing Settings**



You may enable or disable the RIP function (Routing Information Protocol) here. After enabling RIP function, AP can refresh its routing information and send RIP information to other devices.

5.3.4 DHCP

Click **Internet > DHCP** to display the **DHCP Client List** page.



On this page, you can view the clients' information assigned by the DHCP server, including the MAC address, the IP address, and the lease time of the IP address and so on.

5.3.5 QoS

Click **Internet > QoS** to display the **Quality of Service Settings** page.

This page is used to configure the upload bandwidth of WAN interface and QoS rules. The parameters on this page are described as follows:

Field	Description
Quality of Service	Enable or disable QoS. The default QoS setting is Disable . After enabling QoS, you may set the upload bandwidth of the WAN interface.
Upload Bandwidth	You may self-define the bandwidth, or select a proper bandwidth in the drop down list.

After enabling QoS and setting the upload bandwidth (e.g. the upload bandwidth is 128 kbps), click the **Submit** button, and the following page appears.

Internet	Operation Mode	Internet	Wireless	Firewall																						
Lan Wan Advanced Routing DHCP QoS																										
QoS Setting	<h3 style="color: #4CAF50;">Quality of Service Settings</h3> <p>You may setup rules to provide Quality of Service guarantees for specific applications.</p> <hr/> <div style="background-color: #4CAF50; color: white; padding: 2px;">QoS Setup</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 70%;">Quality of Service</td> <td>Enable</td> </tr> <tr> <td>Upload Bandwidth:</td> <td>128k Bits/sec</td> </tr> </table> <p style="text-align: center;"><input type="button" value="Submit"/></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #4CAF50; color: white;"> <th style="width: 40%;">Group</th> <th style="width: 60%;">Attribute</th> </tr> </thead> <tbody> <tr> <td>NoName5</td> <td>Rate:10% <input type="button" value="Modify"/> Ceil:100%</td> </tr> <tr> <td>NoName2</td> <td>Rate:10% <input type="button" value="Modify"/> Ceil:100%</td> </tr> <tr> <td>Default</td> <td>Rate:10% <input type="button" value="Modify"/> Ceil:100%</td> </tr> <tr> <td>NoName1</td> <td>Rate:10% <input type="button" value="Modify"/> Ceil:100%</td> </tr> </tbody> </table> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr style="background-color: #4CAF50; color: white;"> <th style="width: 10%;">No</th> <th style="width: 40%;">Name</th> <th style="width: 40%;">Group</th> <th style="width: 10%;">Info.</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input type="button" value="Add"/></td> <td colspan="3" style="text-align: center;"><input type="button" value="Delete"/></td> </tr> </tbody> </table> <p style="text-align: center; margin-top: 10px;"><input type="button" value="Load default"/></p>				Quality of Service	Enable	Upload Bandwidth:	128k Bits/sec	Group	Attribute	NoName5	Rate:10% <input type="button" value="Modify"/> Ceil:100%	NoName2	Rate:10% <input type="button" value="Modify"/> Ceil:100%	Default	Rate:10% <input type="button" value="Modify"/> Ceil:100%	NoName1	Rate:10% <input type="button" value="Modify"/> Ceil:100%	No	Name	Group	Info.	<input type="button" value="Add"/>	<input type="button" value="Delete"/>		
Quality of Service	Enable																									
Upload Bandwidth:	128k Bits/sec																									
Group	Attribute																									
NoName5	Rate:10% <input type="button" value="Modify"/> Ceil:100%																									
NoName2	Rate:10% <input type="button" value="Modify"/> Ceil:100%																									
Default	Rate:10% <input type="button" value="Modify"/> Ceil:100%																									
NoName1	Rate:10% <input type="button" value="Modify"/> Ceil:100%																									
No	Name	Group	Info.																							
<input type="button" value="Add"/>	<input type="button" value="Delete"/>																									

On this page, group table displays 4 groups of bandwidth assignment attributes. The new rule can join any group. If the new rule joins a group, it indicates that the minimum and the maximum available bandwidths of the new rule are the same as the preset values of the group that it joins.

- **Modify the Group**

Click the **Modify** button of a group in the group table (e.g. NoName5), and the following page appears.

NoName5

Group Name	<input type="text" value="NoName5"/>
Rate:	<input type="text" value="10"/> % of upload bandwidth
Ceil:	<input type="text" value="100"/> % of upload bandwidth

The parameters on this page are described as follows:

Field	Description
-------	-------------

Group Name	Display the group name. You may modify it if necessary.
Rate	When the data flow is large, this value shows that the minimum bandwidth that this group can share. Its value range is between 1 and Ceil .
Ceil	When the data flow is small, this value shows that the maximum bandwidth that this group can share. Its value is between 1 and 100.

- **Add a QoS Rule**

Click the **Add** button on the **Quality of Service Settings** page, and the following page appears.

The parameters on this page are described as follows:

Field	Description
Name	Set the rule name.
Group	Select the group that the rule belongs to.

MAC Address	The source MAC address of the rule. If data packets include the MAC address, the data packets are placed into the group.
Dest. IP address	The destination IP address of the rule. If data packets include the IP address, the data packets are placed into the group.
Src. IP address	The source IP address of the rule. If data packets include the IP address, the data packets are placed into the group.
Packet Length	The packet length of the rule. If data packets match the packet length, the data packets are placed into the group.
DSCP	The DSCP mark. If data packets include the DSCP, the data packets are placed into the group.
Protocol	The protocol types include TCP , UDP , ICMP , and Application . If data packets match the protocol, the data packets are placed into the group. When selecting TCP or UDP , you need to set Src Port and Src Port Range . When selecting Application , you may select a proper protocol in the drop down list.
Remark DSCP as	If data packets match the parameters above, you can determine whether to remark DSCP. The default setting is Auto .

After finishing the settings, click the **Add** button to add the new rule.

- **Delete a QoS Rule**

If there are QoS rules in the QoS rule table, and you want to delete a QoS rule, you can select the rule, and then click the **Delete** button to delete this rule.



- **Load Default Settings**

Click the **Load Default** button on the **Quality of Service Settings** page, system will load the default QoS rules. See the following figure:

Internet | Operation Mode | **Internet** | Wireless | Firewall | Administration | Logout

| Lan | Wan | Advanced Routing | DHCP | QoS

QoS Setting

Quality of Service Settings

You may setup rules to provide Quality of Service guarantees for specific applications.

QoS Setup

Quality of Service: Enable

Upload Bandwidth: 128k Bits/sec

Group	Attribute
High	Rate:30% <input type="button" value="Modify"/> Cell:100%
Middle	Rate:20% <input type="button" value="Modify"/> Cell:100%
Default	Rate:5% <input type="button" value="Modify"/> Cell:100%
Low	Rate:10% <input type="button" value="Modify"/> Cell:100%

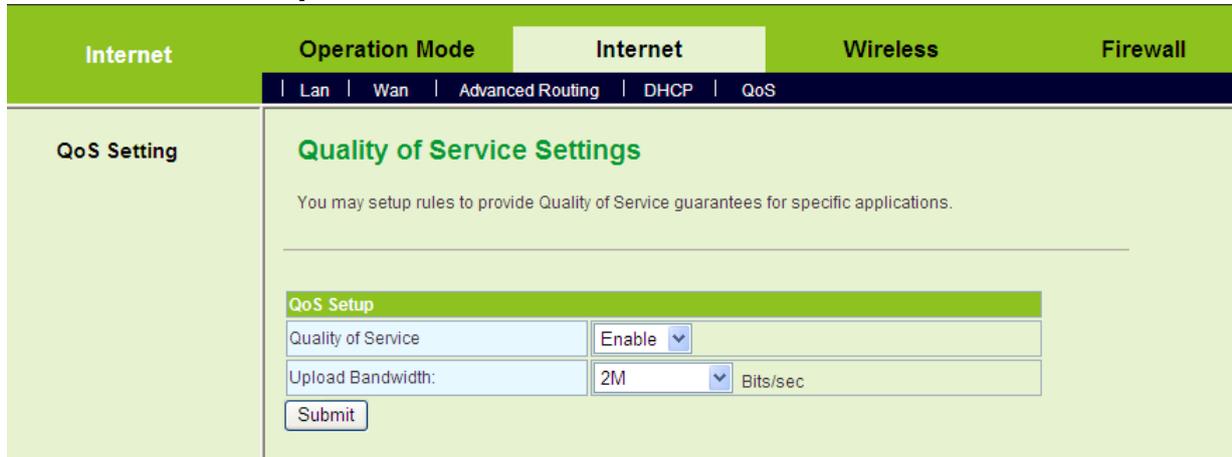
No	Name	Group	Info.
1 <input type="checkbox"/>	ICMP_HIGH	High	Protocol: ICMP Remark DSCP :EF
2 <input type="checkbox"/>	Small_Packet_HIGH	High	Packet Length: 0 - 128 Remark DSCP :EF
3 <input type="checkbox"/>	VoIP_H323_HIGH	High	Protocol: Application Application: h323 Remark DSCP :EF
4 <input type="checkbox"/>	VoIP_SIP_HIGH	High	Protocol: Application Application: sip Remark DSCP :EF
5 <input type="checkbox"/>	VoIP_Skype1_HIGH	High	Protocol: Application Application: skypeout Remark DSCP :EF
6 <input type="checkbox"/>	VoIP_Skype2_HIGH	High	Protocol: Application Application: skypetoskype Remark DSCP :EF
7 <input type="checkbox"/>	RTP_HIGH	High	Protocol: Application Application: rtp Remark DSCP :EF
8 <input type="checkbox"/>	SSH_HIGH	High	Protocol: Application Application: ssh Remark DSCP :EF
9 <input type="checkbox"/>	MSN_Messenger_MIDDLE	Middle	Protocol: Application Application: msnmessenger Remark DSCP :AF21
10 <input type="checkbox"/>	Yahoo_MIDDLE	Middle	Protocol: Application Application: yahoo Remark DSCP :AF21
11 <input type="checkbox"/>	PoP3_LOW	Low	Protocol: Application Application: msnmessenger Remark DSCP :AF11
12 <input type="checkbox"/>	SMTP_LOW	Low	Protocol: Application Application: smtp Remark DSCP :AF11
13 <input type="checkbox"/>	P2P_eMule_LOW	Low	Protocol: Application Application: edonkey Remark DSCP :AF11
14 <input type="checkbox"/>	P2P_BT_LOW	Low	Protocol: Application Application: bittorrent Remark DSCP :AF11

After loading the default rules, the four groups are redefined as **High**, **Middle**, **Default**, and **Low**, and the minimum bandwidth values of the corresponding groups are changed as 30%, 20%, 5%, and 10%. You can also delete the default rules if

necessary.

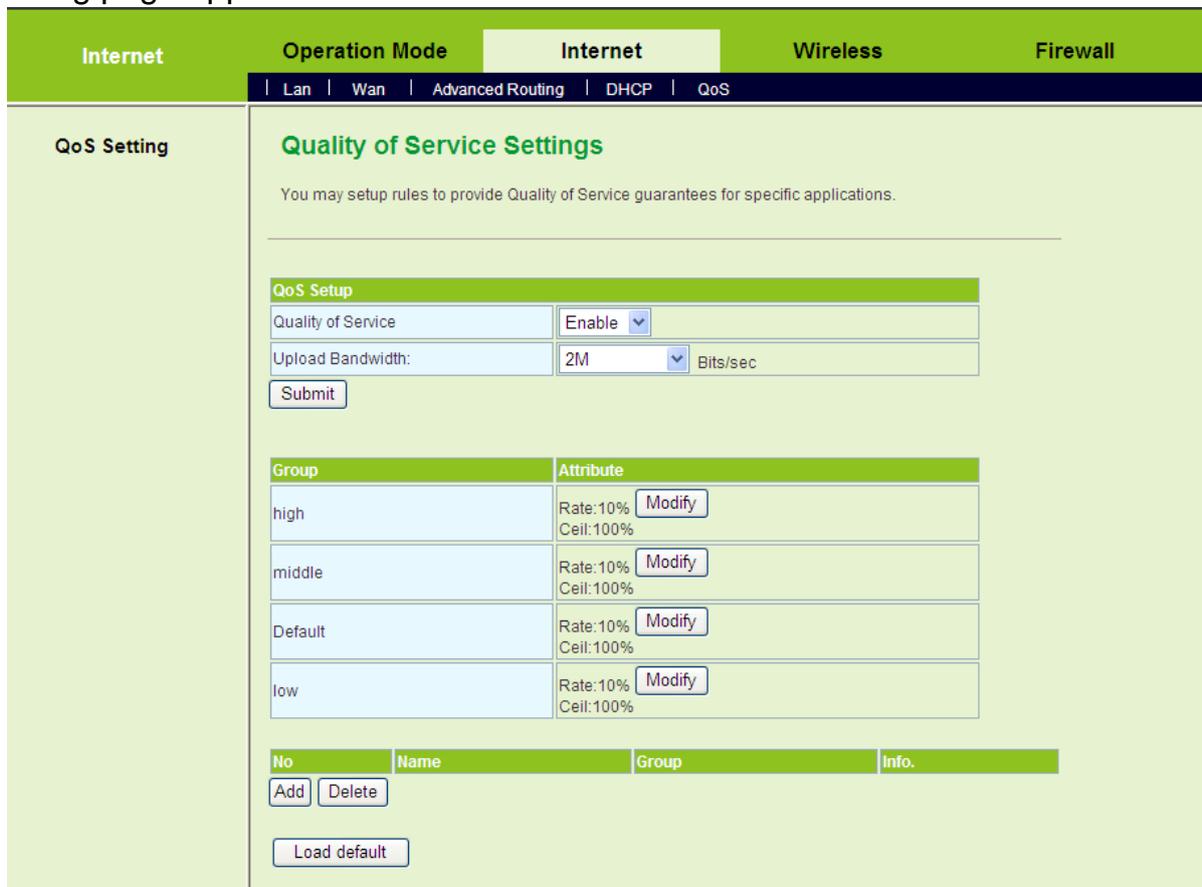
- **The examples of QoS Settings**

- **Set the Upload Bandwidth**



On the **Quality of Service Settings** page, enable the QoS, and set the upload bandwidth. For example, set the value of upload bandwidth to be 2Mbps.

After finishing the settings, click the **Submit** button to submit the settings and the following page appears.



- **Modify a Group Attribute**

After enabling QoS, system establishes 4 groups. Click the **Modify** button of the corresponding group, and you can modify the attribute settings of the corresponding group. Let's take **High** group as an example.

high	
Group Name	high
Rate:	30 % of upload bandwidth
Ceil:	100 % of upload bandwidth
<input type="button" value="Modify"/>	

On this page, set the **Rate** value to be 30. If the upload bandwidth is 2Mbps, when the data flow is large, it indicates that the minimum bandwidth that **High** group can share is 30% of the total bandwidth, that is, 06 Mbps. When the data flow is little, the maximum bandwidth that **High** group can share is 100% of the total bandwidth, that is, 2Mbps.

- **Add a QoS Rule**

Click the **Add** button on the **Quality of Service Settings** page to display the **Classifier Settings** page.

Classifier Settings	
Name	Example1
Group	High
MAC Address	
Dest. IP address	
Src. IP address	
Packet Length	- (ex: 0-128 for small packets)
DSCP	
Protocol	ICMP
Remark DSCP as:	Auto
<input type="button" value="Add"/>	

On this page, you can add a QoS group. For example, set the name to be Example1, add it to the High group, and select the ICMP protocol.

After finishing the settings, click the **Add** button and the following page appears.

No	Name	Group	Info.
1 <input type="checkbox"/>	Example1	High	Protocol: ICMP Remark DSCP :EF
<input type="button" value="Add"/> <input type="button" value="Delete"/>			

- **About DSCP**

DSCP consists of 6 bits of IP packet header. It uses ToS field. This byte is also called DSCP byte. Its position among the byte is as follows:

DS5 DS4 DS3 DS2 DS1 DS0 CU CU

DSCP priority: 6 bits (DS5-DS0)

Unused (CU): 2 bits

The values of DSCP priority are 64 (0~63). 0 is the lowest priority level, and the 63 is the highest priority level. In fact, DSCP field is the superset of the IP priority field. DSCP field is backward compatible with the IP priority. At present, the defined default DSCP is 0. Class selector DSCP is backward compatible with the IP priority. The values are 8, 16, 24, 32, 40, 48, and 56. Usually, EF (Expedited Forwarding) is used for low delay service and the recommended value is 46 (101110). AF (assured forwarding) defines 4 service levels, and each service level includes three descending levels. The following table shows the concrete values as follows:

Service level priority	Type 1	Type 2	Type 3	Type 4
Low discarding priority	AF11 = 10	AF21 = 18	AF31 = 26	AF41 = 34
Medium discarding priority	AF12 = 12	AF22 = 20	AF32 = 28	AF42 = 36
High discarding priority	AF13 = 14	AF23 = 22	AF33 = 30	AF43 = 38

5.4 Wireless Settings (Gateway Mode)

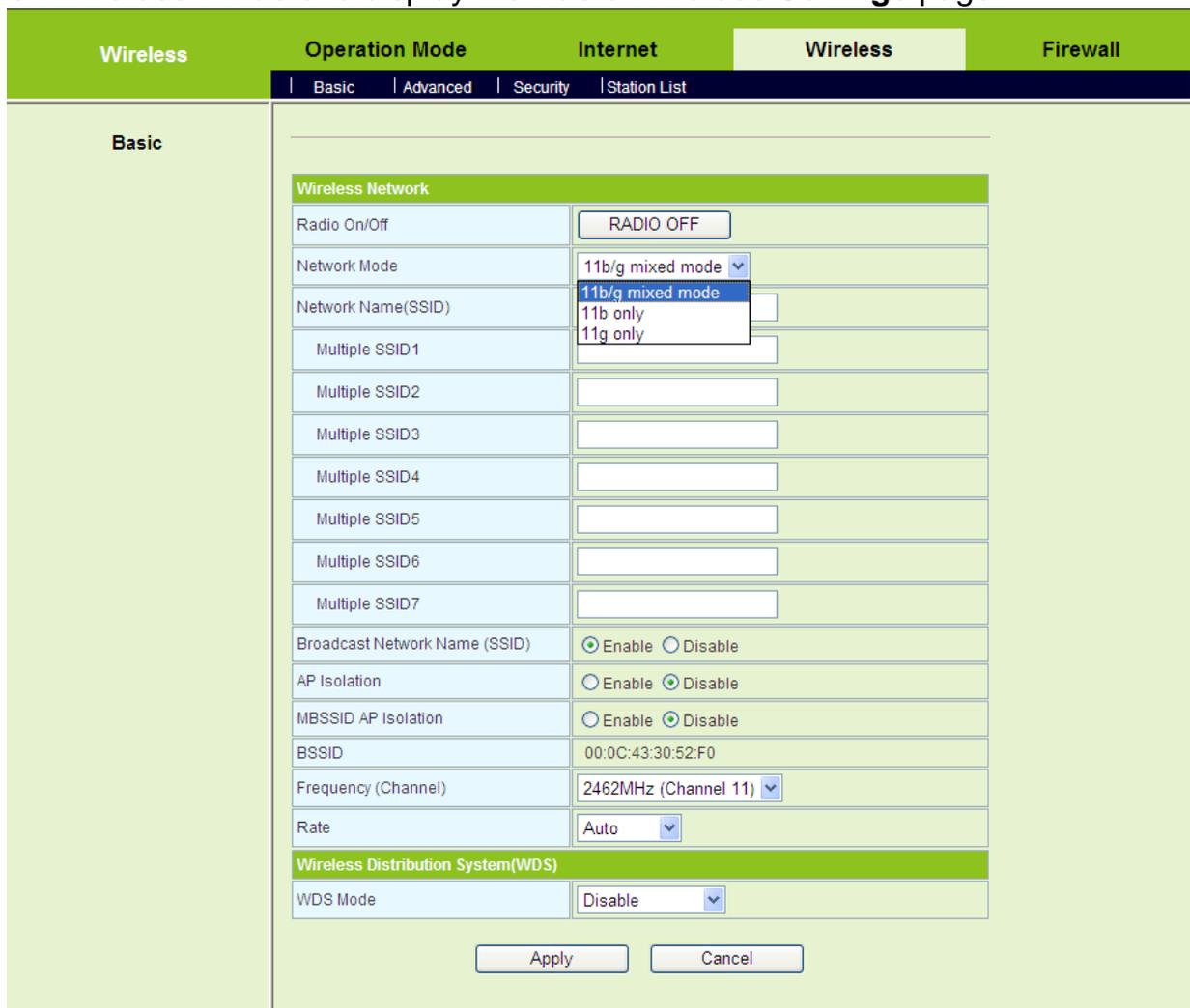
In the gateway mode, the following figure shows the navigation menu of the **Wireless**:



In the gateway mode, the sub-menus of the **Wireless Settings** include **Basic**, **Advanced**, **Security**, and **Station List**.

5.4.1 Basic

Click **Wireless > Basic** to display the **Basic Wireless Settings** page.



On this page, you may set the parameters of wireless network, and WDS.

- **Wireless Network**

The parameters of **Wireless Network** are described as follows:

Field	Description
-------	-------------

Field	Description
Radio On/Off	Enable or disable wireless LAN interface.
Network Mode	You may select a proper network mode in the drop down list. <ul style="list-style-type: none"> ● 11b/g mixed mode ● 11b only ● 11g only
Network Name (SSID)	The maximum character number for SSID is 32 characters. The legal characters include letter, number, underline or the combination of these characters.
Multiple SSID1~7	Accessional network SSID. Each SSID can use wireless security setting independently.
Broadcast Network Name (SSID)	Whether to broadcast SSID. After enabling this function, AP will broadcast its SSID.
AP Isolation	Enable or disable the isolation among AP clients. After enabling this function, the client terminals that connect to the same AP can not communicate each other.
MBSSID AP Isolation	Enable or disable the isolation among different SSIDs. After enabling this function, the client terminals with different SSIDs can not communicate each other.
BSSID	The MAC address of the wireless interface.
Frequency(Channel)	You may select a proper channel in the drop down list. The default channel is Channel 11.
Rate	Select a proper rate in the drop down list.

- **Wireless Distribution System (WDS)**

WDS modes include **Lazy Mode**, **Bridge Mode**, and **Repeater Mode**. You can also enable WDS.

- **Lazy Mode**

Wireless Distribution System(WDS)	
WDS Mode	Lazy Mode ▾
Phy Mode	CCK ▾
EncrypType	WEP ▾
Encryp Key	<input type="text"/>

The parameters of **Lazy Mode** are described as follows:

Field	Description
WDS Mode	Select the Lazy Mode in the drop down list.
Phy Mode	The physical modes in the drop down list include CCK , and OFDM .
Encryp Type	The encryption types you can select include NONE , WEP , TKIP , and AES . If selecting WEP , TKIP , or AES , you need to set the encryption key.
Encryp Key	Set the encryption key.

- Bridge Mode

Wireless Distribution System(WDS)	
WDS Mode	Bridge Mode ▾
Phy Mode	OFDM ▾
EncrypType	WEP ▾
Encryp Key	<input type="text"/>
AP MAC Address	<input type="text"/>

The parameters of **Bridge Mode** are described as follows:

Field	Description
WDS Mode	Select the Bridge Mode .

Field	Description
Phy Mode	The physical modes in the drop down list include CCK , and OFDM .
Encryp Type	The encryption types you can select include NONE , WEP , TKIP , and AES . If selecting WEP , TKIP , or AES , you need to set the encryption key.
Encryp Key	Set the encryption key.
AP MAC Address	The MAC address of another AP that connects to the GR-124W by WDS.

- Repeater Mode

Wireless Distribution System(WDS)	
WDS Mode	Repeater Mode <input type="button" value="v"/>
Phy Mode	CCK <input type="button" value="v"/>
EncrypType	NONE <input type="button" value="v"/>
AP MAC Address	<input type="text"/>

The parameters' description of **Repeater Mode**, please refer to the **Bridge Mode**.

5.4.2 Advanced Settings

Click **Wireless > Advanced** to display the **Advanced Wireless Settings** page.

Wireless	Operation Mode	Internet	Wireless	Firewall	Administration																						
	Basic	Advanced	Security	Station List																							
Advanced	<h3>Advanced Wireless Settings</h3> <p>Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.</p>																										
<h4>Advanced Wireless</h4> <table border="1"> <tr> <td>BG Protection Mode</td> <td>Auto</td> </tr> <tr> <td>Beacon Interval</td> <td>100 ms (range 20 - 999, default 100)</td> </tr> <tr> <td>Data Beacon Rate (DTIM)</td> <td>1 ms (range 1 - 255, default 1)</td> </tr> <tr> <td>Fragment Threshold</td> <td>2346 (range 256 - 2346, default 2346)</td> </tr> <tr> <td>RTS Threshold</td> <td>2347 (range 1 - 2347, default 2347)</td> </tr> <tr> <td>TX Power</td> <td>50 (range 1 - 100, default 100)</td> </tr> <tr> <td>Short Preamble</td> <td><input type="radio"/> Enable <input checked="" type="radio"/> Disable</td> </tr> <tr> <td>Short Slot</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>Tx Burst</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>Pkt_Aggregate</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>Country Code</td> <td>US (1-11)</td> </tr> </table>						BG Protection Mode	Auto	Beacon Interval	100 ms (range 20 - 999, default 100)	Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)	Fragment Threshold	2346 (range 256 - 2346, default 2346)	RTS Threshold	2347 (range 1 - 2347, default 2347)	TX Power	50 (range 1 - 100, default 100)	Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Country Code	US (1-11)
BG Protection Mode	Auto																										
Beacon Interval	100 ms (range 20 - 999, default 100)																										
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)																										
Fragment Threshold	2346 (range 256 - 2346, default 2346)																										
RTS Threshold	2347 (range 1 - 2347, default 2347)																										
TX Power	50 (range 1 - 100, default 100)																										
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																										
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																										
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																										
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																										
Country Code	US (1-11)																										
<h4>Wi-Fi Multimedia</h4> <table border="1"> <tr> <td>WMM Capable</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>APSD Capable</td> <td><input type="radio"/> Enable <input checked="" type="radio"/> Disable</td> </tr> <tr> <td>DLS Capable</td> <td><input type="radio"/> Enable <input checked="" type="radio"/> Disable</td> </tr> <tr> <td>WMM Parameters</td> <td>WMM Configuration</td> </tr> </table>						WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	WMM Parameters	WMM Configuration														
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																										
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																										
DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																										
WMM Parameters	WMM Configuration																										
<h4>Multicast-to-Unicast Converter</h4> <table border="1"> <tr> <td>Multicast-to-Unicast</td> <td><input type="radio"/> Enable <input checked="" type="radio"/> Disable</td> </tr> </table>						Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																				
Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																										
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>																											

On this page, you may configure advanced wireless parameters, such as beacon interval, data beacon rate, and Tx power.

Note:

The advanced wireless setting is only for advanced user. For the common user, do not change any setting on this page.

- **Advanced Wireless**

Advanced Wireless	
BG Protection Mode	Auto <input type="button" value="v"/>
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	50 (range 1 - 100, default 100)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Country Code	US (1-11) <input type="button" value="v"/>

The parameters of **Advanced Wireless** are described as follows:

Field	Description
BG Protection Mode	You may select On , Off , or Auto . The default BG protection mode is Auto .
Beacon Interval	By default, wireless beacon signal sends data to station every other 100 ms. The range is 20~999.
Data Beacon Rate (DTIM)	The default DTIM is 1ms. The range is 1~255.
Fragment Threshold	The default fragment threshold is 2346. The range is 256~2346.
RTS Threshold	The default RTS threshold is 2347. The range is 1~2347.
TX Power	Set the Tx power. 100% indicates full power.
Short Preamble	Enable or disable short preamble. The default setting is Disable . Preamble defines the length of CRC correction block for wireless devices. Short preamble adopts 56-bit synchronization field. The network whose

Field	Description
	network traffic is dense should use shorter preambles. Short Preamble is mainly applied to the efficiency improvement of real- time applications, such as streaming video, and Voice-Over-IP telephony.
Short Slot	Enable or disable short slot.
Tx Burst	Tx Burst can be used to improve the efficiency of data transmission. It can make system transmit more data during a period of time.
Pkt_Aggregate	Pkt_Aggregate can aggregate multiple data packets together for improving the transmission efficiency.
Country Code	Select a proper country code in the drop down list.

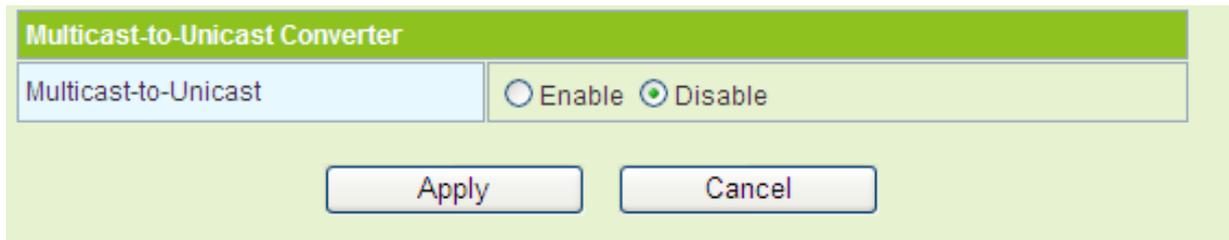
● Wi-Fi Multimedia

Wi-Fi Multimedia	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Parameters	<input type="button" value="WMM Configuration"/>

The parameters of WMM are described as follows:

Field	Description
Wi-Fi Capable	Enable or disable WMM. After enabling WMM, AP can process different types of wireless data according to their priority levels.
APSD Capable	Enable or disable APSD. After enabling APSD, it can decrease the consumption of the power supply device.
DLS Capable	Enable or disable DLS.
WMM Parameters	Click the WMM Configuration button to display the configuration page of WMM parameters.

- **Multicast-to-Unicast Converter**



Enable or disable **Multicast-to-Unicast**. After enabling this function, the transmission quality of wireless multicast stream can be improved.

- **About WMM**

- **WMM Access Categories**

At present, WMM defines traffic into 4 access categories.

Access Category	Description	802.1d Tags
WMM Voice Priority	Highest priority Allows multiple concurrent VoIP calls, with low latency and toll voice quality	7, 6
WMM Video Priority	Prioritize video traffic above other data traffic One 802.11g or 802.11a channel can support 3-4 SDTV streams or 1 HDTV streams	5, 4
WMM Best Effort Priority	Traffic from legacy devices, or traffic from applications or devices that lack QoS capabilities Traffic less sensitive to latency, but affected by long delays, such as Internet surfing	0, 3
WMM Background Priority	Low priority traffic (file downloads, print jobs) that does not have strict latency and throughput requirements	2, 1

AC_VO: Voice (highest priority)

AC_VI: Video (high priority)

AC_BE: Best effort (medium priority)

AC_BK: Background (low priority)

802.11 uses DCF (Distributed Coordination Function) scheme of the CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) protocol to reduce the chances of packets collision while one more devices access the wireless media at the same time. A client wishing to transmit has to first listen to the channel for a predetermined amount of time so as to check for any activity on the channel. If the channel is sensed "idle" then the client is permitted to transmit. If the channel is sensed as "busy" the station has to defer its transmission. The random interval provides a fair transmission chance for all the devices.

When each priority queue waits for sending packets, it has to wait a fixed time AIFSN and a random time CW. They define time values by multiple time slots. For 802.11b, its time slot is 20ms. The time slot of 802.11a and 802.11g is 9 ms. CW insures the random delay time of DCF, so that the packets collision among the devices with the same access category can be avoided. If collision occurs, CW is doubled until it exceeds its maximum value. After every successful transmission, CW returns to the minimum value.

The priority queue that succeeds in the competition of sending packets will acquire Txop time to send packets. If the txop value is 0, it is limited to be a MSDC (MAC Service Data Unit).

- **Set WMM Parameters**

Click the **WMM Configuration** button on the **Advanced Wireless Settings** page, the following page appears.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

On this page, you can configure the WMM parameters of access point and station.

Note:

GR-124W provides standard WMM settings. If you want to modify the parameters above, please refer to the WMM settings of your WMM products.

The parameters on this page are described as follows:

Field	Description
Aifsn	Aifsn (Arbitrary Inter-Frame Space Number). This parameter influences the delay time of WMM access category. If you use voice or video service, you'd better set this parameter to be smaller in the fields of AC_VI and AC_VO. If it is E-mail or Web service, you should set a bigger value in the fields of AC_BE and AC_BK.
Cwmin	Cwmin (Mini. Contention Window) also influences the delay time of WMM access category. The difference between AC_VI and AC_VO should be smaller, but the difference between AC_BE and AC_BK should be bigger.
Cwmax	Cwmax (Max. Contention Window)
Txop	Txop (Opportunity to Transmit) may optimize the WMM access. Compared to the WMM access that needs a higher priority, such as AC_VI and AC_VO, this value should be bigger.
ACM	ACM (Admission Control Mandatory) parameter only reacts on AC_VI and AC_VO. If you set this value to be 0, it indicates that AP is in the charge of the access commands. If this value is 1, it means the client is in the charge of the access commands.
Ackpolicy	When WMM packets are transmitting, AP will receive an echo request. If you set this value is 0, it means AP does not send back an echo request, which will bring positive effect for WMM. If this value is 1, AP generates the response to the request.

- **DLS (Direct Link Setup)**

GR-124W provides DLS function. Suppose that there are two WMM devices. Enter the MAC address of a WMM device in the DLS setting of the other device, and then connect the two WMM devices to the GR-124W. In this way, these two WMM devices can transmit message directly.

If you want to configure WMM DLS, do as follows:

Step1 Prepare two wireless network cards (A and B) and one GR-124W.

Step2 Enable the DLS function on the **Advanced Wireless Settings** page.

Wi-Fi Multimedia	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DLS Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM Parameters	<input type="button" value="WMM Configuration"/>

Step3 Enable the DLS function of wireless network cards. Enter the MAC address of wireless card A on the **WMM** page of the wireless network card B, and then click the **Apply** button.

The screenshot shows the RaUI WMM Setup Status page. The 'WMM Setup Status' section displays 'WMM >> Enabled', 'Power Save >> Disabled', and 'Direct Link >> Enabled'. Below this, the 'WMM Enable' checkbox is checked and highlighted with a red box. Underneath, 'WMM - Power Save Enable' is unchecked, with sub-options 'AC_BK', 'AC_BE', 'AC_VI', and 'AC_VO' also unchecked. The 'Direct Link Setup Enable' checkbox is checked and highlighted with a red box. Below it, the 'MAC Address' field is populated with '00 18 6e 39 ca 81' and highlighted with a red box. The 'Timeout Value' is set to '60 sec'. At the bottom right, the 'Apply' button is highlighted with a red box, and the 'Tear Down' button is visible below it.

Step4 If DLS succeeds, you can view the MAC address of wireless card A on the **WMM** page of wireless card B, and vice versa.

This screenshot shows the RaUI WMM Setup Status page after configuration. The 'WMM Setup Status' section remains the same. The 'WMM Enable' checkbox is checked. The 'Direct Link Setup Enable' checkbox is checked. The 'MAC Address' field is now populated with '00 18 6e 39 ca 81' and highlighted with a red box. Below this, a table displays the MAC address '00-1E-E3-00-61-8A' and the '60' timeout value, both highlighted with a red box. The 'Apply' and 'Tear Down' buttons are visible at the bottom right.

5.4.3 Security

Click **Wireless > Security** to display the **Wireless Security/Encryption Settings** page.

Wireless | **Operation Mode** | **Internet** | **Wireless** | **Firewall** | **Administration**

Basic | Advanced | **Security** | Station List

Security

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID

SSID choice: Getnet

"Getnet"

Security Mode: Disable

Access Policy

Policy: Disable

Add a station Mac:

Apply Cancel

This page allows you to configure wireless security modes and set the encryption keys, to prevent unauthorized access and monitoring.

- **Select SSID**

Select SSID

SSID choice: Getnet

SSID choice: select SSID that you want to configure.

- **Security Mode**

This page provides 10 types of security modes, including OPEN, SHARED, WPAUTO, WPA-Enterprise, WPA-PSK, WPA2-Enterprise, WPA2-PSK, WPA-PSK/WPA2PSK, WPA1/WPA2-Enterprise, and Dynamic WEP 8021.X.

- **OPEN**

Select SSID	
SSID choice	Getnet ▾
"Getnet"	
Security Mode	Open ▾
Wire Equivalence Protection (WEP)	
Default Key	Key 1 ▾
WEP Keys	WEP Key 1 : <input type="text"/> Hex ▾
	WEP Key 2 : <input type="text"/> Hex ▾
	WEP Key 3 : <input type="text"/> Hex ▾
	WEP Key 4 : <input type="text"/> Hex ▾

The parameters of **OPEN** mode are described as follows:

Field	Description
Security Mode	Select OPEN .
Default Key	Select a key as the default key.
WEP Keys WEP Key (1/2/3/4)	Set 64-bit or 128-bit key. The key format is Hex or ASCII .

- **SHARED**

Select SSID	
SSID choice	Getnet ▼
"Getnet"	
Security Mode	Shared ▼
Encrypt Type	WEP ▼
Wire Equivalence Protection (WEP)	
Default Key	Key 1 ▼
WEP Keys	WEP Key 1 : <input type="text"/> Hex ▼
	WEP Key 2 : <input type="text"/> Hex ▼
	WEP Key 3 : <input type="text"/> Hex ▼
	WEP Key 4 : <input type="text"/> Hex ▼

The parameters of **SHARED** mode are described as follows:

Field	Description
Security Mode	Select SHARED .
Encrypt Type	Only WEP is provided.
Default Key	Select a key as the default key.
WEP Keys (WEP Key1/2/3/4)	Set 64-bit or 128-bit key. The key format is Hex or ASCII .

- **WEPAUTO**

Select SSID			
SSID choice	Getnet ▼		
"Getnet"			
Security Mode	WEPAUTO ▼		
Wire Equivalence Protection (WEP)			
Default Key	Key 1 ▼		
WEP Keys	WEP Key 1 :	<input type="text"/>	Hex ▼
	WEP Key 2 :	<input type="text"/>	Hex ▼
	WEP Key 3 :	<input type="text"/>	Hex ▼
	WEP Key 4 :	<input type="text"/>	Hex ▼

The parameters' description of **WEPAUTO** mode, please refer to **OPEN** mode.

- **WPA-Enterprise**

Select SSID	
SSID choice	Getnet ▼
"Getnet"	
Security Mode	WPA-Enterprise ▼
WPA	
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIP+AES
Key Renewal Interval	<input type="text" value="3600"/> seconds
Radius Server	
IP Address	<input type="text"/>
Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="0"/>
Idle Timeout	<input type="text"/>

The parameters of **WPA-Enterprise** mode are described as follows:

Field	Description
Security Mode	Select WPA-Enterprise .
WPA Algorithms	You may select TKIP or AES .
Key Renewal Interval	Set the key renewal interval.
IP Address	The IP address of RADIUS server.
Port	The default port number is 1812. You may change it according to the server setting.
Shared Secret	The shared key that RADIUS server needs to authenticate.
Session Timeout	If this value is 0, it indicates that there is no session time limit.
Idle Timeout	Set the idle timeout.

- WPA-PSK

The screenshot shows a configuration interface for WPA-PSK. The 'Security Mode' is set to 'WPA-PSK'. Under the 'WPA' section, the 'WPA Algorithms' are set to 'TKIP', 'AES', and 'TKIP+AES'. The 'Pass Phrase' is '12345678'. The 'Key Renewal Interval' is '3600' seconds.

The parameters of **WPA-PSK** mode are described as follows:

Field	Description
Security Mode	Select WPA-PSK .
WPA Algorithms	Select TKIP or AES .
Pass Phrase	Set 8-bit to 64-bit key.

Field	Description
Key Renewal Interval	Set the key renewal interval.

- WPA2-Enterprise

"Getnet"

Security Mode	WPA2-Enterprise ▼
---------------	-------------------

WPA

WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIP+AES
Key Renewal Interval	<input type="text" value="3600"/> seconds
PMK Cache Period	<input type="text" value="10"/> minute
Pre-Authentication	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Radius Server

IP Address	<input type="text"/>
Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="0"/>
Idle Timeout	<input type="text"/>

The parameters of **WPA2-Enterprise** are described as follows:

Field	Description
Security Mode	Select WPA2-Enterprise .
WPA Algorithms	You may select TKIP , AES , or TKIP + AES .
Key Renewal Interval	Set the key renewal interval.
PMK Cache Period	Set the PMK (Pairwise Master Key) cache period. PMK scheme allows the roaming users that pass through the 802.11X/EAP handshake protocol roam to the previous AP again. PMK can decrease the

Field	Description
	roaming delay and improve the roaming speed.
Pre-Authentication	Enable or disable pre-authentication.
IP Address	The IP address of RADIUS server.
Port	The default port number is 1812. You may change it according to the server setting.
Shared Secret	The shared key that RADIUS server needs to authenticate.
Session Timeout	If this value is 0, it indicates that there is no session time limit.
Idle Timeout	Set the idle timeout.

- WPA2-PSK

"Getnet"

Security Mode	<input type="text" value="WPA2-PSK"/>
---------------	---------------------------------------

WPA

WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIP+AES
Pass Phrase	<input type="text" value="12345678"/>
Key Renewal Interval	<input type="text" value="3600"/> seconds

The parameters of **WPA2-PSK** mode are described as follows:

Field	Description
Security Mode	Select WPA2-PSK .
WPA Algorithms	You may select TKIP , AES , or TKIP + AES .
Pass Phrase	Set 8-bit to 64-bit key.
Key Renewal Interval	Set the key renewal interval.

- WPA-PSK/WPA2-PSK

"Getnet"	
Security Mode	WPA-PSK/WPA2-PSK ▼
WPA	
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIP+AES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds

The parameters' description of **WPA-PSK/WPA2-PSK** mode, please refer to **WPA2-PSK**.

- **WPA1/WPA2-Enterprise**

"Getnet"	
Security Mode	WPA1/WPA2-Enterprise ▼
WPA	
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIP+AES
Key Renewal Interval	3600 seconds
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	

The parameters of **WPA1/WPA2-Enterprise** are described as follows:

Field	Description
Security Mode	Select WPA1/WPA2-Enterprise .
WPA Algorithms	You may select TKIP , AES , or TKIP + AES .
Key Renewal Interval	Set the key renewal interval.

Field	Description
IP Address	The IP address of RADIUS server.
Port	The default port number is 1812. You may change it according to the server setting.
Shared Secret	The shared key that RADIUS server needs to authenticate.
Session Timeout	If this value is 0, it indicates that there is no session time limit.
Idle Timeout	Set the idle timeout.

- Dynamic WEP 802.1X

"Getnet"

Security Mode	Dynamic WEP 802.1X ▼
Radius Server	
IP Address	<input type="text"/>
Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="0"/>
Idle Timeout	<input type="text"/>

The parameters of **Dynamic WEP 802.1X** mode are described as follows:

Field	Description
Security Mode	Select Dynamic WEP 802.1X .
IP Address	The IP address of RADIUS server.
Port	The default port number is 1812. You may change it according to the server setting.
Shared Secret	The shared key that RADIUS server needs to authenticate.
Session Timeout	If this value is 0, it indicates that there is no session time limit.
Idle Timeout	Set the idle timeout.

- **Access Policy**

The parameters of **Access Policy** are described as follows:

Field	Description
Policy	<p>Disable: Stop the access control to the wireless devices in the MAC list.</p> <p>Allow: Allow the access control to the wireless devices in the MAC list.</p> <p>Reject: Reject the access control to the wireless devices in the MAC list.</p>
Add a station Mac	Enter the MAC address of wireless device that you want to allow or reject.

After finishing the settings, click the **Apply** button to apply the settings.

5.4.4 Station List

Click **Wireless > Station List** to display the **Station List** page.

On this page, you can view the wireless networks that connect to the GR-124W. If there is any wireless network connects to GR-124W, refresh this page and the

connection information of the wireless network is displayed. See the following figure:

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
00:21:27:0D:61:C7	1	0	0	7	20M	0	0

5.4.5 Wireless WDS Setting

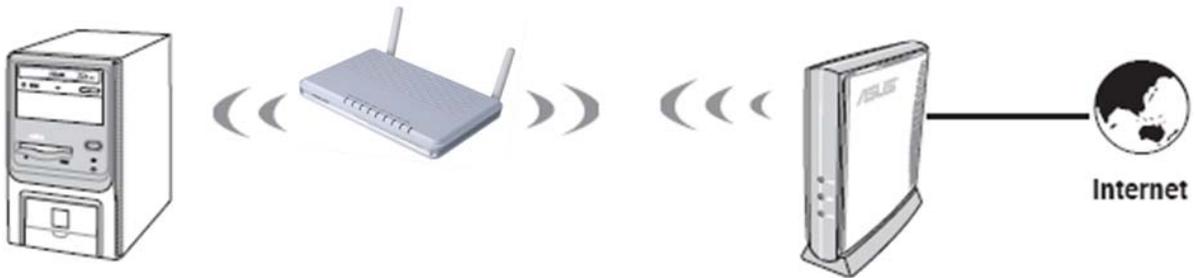
The WDS modes of the GR-124W include **Repeater** mode, **Bridge** mode, and **Lazy** mode.

Note:

For better compatibility, please try to adopt the products with the same model to connect to the GR-124W.

- **WDS Repeater Mode**

In the Repeater mode, you can use the GR-124W to connect to the primary router, for extending the wireless coverage.



Step1 Click **Wireless > Basic** to display the **Basic Wireless Settings** page.

Wireless		Operation Mode	Internet	Wireless	Firewall																																						
Basic		Basic	Advanced	Security	Station List																																						
<h3>Basic Wireless Settings</h3> <p>You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.</p>																																											
<table border="1"> <thead> <tr> <th colspan="2">Wireless Network</th> </tr> </thead> <tbody> <tr> <td>Radio On/Off</td> <td>RADIO OFF</td> </tr> <tr> <td>Network Mode</td> <td>11b/g mixed mode</td> </tr> <tr> <td>Network Name(SSID)</td> <td>Getnet</td> </tr> <tr> <td>Multiple SSID1</td> <td></td> </tr> <tr> <td>Multiple SSID2</td> <td></td> </tr> <tr> <td>Multiple SSID3</td> <td></td> </tr> <tr> <td>Multiple SSID4</td> <td></td> </tr> <tr> <td>Multiple SSID5</td> <td></td> </tr> <tr> <td>Multiple SSID6</td> <td></td> </tr> <tr> <td>Multiple SSID7</td> <td></td> </tr> <tr> <td>Broadcast Network Name (SSID)</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>AP Isolation</td> <td><input type="radio"/> Enable <input checked="" type="radio"/> Disable</td> </tr> <tr> <td>MBSSID AP Isolation</td> <td><input type="radio"/> Enable <input checked="" type="radio"/> Disable</td> </tr> <tr> <td>BSSID</td> <td>00:0C:43:30:52:F0</td> </tr> <tr> <td>Frequency (Channel)</td> <td>2462MHz (Channel 11)</td> </tr> <tr> <td>Rate</td> <td>Auto</td> </tr> <tr> <th colspan="2">Wireless Distribution System(WDS)</th> </tr> <tr> <td>WDS Mode</td> <td>Disable</td> </tr> </tbody> </table>						Wireless Network		Radio On/Off	RADIO OFF	Network Mode	11b/g mixed mode	Network Name(SSID)	Getnet	Multiple SSID1		Multiple SSID2		Multiple SSID3		Multiple SSID4		Multiple SSID5		Multiple SSID6		Multiple SSID7		Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	BSSID	00:0C:43:30:52:F0	Frequency (Channel)	2462MHz (Channel 11)	Rate	Auto	Wireless Distribution System(WDS)		WDS Mode	Disable
Wireless Network																																											
Radio On/Off	RADIO OFF																																										
Network Mode	11b/g mixed mode																																										
Network Name(SSID)	Getnet																																										
Multiple SSID1																																											
Multiple SSID2																																											
Multiple SSID3																																											
Multiple SSID4																																											
Multiple SSID5																																											
Multiple SSID6																																											
Multiple SSID7																																											
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																																										
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																																										
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																																										
BSSID	00:0C:43:30:52:F0																																										
Frequency (Channel)	2462MHz (Channel 11)																																										
Rate	Auto																																										
Wireless Distribution System(WDS)																																											
WDS Mode	Disable																																										
<p style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p>																																											

- Step2** On this page, set the AP channel to accord with the peer AP (An AP that wants to connect to the GR-124W by WDS).
- Step3** On the **Basic Wireless Settings** page, set the WDS mode to be **Repeater Mode**, set the physical mode and the encryption type of AP to accord with that of peer AP, and then enter the MAC address of the peer AP. After finishing the settings, click the **Apply** button to apply the settings. The GR-124W will work in the **Repeater Mode**.

Wireless Distribution System(WDS)	
WDS Mode	Repeater Mode ▾
Phy Mode	CCK ▾
EncryptType	NONE ▾
AP MAC Address	00:0C:43:28:60:E8
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>

Step4 Click **Wireless > Security** to display the **Wireless Security/Encryption Settings** page.

Select SSID	
SSID choice	Getnet ▾
"Getnet"	
Security Mode	WPA2-PSK ▾
<div style="border: 1px solid black; padding: 5px;"> Disable Open Shared WEPAUTO WPA-Enterprise WPA-PSK WPA2-Enterprise WPA2-PSK WPA-PSK/WPA2-PSK WPA1/WPA2-Enterprise Dynamic WEP 802.1X </div>	
WPA	
WPA Algorithms	<input type="text"/>
Pass Phrase	<input type="text"/>
Key Renewal Interval	<input type="text"/>
Access Policy	
Policy	Disable ▾
Add a station Mac:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

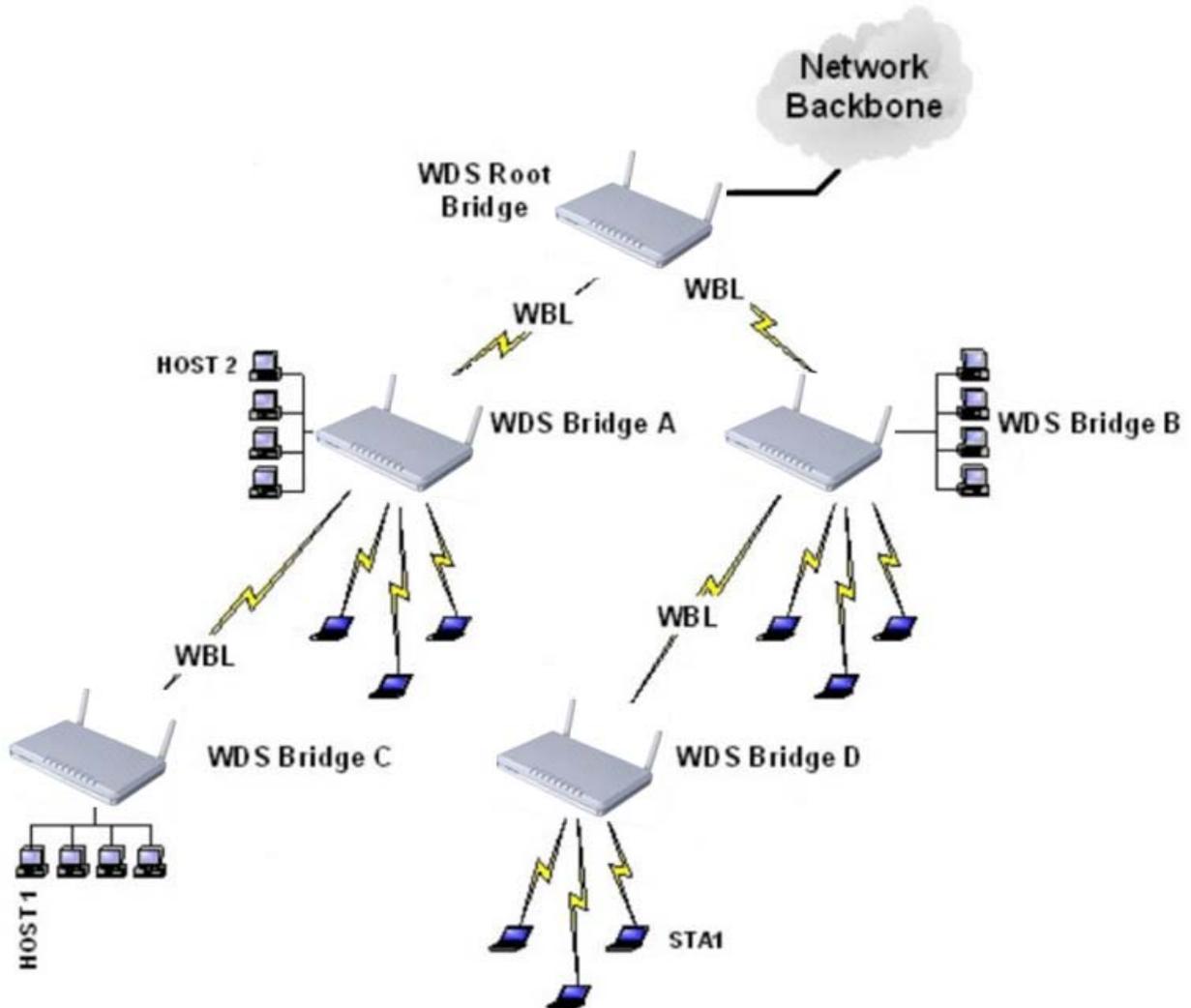
Step5 On this page, set the security mode of the GR-124W to accord with the peer AP.

Note:

In the WDS mode, do not set any mixed modes, for example, WPA-PSK/WPA2-PSK.

- **WDS Bridge Mode**

In the Bridge mode, you can use the GR-124W to connect to your router, for extending wireless coverage. Meanwhile, it can also decrease the working load of the AP that accesses the Internet. In that case, the wireless card does not directly communicate with the wireless device that accesses the Internet, but it directly communicates with the GR-124W.



Step1 On the **Basic Wireless Settings** page, select the WDS mode to be **Bridge Mode**.

Wireless Distribution System(WDS)	
WDS Mode	Bridge Mode ▾
Phy Mode	CCK ▾
EncryptType	NONE ▾
AP MAC Address	00:DC:43:28:60:E8
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>

Step2 On the **Basic Wireless Settings** page, set the physical mode and the encryption type of AP to accord with that of peer AP, and then enter the MAC address of the peer AP. After finishing the settings, click the **Apply** button to apply the settings. The GR-124W will work in the **Bridge** mode.

Step3 On this page, set the security mode of the GR-124W to accord with the peer AP.

Select SSID	
SSID choice	Getnet ▾
"Getnet"	
Security Mode	WPA2-PSK ▾
<div style="border: 1px solid black; padding: 5px;"> Disable Open Shared WPA WPA Algorithms WEPAUTO WPA-Enterprise WPA-PSK WPA2-Enterprise WPA2-PSK WPA-PSK/WPA2-PSK WPA1/WPA2-Enterprise Dynamic WEP 802.1X </div>	
WPA	
WPA Algorithms	WEPAUTO
Pass Phrase	WPA-Enterprise
Key Renewal Interval	WPA-PSK
Access Policy	
Policy	Disable ▾
Add a station Mac:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Note:

In the WDS mode, do not set any mixed modes, for example, WPA-PSK/WPA2-PSK.

- **WDS Lazy Mode**

In the Lazy mode, the GR-124W automatically connects to the WDS devices that use the same SSID, channel, encryption mode, and physical mode. You do not need to manually enter other MAC addresses of peer APs.

Wireless Distribution System(WDS)	
WDS Mode	Lazy Mode
Phy Mode	CCK
EncryptType	NONE

Step1 On the **Basic Wireless Settings** page, set the WDS mode to be **Lazy Mode**, set the physical mode and the encryption type of AP to accord with that of peer AP, and then enter the MAC address of peer AP. After finishing the settings, click the **Apply** button to apply the settings. The GR-124W will work in the **Lazy** mode.

Step2 On this page, set the security mode of the GR-124W to accord with the peer AP.

Select SSID	
SSID choice	Getnet
"Getnet"	
Security Mode	WPA2-PSK
WPA	
WPA Algorithms	WPA2-PSK
Pass Phrase	
Key Renewal Interval	
Access Policy	
Policy	Disable
Add a station Mac:	
Apply Cancel	

Note:

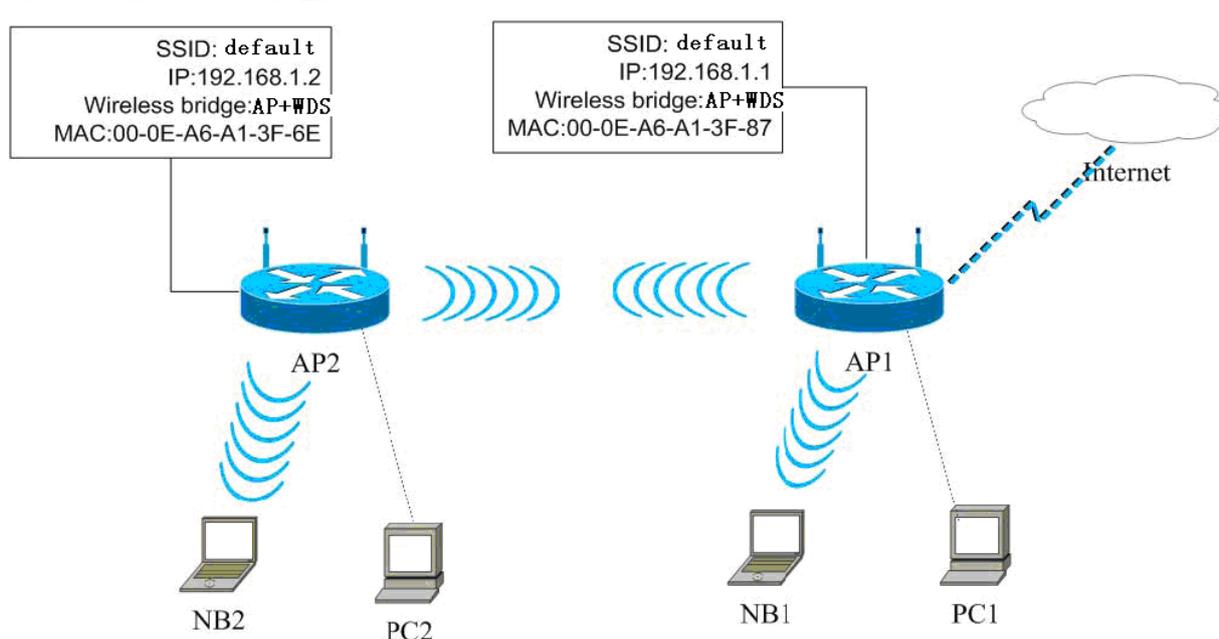
In the WDS mode, do not set any mixed modes, for example, WPA-PSK/WPA2-PSK.

Do not set all the WDS APs to be **Lazy** mode, please ensure that at least one WDS AP acts as **Root Bridge**, and enter the MAC addresses in the WDS table on the **Basic Wireless Settings** page.

- **Establishing a Network by WDS Bridge Mode**

The following description shows how to use the WDS bridge modes of two devices to establish a network. You may add more devices to establish a network.

Suppose that there are two APs. One is AP1, the other is AP2. Enable the DHCP server of AP1 and AP2.



The following table shows the settings of AP1 and AP2.

	Access Point 1	Access Point 2
SSID	default	default
LAN IP Address	192.168.1.1	192.168.1.2
Encryption	NONE	NONE
Wireless Bridge	WDS Mode	WDS Mode
MAC Address	00:0E:A6:A1:3F:87	00:0E:A6:A1:3F:6E
Allow Anonymous	No	No
DHCP Server	Yes	No

- **Set AP1**

Step1 Enter <http://192.168.1.1> in the IE address bar, and then enter the user name (by default, **admin**) and the password (by default, **admin**) to log in to the Web page.

Step2 On the **Basic Wireless Settings** page, set the WDS mode to be **Bridge Mode**, and enter the MAC address of the AP2.

Wireless Distribution System(WDS)	
WDS Mode	Bridge Mode ▾
Phy Mode	CCK ▾
EncryptType	NONE ▾
AP MAC Address	00:0E:A6:A1:3F:6E
AP MAC Address	
AP MAC Address	
AP MAC Address	

Step3 Set the SSID of AP1. AP1 and AP2 must use the same SSID and channel.

Wireless Network	
Radio On/Off	RADIO OFF
Network Mode	11b/g mixed mode ▾
Network Name(SSID)	Getnet
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Multiple SSID6	
Multiple SSID7	
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:0C:43:30:52:F0
Frequency (Channel)	2462MHz (Channel 11) ▾
Rate	Auto ▾

Step4 On the **Wireless Security /Encryption Settings** page, disable the security mode.

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID

SSID choice	Getnet ▼
-------------	----------

"Getnet"

Security Mode	Disable ▼
---------------	-----------

Access Policy

Policy	Disable ▼
Add a station Mac:	<input type="text"/>

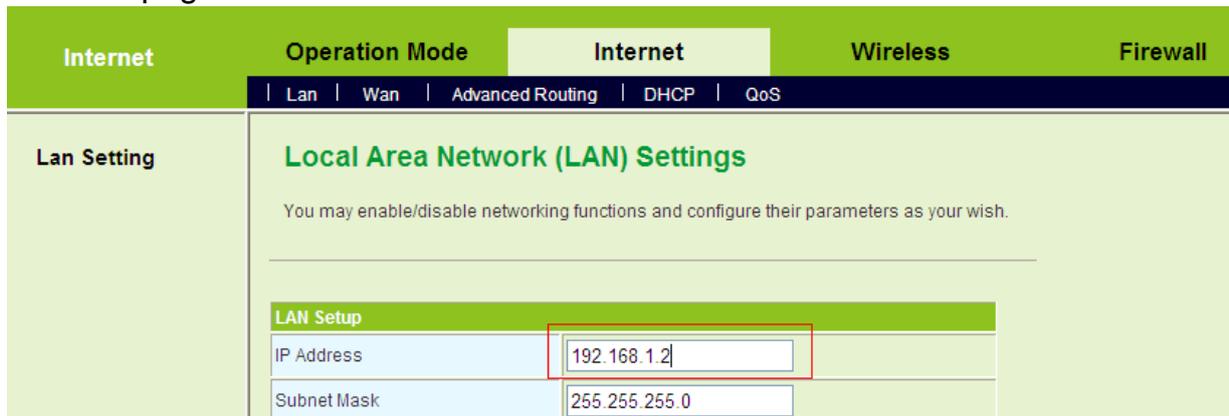
Step5 Click **Internet > LAN** to display the **Local Area Network (LAN) Settings** page. Set the IP address of AP1 to be 192.168.1.1.

Internet	Operation Mode	Internet	Wireless				
	Lan Wan Advanced Routing DHCP QoS						
Lan Setting	<div style="background-color: #92d050; padding: 5px; margin-bottom: 10px;"> Local Area Network (LAN) Settings </div> <p>You may enable/disable networking functions and configure their parameters as your wish.</p> <hr/> <div style="background-color: #92d050; padding: 5px; margin-bottom: 10px;"> LAN Setup </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">IP Address</td> <td>192.168.1.1</td> </tr> <tr> <td>Subnet Mask</td> <td>255.255.255.0</td> </tr> </table>			IP Address	192.168.1.1	Subnet Mask	255.255.255.0
IP Address	192.168.1.1						
Subnet Mask	255.255.255.0						

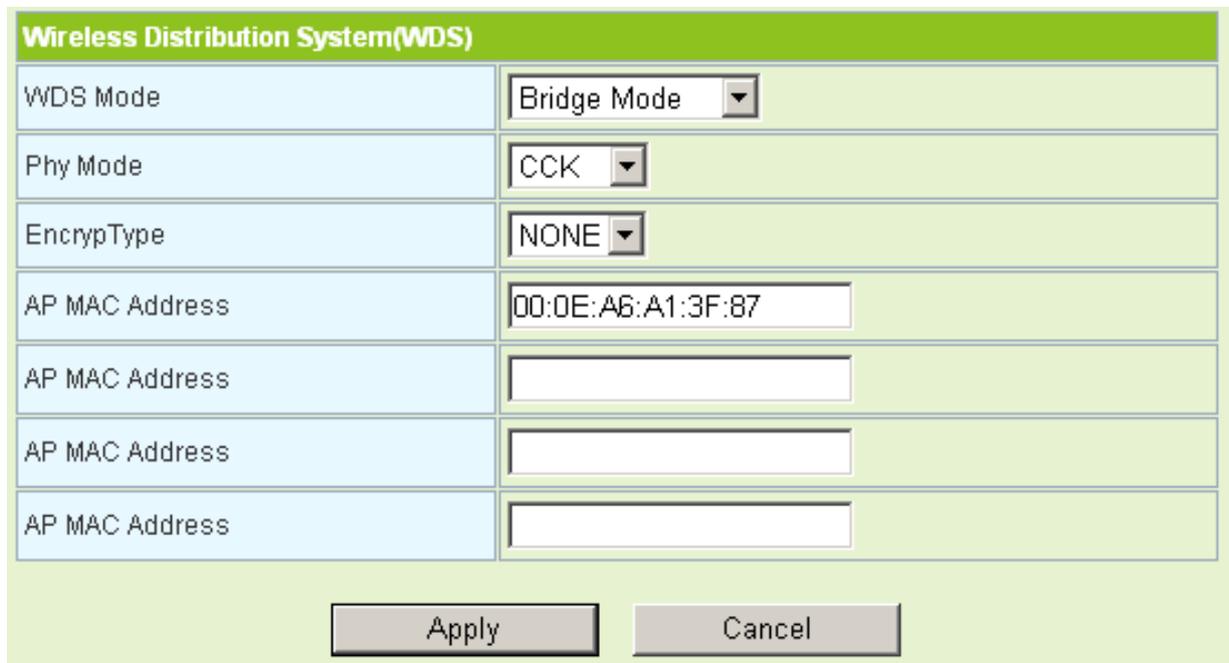
Step6 Click **Administration > Statistics** to display the **Statistic** page. On this page, you can view the information of WDS AP, such as MAC address, and the number of transmitted frames.

- **Set AP2**

Step1 Click **Internet > LAN** to display the **Local Area Network (LAN) Settings** page. Set the IP address of AP2 to be **192.168.1.2**.

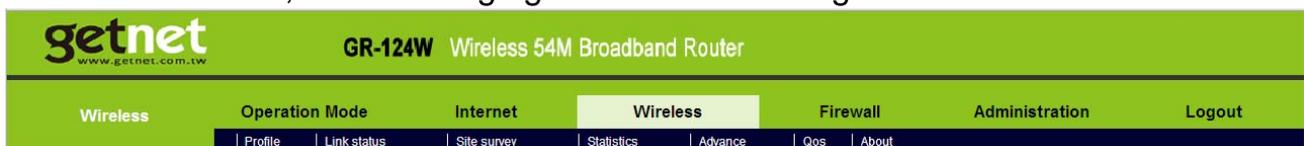


Step2 On the **Basic Wireless Settings** page, set the WDS mode to be **Bridge Mode** and enter the MAC address of the AP1.



5.5 Wireless Settings (WISP Mode)

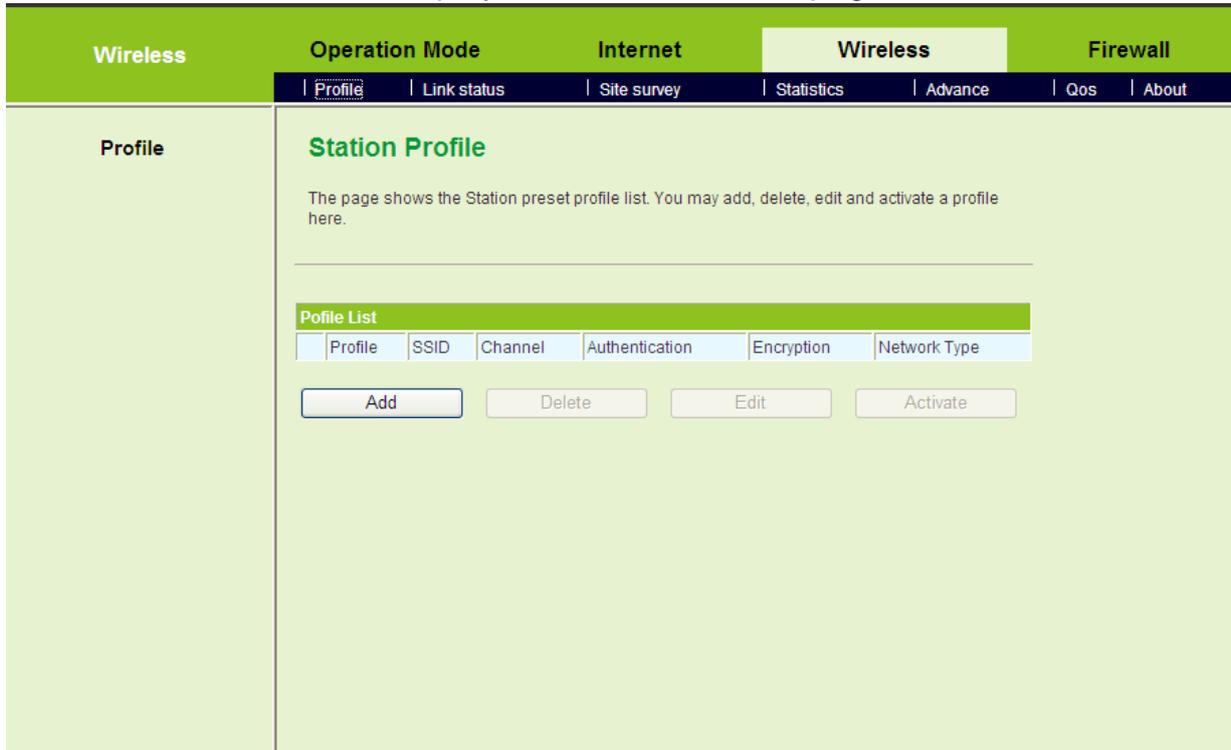
In the WISP mode, the following figure shows the navigation menu of the **Wireless**:



In the WISP mode, the sub-menus of the **Wireless Settings** include **Profile**, **Link Status**, **Site Survey**, **Statistics**, **Advance**, **QoS**, and **About**.

5.5.1 Profile

Click **Wireless > Profile** to display the **Station Profile** page.



On this page, you can add a new profile, delete, edit, and active a preset profile in the profile list.

- **Add a Profile**

Click the **Add** button on the **Station Profile** page, and the **System Configuration** page appears.

System Configuration	
Profile Name	PROF001
SSID	
Network Type	Infrastructure
Power Saving Mode	<input checked="" type="radio"/> CAM (Constantly Awake Mode) <input type="radio"/> Power Saving Mode
RTS Threshold	<input type="checkbox"/> Used 2347
Fragment Threshold	<input type="checkbox"/> Used 2346

Security Policy	
Security Mode	OPEN

Wire Equivalence Protection (WEP)		
WEP Key Length	64 bit (10 hex digits / 5 ascii keys)	
WEP Key Entry Method	Hexadecimal	
WEP Keys	WEP Key 1 :	
	WEP Key 2 :	
	WEP Key 3 :	
	WEP Key 4 :	
Default Key	Key 1	

- System Configuration

The parameters of **System Configuration** page are described as follows:

Field	Description
Profile Name	Set a profile name.
SSID	Enter the SSID of AP that you want to connect.
Network Type	<ul style="list-style-type: none"> ● Infrastructure: An application mode for integrating the cable LAN and the wireless

Field	Description
	<p>LAN structures. The devices need an AP to communicate each other.</p> <ul style="list-style-type: none"> ● 802.11 Ad Hoc :A point to point connection mode without AP.
Power Saving Mode	<ul style="list-style-type: none"> ● CAM (Constantly Awake Mode) is not a power saving mode. CAM is the default setting. ● Power Saving Mode: For saving power.
Channel	<p>When selecting the network type to be 802.11 Ad hoc, you may select a proper channel in the drop down list.</p>
11B Preamble Type	<p>When selecting the network type to be 802.11 Ad hoc, you are allowed to set the 11B preamble type. You may select Auto or Long.</p>
RTS Threshold	<p>Whether to set the RTS Threshold. The default value is 2347.</p>
Fragment Threshold	<p>Whether to set the fragment threshold. The default value is 2346.</p>

- **Security Policy (OPEN and SHARED Mode)**

When selecting the security mode to be **OPEN** or **SHARED**, the WEP table appears on the **System Configuration** page.

Security Policy		
Security Mode	OPEN	
Wire Equivalence Protection (WEP)		
WEP Key Length	64 bit (10 hex digits / 5 ascii keys)	
WEP Key Entry Method	Hexadecimal	
WEP Keys	WEP Key 1 :	<input type="text"/>
	WEP Key 2 :	<input type="text"/>
	WEP Key 3 :	<input type="text"/>
	WEP Key 4 :	<input type="text"/>
Default Key	Key 1	

The parameters of **WEP** (Wire Equivalence Protection) are described as follows:

Field	Description
WEP Key Length	When selecting 64 bit (10 hex digits/5 ascii keys), it allows you to set 10-hex-digit or 5-ASCII-character key. When selecting 128 bit (26 hex digits/13 ascii keys), it allows you to set 26-hex-digit or 13 - ASCII-character key.
WEP Key Entry Method	You may select Hexadecimal or ASCII text .
WEP Keys (WEP key 1~4)	For setting WEP keys.
Default Key	Set a default key.

- **Security Policy (WPA-Personal or WPA2-Personal Mode)**

When selecting the security mode to be **WPA-Personal** or **WPA2-Personal**, the WPA table appears on the **System Configuration** page.

Security Policy

Security Mode: WPA-Personal

WPA

WPA Algorithms: TKIP AES

Pass Phrase:

Apply Cancel

The parameters of **WPA** are described as follows:

Field	Description
WPA Algorithms	You may select TKIP or AES .
Pass Phrase	Set the encryption key.

- **Delete a Profile**

If you want to delete a preset profile (e.g. PROF001), choose this profile and then click the **Delete** button. See the following figure:

Profile List

	Profile	SSID	Channel	Authentication	Encryption	Network Type
<input checked="" type="checkbox"/>	PROF001	Getnet12	Auto	OPEN	NONE	Infrastructure

Add Delete Edit Activate

- **Edit a Profile**

If you want to delete a preset profile (e.g. PROF001), choose this profile and then click the **Edit** button. See the following figure:

System Configuration		
Profile Name	PROF001	
SSID	Getnet12	
Network Type	Infrastructure	
Power Saving Mode	<input checked="" type="radio"/> CAM (Constantly Awake Mode) <input type="radio"/> Power Saving Mode	
RTS Threshold	<input type="checkbox"/> Used 2347	
Fragment Threshold	<input type="checkbox"/> Used 2346	
Security Policy		
Security Mode	OPEN	
Wire Equivalence Protection (WEP)		
WEP Key Length	64 bit (10 hex digits/ 5 ascii keys)	
WEP Key Entry Method	Hexadecimal	
WEP Keys	WEP Key 1 :	
	WEP Key 2 :	
	WEP Key 3 :	
	WEP Key 4 :	
Default Key	Key 1	

On this page, you can modify the parameters of PROF001, such as SSID, network type and security mode.

- **Activate a Profile**

If you want to delete a preset profile (e.g. PROF001), choose this profile and then click the **Activate** button. The activated file will be marked with an icon . See the following figure:

Profile List						
	Profile	SSID	Channel	Authentication	Encryption	Network Type
<input checked="" type="checkbox"/>	PROF001	Getnet12	Auto	OPEN	NONE	Infrastructure

5.5.2 Link Status

Click **Wireless > Link Status** to display the **Station Link Status** page.

Wireless	Operation Mode	Internet	Wireless	Firewall	Administration
	Profile <u>Link status</u>	Site survey	Statistics Advance	Qos	About

Link status

Station Link Status

Information about current connection status, such as link speed, link quality and signal strength.

Link Status	
Status	luolei1 <--> 06-15-EB-8C-52-18
Extra Info	Link is Up
Channel	6 <--> 2437000 KHz ; Central Channel: 6
Link Speed	Tx(Mbps) 2.0 Rx(Mbps) 2.0
Throughput	Tx(Kbps) 0.0 Rx(Kbps) 0.0
Link Quality	Good 74%
Signal Strength 1	Weak 0%
Signal Strength 2	Weak 0%
Signal Strength 3	Weak 0%
Noise Level	Low 50%

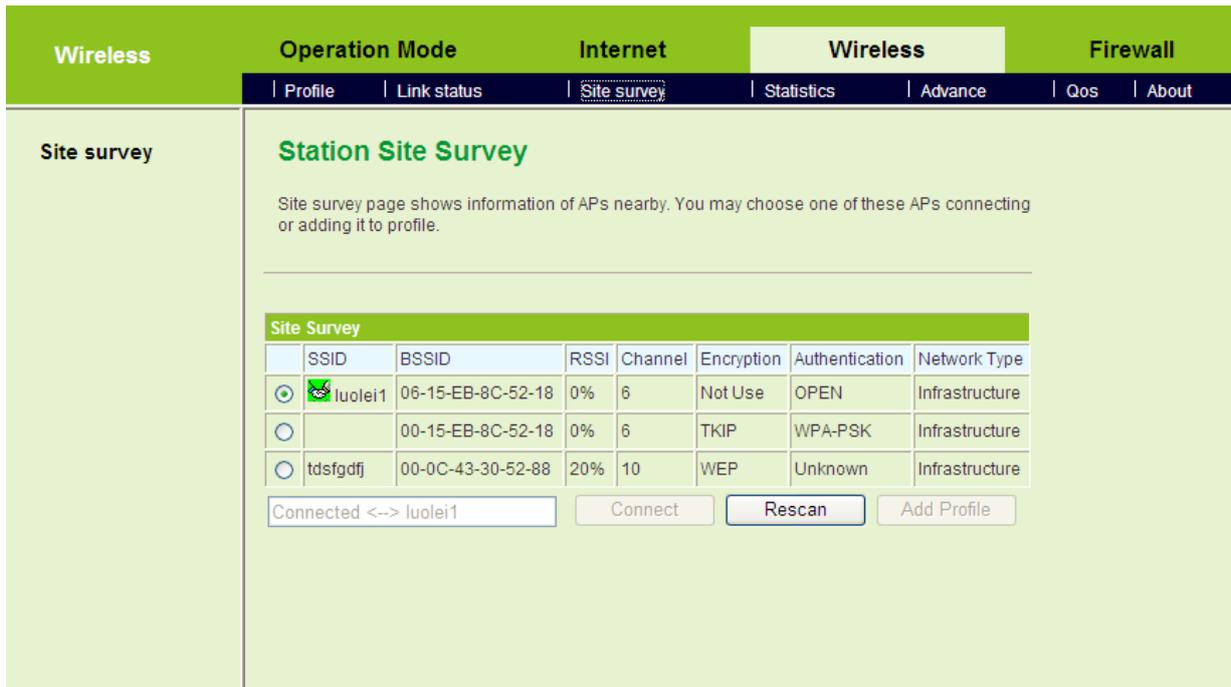
dBm format

HT	
BW	20
GI	long
STBC	none
MCS	1
SNR0	13
SNR1	4886928

On this page, you can view the connection status of AP in the STA mode.

5.5.3 Site Survey

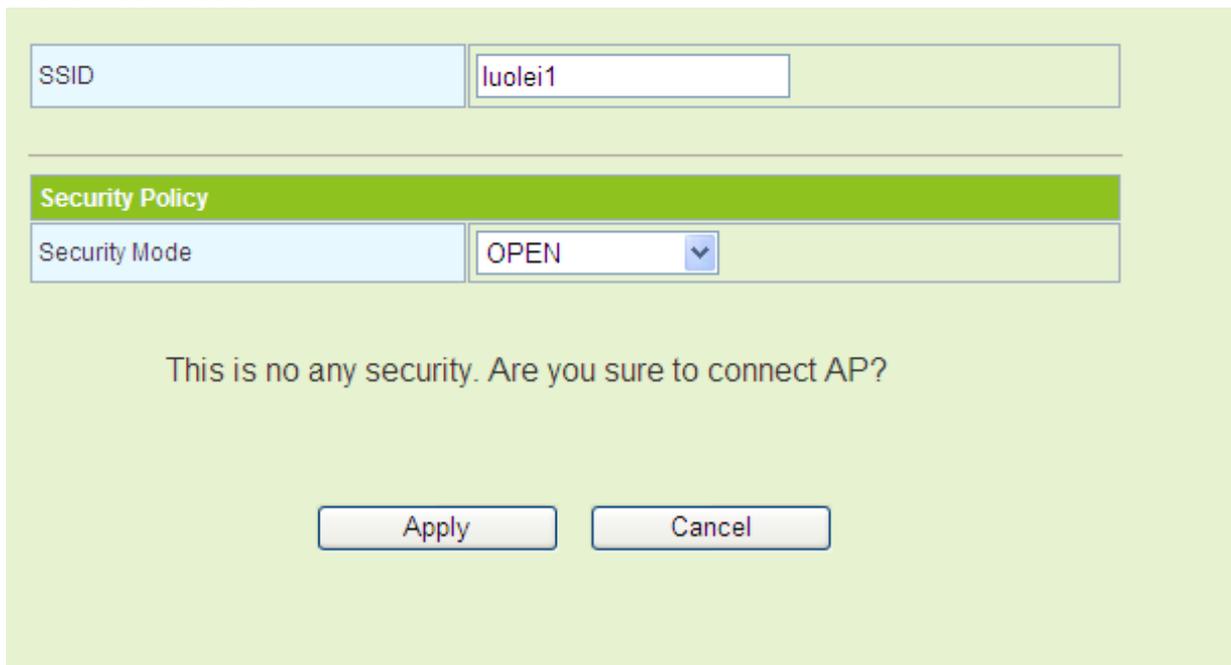
Click **Wireless > Site Survey** to display the **Station Site Survey** page.



On this page, you can view the scanned APs, scan the nearby APs, connect an AP, or add the connection parameters of an AP to the profile list.

- **Connect an AP**

If you want to connect an AP, choose the AP's SSID, and then click the **Connect** button. If this AP is not encrypted, click the **Apply** button on the following page to establish connection.



If this AP is encrypted, click the **Connect** button, and the following page appears.

SSID

Security Policy

Security Mode

WPA

WPA Algorithms TKIP AES

Pass Phrase

On this page, you need to enter the password in the **Pass Phrase** field. After clicking the **Apply** button, and if this encrypted AP is connected successfully, the SSID of this AP is marked with a green icon .

Wireless Operation Mode Internet **Wireless** Firewall

Profile Link status Site survey Statistics Advance Qos About

Site survey

Station Site Survey

Site survey page shows information of APs nearby. You may choose one of these APs connecting or adding it to profile.

Site Survey							
	SSID	BSSID	RSSI	Channel	Encryption	Authentication	Network Type
<input checked="" type="radio"/>	 luolei1	06-15-EB-8C-52-18	0%	6	Not Use	OPEN	Infrastructure
<input type="radio"/>	tdsfgdfj	00-0C-43-30-52-88	20%	10	WEP	Unknown	Infrastructure

Connected <--> luolei1

- **Scan APs**

Click the **Rescan** button on the **Station Site Survey** page, and then you can rescan the nearby APs. If new APs are detected, **Site Survey** table will be refreshed.

- **Add a Profile**

On the **Station Site Survey** page, select an AP in the **Site Survey** table, and then click the **Add Profile** button to enter **System Configuration** page. On **System Configuration** page, click the **Apply** button to add this AP to the profile list.

5.5.4 Statistics

Click **Wireless > Statistics** to display the **Station Statistics** page.

The screenshot shows the 'Station Statistics' page. At the top, there is a navigation bar with tabs for 'Wireless', 'Operation Mode', 'Internet', 'Wireless', and 'Firewall'. Under the 'Wireless' tab, there are sub-tabs for 'Profile', 'Link status', 'Site survey', 'Statistics', 'Advance', 'Qos', and 'About'. The 'Statistics' sub-tab is selected. The main content area has a sidebar on the left with 'Statistics' selected. The main content area is titled 'Station Statistics' and contains a description: 'The page shows the Station statistic information of transmitted and received frames.' Below this is a table with two sections: 'Transmit Statistics' and 'Receive Statistics'. The 'Transmit Statistics' table has 6 rows, and the 'Receive Statistics' table has 4 rows. At the bottom of the page, there is a 'Reset Counters' button.

Transmit Statistics	
Frames Transmitted Successfully	1064
Frames Transmitted Successfully Without Retry	202
Frames Transmitted Successfully After Retry(s)	862
Frames Fail To Receive ACK After All Retries	56
RTS Frames Successfully Receive CTS	0
RTS Frames Fail To Receive CTS	0

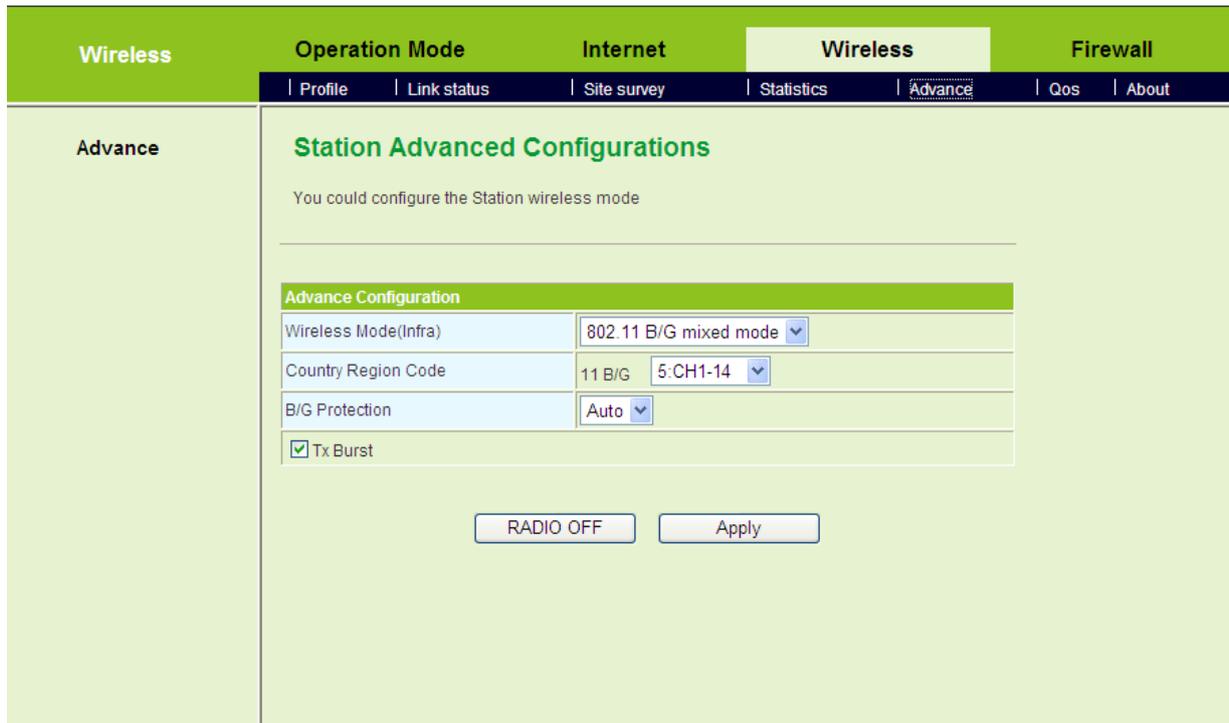
Receive Statistics	
Frames Received Successfully	3196
Frames Received With CRC Error	5290
Frames Dropped Due To Out-of-Resource	0
Duplicate Frames Received	11

On this page, you can view the status of transmitted and received data.

Click the **Reset Counters** button, and then the data statistic information can be refreshed.

5.5.5 Advance

Click **Wireless > Advance** to display the **Station Advanced Configurations** page.



This page is used to configure wireless advanced properties.

The parameters of **Advance Configuration** are described as follows:

Field	Description
Wireless Mode (Infra)	<p>The wireless modes include:</p> <ul style="list-style-type: none"> ● 802.11 B/G mixed mode ● 802.11 B Only ● 802.11 G Only <p>The default wireless mode is 802.11 B/G mixed mode.</p>
Country Region Code	<p>Select the proper country region code. For example, America's (FCC) channel range is 1~11. Europe (ETSI) channel range is 1~13.</p>
B/G Protection	<p>If 802.11b and 802.11g coexist on your network, it is recommended you enable this option. In this way, the probability of data collision will be reduced, but the transmission efficiency will also be reduced.</p> <p>You may select Auto, On, or Off.</p> <ul style="list-style-type: none"> ● Auto: If selecting this option, AP enables or disables the B/G protection mode according to the network status.

Field	Description
	<ul style="list-style-type: none"> ● On: Enable the B/G protection mode. ● Off: Disable the B/G protection mode.
Tx Burst	Enable or disable Tx Burst. After enabling this option, the transmission efficiency can be improved.

5.5.6 QoS

Click **Wireless > QoS** to display the **Station QoS Configurations** page.

QoS

Station QoS Configurations

You could configure the wireless QoS advanced parameters.

QoS Configuration

WMM	<input checked="" type="checkbox"/> enable
WMM Power Saving	<input type="checkbox"/> enable
PS Mode	<input type="checkbox"/> AC_BE <input type="checkbox"/> AC_BK <input type="checkbox"/> AC_VI <input type="checkbox"/> AC_VO
Direct Link Setup	<input type="checkbox"/> enable

Direct Link Setup

MAC Address	<input type="text"/> - <input type="text"/>
Timeout Value	<input type="text"/> sec

DLS Status

MAC Address	Timeout
-------------	---------

This page is used to configure the wireless QoS properties in the station mode.

- **QoS Configuration**

Qos Configuration	
WMM	<input checked="" type="checkbox"/> enable
WMM Power Saving	<input type="checkbox"/> enable
PS Mode	<input type="checkbox"/> AC_BE <input type="checkbox"/> AC_BK <input type="checkbox"/> AC_VI <input type="checkbox"/> AC_VO
Direct Link Setup	<input type="checkbox"/> enable

The parameters of **QoS Configuration** are described as follows:

Field	Description
WMM	Enable or disable WMM.
WMM Power Saving	Enable or disable WMM power saving mode.
PS Mode	Power saving modes include AC_BE, AC_BK, AC_VI, and AC_VO.
Direct Link Setup	Enable or disable direct link setup.

- **Direct Link Setup (DLS)**

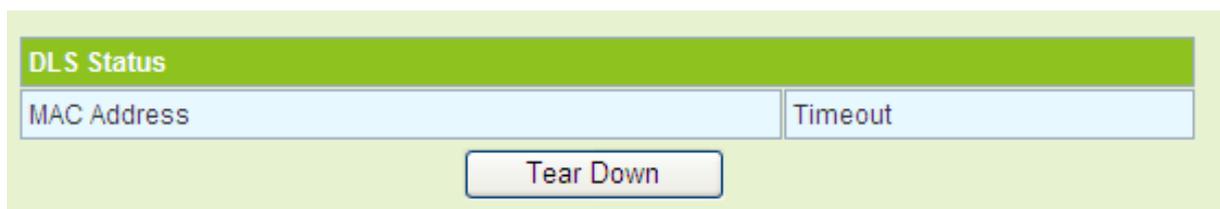
After enabling direct link setup, you are allowed to set the MAC address and timeout value.

Direct Link Setup	
MAC Address	<input type="text"/> - <input type="text"/>
Timeout Value	<input type="text"/> sec

The parameters of **Direct Link Setup** are described as follows:

Field	Description
MAC Address	Enter the MAC address of the DLS client.
Timeout Value	Enter the timeout value for stopping DLS.

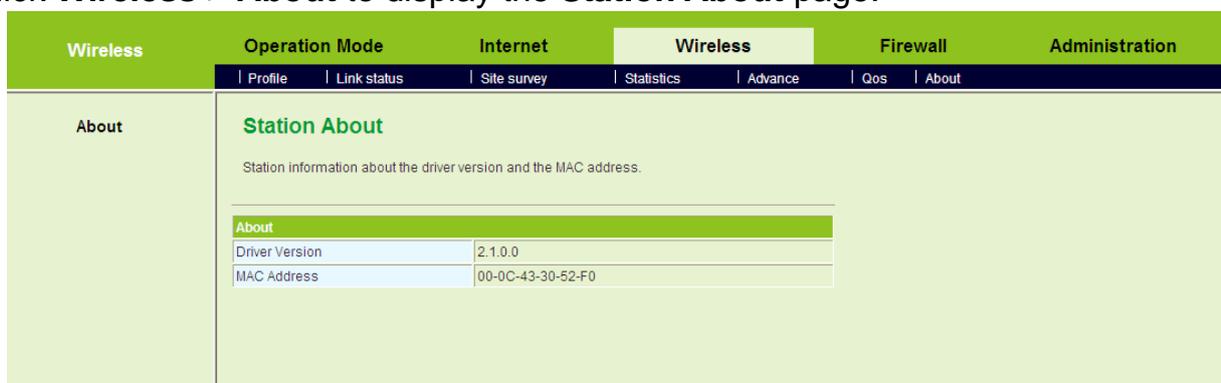
- **DLS Status**



The figure above displays the DLS clients' status.

5.5.7 About

Click **Wireless > About** to display the **Station About** page.



On this page, you can view the AP's driver version and MAC address.

5.6 Firewall

The following figure shows the navigation menu of **Firewall**:



Firewall is an advanced setting, which is used to block or allow the data packets that pass through the AP. The sub-menus of the **Firewall** include **Filtering**, **Forward**, **DMZ**, **System Security**, and **Content Filtering**.

5.6.1 Filtering

Click **Firewall > Filtering** to display the **MAC/IP/Port Filtering Settings** page.

Firewall | Operation Mode | Internet | Wireless | **Firewall** | Administration | Logout

Filtering | Forward | DMZ | System Security | Content Filtering

MAC/IP/Port Filtering Settings

You may setup firewall rules to protect your network from virus,worm and malicious activity on the Internet.

Basic Settings

MAC/IP/Port Filtering:

Default Policy -- The packet that don't match with any rules would be:

MAC/IP/Port Filter Settings

MAC address:

Dest IP Address:

Source IP Address:

Protocol:

Dest Port Range: -

Source Port Range: -

Action:

Comment:

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system:

No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
1	<input type="checkbox"/> 00:C0:26:A3:87:5B	192.168.3.15	172.16.3.45	TCP	-	-	Accept	test	-
Others would be accepted									-

- **Basic Settings**

Basic Settings

MAC/IP/Port Filtering:

Default Policy -- The packet that don't match with any rules would be:

The parameters of **Basic Settings** are described as follows:

Field	Description
MAC/IP/Port Filtering	Enable or disable MAC/IP/Port filtering. The default setting is Disable .
Default Policy	By default, AP will accept all the packets that do not match any rule.

- **MAC/IP/Port Filter Settings**

MAC/IP/Port Filter Settings

MAC address	<input type="text"/>
Dest IP Address	<input type="text"/>
Source IP Address	<input type="text"/>
Protocol	None <input type="button" value="v"/>
Dest Port Range	<input type="text"/> - <input type="text"/>
Source Port Range	<input type="text"/> - <input type="text"/>
Action	Drop <input type="button" value="v"/>
Comment	<input type="text"/>

(The maximum rule count is 32.)

The filter modes of **MAC/IP/Port Filter Settings** are described as follows:

Filter Mode	Description
MAC Filter	MAC filter can block the hosts on the local network to access the Internet.
IP Filter	IP filter can block a user on the LAN to access the Internet.
Port Filter	Port filter can block certain ports of the IP addresses or the traffic of all the ports.

On this page, the maximum rule number you can add is 32.

When the data packets match the following parameters, the data packets will be

discarded.

The parameters of **MAC/IP/Port Filter Settings** are described as follows:

Field	Description
MAC Address	The MAC addresses included in the data packets. It can be a destination MAC address or a source MAC address.
Dest IP Address	The destination IP address.
Source IP Address	The source IP address.
Protocol	The protocol types of data packets, includes TCP , UDP , and ICMP .
Dest Port Range	The destination port range is 1~65535.
Source Port Range	The source port range is 1~65535.
Action	Select Accept or Drop .
Comment	Comment about the rule.

Note:

You should set at least a parameter above, or you may set several parameters or all the parameters above.

- **Current MAC/IP/Port Filtering Rules in System**

Current MAC/IP/Port filtering rules in system:									
No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
1	<input type="checkbox"/> 00:C0:26:A3:87:5B	192.168.3.15	172.16.3.45	TCP	-	-	Accept	test	-
Others would be accepted									-

The figure above shows the current rules in the system.

5.6.2 Virtual Server

Firewall can prevent unexpected stream on the Internet from your host on the LAN. The virtual server can create a channel that can pass through the firewall. In that case, the host on the Internet can communicate with a host on your LAN within certain port range.

Click **Firewall > Forward** to display the **Virtual Server Settings** page.

Firewall | Operation Mode | Internet | Wireless | Firewall

Filtering | Forward | DMZ | System Security | Content Filtering

port Forward

Virtual Server Settings

You may setup Virtual Servers to provide services on Internet.

Virtual Server Settings

Virtual Server Settings: Enable ▾

IP Address:

Port Range: -

Protocol: TCP&UDP ▾

Comment:

(The maximum rule count is 32.)

Apply Reset

Current Virtual Servers in system:

No.	IP Address	Port Range	Protocol	Comment
1 <input type="checkbox"/>	172.15.14.14	1 - 100	TCP + UDP	

Delete Selected Reset

- **Virtual Server Settings**

Virtual Server Settings

Virtual Server Settings: Enable ▾

IP Address:

Port Range: -

Protocol: TCP&UDP ▾

Comment:

(The maximum rule count is 32.)

Apply Reset

The parameters of **Virtual Server Settings** are described as follows:

Field	Description
Virtual Server Settings	Enable or disable the virtual server settings.

Field	Description
IP Address	Enter the IP address that you allow to access.
Protocol	Select the protocol that you allow to access. You may select TCP , UDP or TCP&UDP .
Port Range	Enter the port range that you allow to access.
Comment	Enter the comment about the virtual server.

- **Current Virtual Servers in System**

Current Virtual Servers in system:

No.	IP Address	Port Range	Protocol	Comment
1 <input type="checkbox"/>	172.15.14.14	1 - 100	TCP + UDP	

The figure above shows the current virtual server in the system.

5.6.3 DMZ

DMZ allows all the ports of a PC on your LAN to be exposed to the Internet. Set the IP address of the PC to be DMZ host, so that the DMZ host will not be blocked by firewall.

Click **Firewall > DMZ** to display the **DMZ Settings** page.

Firewall
Operation Mode
Internet
Wireless
Firewall

Filtering
Forward
DMZ
System Security
Content Filtering

DMZ

DMZ Settings

You may setup a De-militarized Zone(DMZ) to separate internal network and Internet.

DMZ Settings

DMZ Settings

DMZ IP Address

The parameters of **DMZ settings** are described as follows:

Field	Description
DMZ Settings	Enable or disable the DMZ settings.
DMZ IP Address	Enter the IP address of the DMZ host.

After finishing the settings, click the **Apply** button to apply the settings.

5.6.4 System Security

Click **Firewall > System Security** to display the **System Security Settings** page.

This page provides the security management for the WAN interface.

The parameters of **System Security Settings** are described as follows:

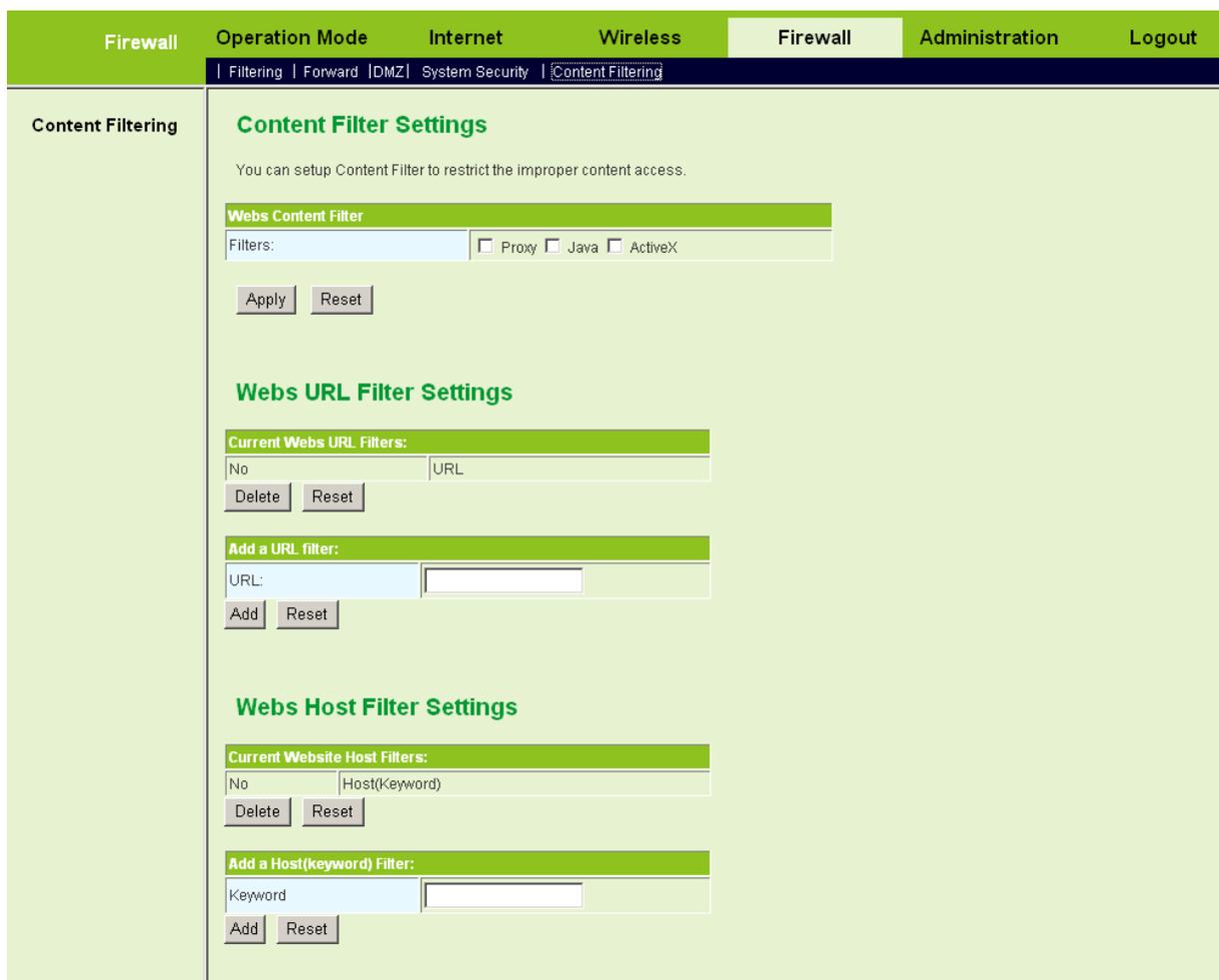
Field	Description
Remote management (Via WAN)	Enable or disable remote management. You may select Deny or Allow . If selecting Allow , users in other regions can access the Internet and configure AP.
WAN Ping Filter	Enable or disable WAN Ping filter. Note: <i>When the remote management is Allow, the WAN Ping filter is disabled.</i>
SPI Firewall	Enable or disable SPI (Stateful Packet Inspection) firewall. Stateful inspection tracks each connection traversing all interfaces of

Field	Description
	<p>the firewall and makes sure that they are valid. When an IP packet arrives at the firewall from the Internet, the firewall inspects the packet to see what connections have been opened from the inside of the network to the Internet. If there is a connection open that applies to the packet that has arrived from the Internet, this incoming packet is let through; otherwise, this incoming packet is rejected. Compared to the NAT firewall, the security level of the SPI firewall is higher.</p>

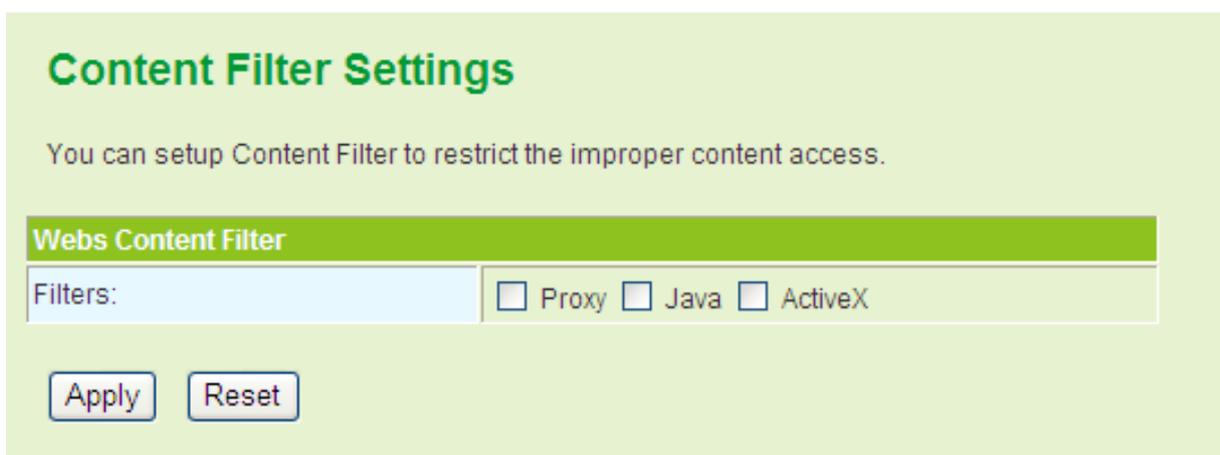
5.6.5 Content Filtering

Content filter can prevent user on LAN from accessing some Web sites on the Internet.

Click **Firewall > Content Filtering** to display the **Content Filtering Settings** page.



- **Webs Content Filter**



Webs Content Filter includes three types of filters. See the following table:

Filter	Description
Proxy	For filtering the proxy pages.
Java	For filtering pages that use Java script.
ActiveX	For filtering plug-in pages.

- **Current Webs URL Filters**

The screenshot shows a web interface titled "Current Webs URL Filters:". Below the title is a table with two columns. The first column contains the text "No" and the second column contains "URL". Below the table are two buttons: "Delete" and "Reset".

Current Webs URL Filters:	
No	URL

The figure above shows the current Web URL filters in the system.

- **Add a URL Filter**

The screenshot shows a web interface titled "Add a URL filter:". Below the title is a form with a label "URL:" followed by an empty input field. Below the input field are two buttons: "Add" and "Reset".

URL:

URL: Enter the URL that needs to be filtered.

- **Current Website Host Filters**

The screenshot shows a web interface titled "Webs Host Filter Settings". Below the title is a section titled "Current Website Host Filters:". Below this section is a table with two columns. The first column contains the text "No" and the second column contains "Host(Keyword)". Below the table are two buttons: "Delete" and "Reset".

Webs Host Filter Settings

Current Website Host Filters:

No	Host(Keyword)
----	---------------

The figure above shows the current Website host filters in the system.

- **Add a Host (keyword) Filter**

Add a Host(keyword) Filter:

Keyword

Keyword: Enter the key words of the host that needs to be filtered.
After finishing the settings, click the **Add** button to add a new host filter.

5.7 Administration

The following figure shows the navigation menu of the **Administration**:



The sub-menus of the **Administration** include **Management**, **Upload**, **Settings**, **Status**, **Statistics** and **Log**.

5.7.1 Management

Click **Administration** > **Management** to display the **System Management** page.

Administration **Operation Mode** **Internet** **Wireless** **Firewall** **Administration**

Management | Upload | Settings | Status | Statistics | Log

Management

System Management

You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.

Administrator Settings

Account:

Password:

NTP Settings

Current Time:

Time Zone:

NTP Server:

ex: time.nist.gov
ntp0.broad.mit.edu
time.stdtime.gov.tw

NTP synchronization(hours):

DDNS Settings

Dynamic DNS Provider:

Account:

Password:

DDNS:

This page provides administration settings, NTP settings, and DDNS settings.

- **Administrator Settings**

Administrator Settings

Account:

Password:

The parameters of **Administrator Settings** are described as follows:

Field	Description
Account	Enter the account that you want to change.
Password	Enter the password for the new account.

Note:

If you forget the account and the password, please press the **Reset** button. The system will return to the factory default settings. The default account and the password are **Admin**.

- **NTP Settings**

You may set the AP time to synchronize the time with your PC or the NTP server.

The parameters of the **NTP Settings** are described as follows:

Field	Description
Current Time	Display the current system time. Click the Sync with Host button, and then AP can synchronize its time with your PC.
Time Zone	Select your proper time zone.
NTP Server	Enter the URL of the time server.
NTP synchronization (hours)	Set the interval for synchronizing with the time server.

- **DDNS Settings**

The parameters of **DDNS Settings** are described as follows:

Field	Description
Dynamic DNS Provider	You may select a proper DDNS provider in the drop down list. The DDNS providers include Dyndns.org, freedns.afraid.org, www.zoneedit.com, and www.no-ip.com
Account	Enter the DDNS account.
Password	Enter the DDNS password.
DDNS	Enter the domain name of DDNS.

5.7.2 Upload Firmware

Click **Administration > Upload** to display the **Upload Firmware** page.

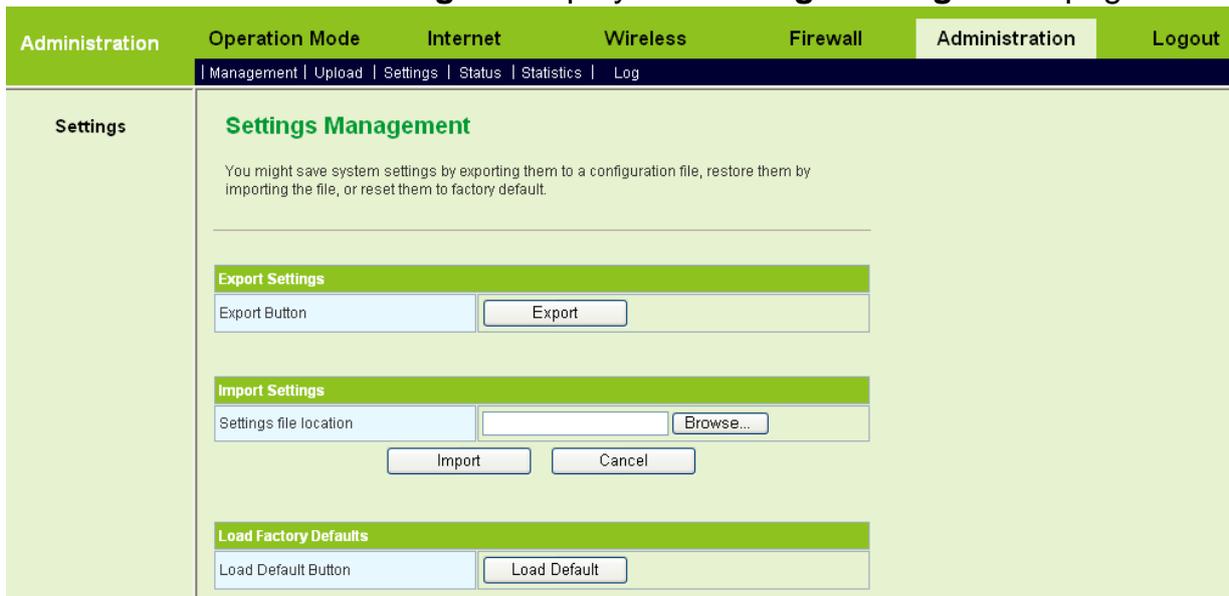
If you want to upload the firmware, click the **Browse...** button to choose the correct new firmware, and then click the **Apply** button. System begins to upgrade firmware. After upgrading, system reboots and automatically enters the Web page.

Note:

Upgrading firmware will make the AP return to the factory defaults. In order to avoid the settings loss, please save the settings before upgrading firmware. During upgrading, do not cut off the power or press the **Reset** button.

5.7.3 Settings Management

Click **Administration > Settings** to display the **Settings Management** page.



The parameters on this page are described as follows:

Field	Description
Export Settings	Click the Export button to save the settings to your local PC.
Import Settings	Click the Browse... button to choose the settings on your PC, and then click the Import button to import the settings to AP.
Load Factory Defaults	Click the Load Default button, and then system returns to the factory default settings.

5.7.4 Status

Click **Administration > Status** to display the **Access Point Status** page.

Administration Operation Mode Internet Wireless Firewall Administration

Management | Upload | Settings | **Status** | Statistics | Log

Status

Access Point Status

Let's take a look at the status of Getnet SoC Platform.

System Info	
SDK Version	v1.0.1.3
status uboot version	v3.2.3
System Up Time	2 hours, 8 mins, 50 secs
Operation Mode	Gateway Mode

Internet Configurations	
Connected Type	DHCP
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	
Secondary Domain Name Server	
MAC Address	00:0C:43:30:52:F0

Local Network	
Local IP Address	192.168.1.1
Local Netmask	255.255.255.0
MAC Address	00:0C:43:30:52:F0

Ethernet Port Status

This page displays system information, Internet configuration, and local network settings.

5.7.5 Statistic

Click **Administration > Statistics** to display the **Statistic** page.

Administration Operation Mode Internet Wireless Firewall Administration

Management | Upload | Settings | Status | **Statistics** | Log

Statistics

Statistic

Take a look at the Getnet SoC statistics

Memory	
Memory total:	13892 kB
Memory left:	1720 kB

WAN/LAN	
WAN Rx packets:	0
WAN Rx bytes:	0
WAN Tx packets:	189
WAN Tx bytes:	112266
LAN Rx packets:	820
LAN Rx bytes:	82235
LAN Tx packets:	1267
LAN Tx bytes:	725711

All interfaces	
Name	lo
Rx Packet	270
Rx Byte	24154
Tx Packet	270
Tx Byte	24154
Name	eth2
Rx Packet	5772
Rx Byte	694912
Tx Packet	9874
Tx Byte	4317993
Name	eth2.1
Rx Packet	0
Rx Byte	0
Tx Packet	871
Tx Byte	302430

This page displays the memory status, the numbers of transmitted and received data packets of the WLAN, LAN, and WAN.

5.7.6 System Log

Click **Administration > Log** to display the **System Log** page.

The screenshot shows a web interface with a navigation bar at the top containing 'Administration', 'Operation Mode', 'Internet', 'Wireless', 'Firewall', and 'Administration'. Below the navigation bar is a sub-menu with 'Management', 'Upload', 'Settings', 'Status', 'Statistics', and 'Log'. The main content area is titled 'Log' and contains a 'System Log' section. This section includes a text box for setting a remote log server, 'Refresh' and 'Clear' buttons, and a 'Remote System Log Settings' form with an 'Enable' checkbox and an 'IP Address' input field, followed by an 'Apply' button. Below the form is a scrollable 'System Log' window displaying a list of system messages with timestamps and details.

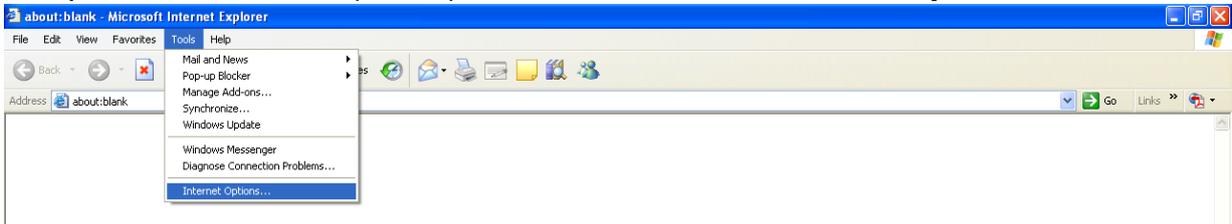
```
Jan 1 00:00:14 (none) user.notice kernel: number of CFI chips: 1
Jan 1 00:00:14 (none) user.notice kernel: cfi_cmdset_0002: Disabling erase-susp
Jan 1 00:00:14 (none) user.notice kernel: Creating 6 MID partitions on "Ralink
Jan 1 00:00:14 (none) user.notice kernel: 0x00000000-0x00030000 : "Bootloader"
Jan 1 00:00:14 (none) user.notice kernel: 0x00030000-0x00040000 : "Config"
Jan 1 00:00:14 (none) user.notice kernel: 0x00040000-0x00050000 : "Factory"
Jan 1 00:00:14 (none) user.notice kernel: 0x00050000-0x00107312 : "Kernel"
Jan 1 00:00:14 (none) user.warn kernel: mtd: partition "Kernel" doesn't end on
Jan 1 00:00:14 (none) user.notice kernel: 0x00107312-0x01000000 : "RootFS"
Jan 1 00:00:14 (none) user.warn kernel: mtd: partition "RootFS" extends beyond
Jan 1 00:00:14 (none) user.warn kernel: mtd: partition "RootFS" doesn't start o
Jan 1 00:00:14 (none) user.notice kernel: 0x00050000-0x01000000 : "Kernel_RootF
Jan 1 00:00:14 (none) user.warn kernel: mtd: partition "Kernel_RootFS" extends
Jan 1 00:00:14 (none) user.info kernel: block2mtd: version $Revision: 1.1.1.1 $
Jan 1 00:00:14 (none) user.warn kernel: Netfilter messages via NETLINK v0.30.
Jan 1 00:00:14 (none) user.warn kernel: ip_conntrack version 2.4 (128 buckets,
Jan 1 00:00:14 (none) user.warn kernel: ip_conntrack_pptp version 3.1 loaded
Jan 1 00:00:14 (none) user.warn kernel: ip_nat_pptp version 3.0 loaded
Jan 1 00:00:14 (none) user.warn kernel: ip_tables: (C) 2000-2006 Netfilter Core
Jan 1 00:00:14 (none) user.notice kernel: ClusterIP Version 0.8 loaded s
Jan 1 00:00:14 (none) user.info kernel: successfully
Jan 1 00:00:14 (none) user.warn kernel: arp_tables: (C) 2002 David S. Miller
Jan 1 00:00:14 (none) user.info kernel: TCP cubic registered
Jan 1 00:00:14 (none) user.info kernel: NET: Registered protocol family 1
Jan 1 00:00:14 (none) user.info kernel: NET: Registered protocol family 17
Jan 1 00:00:14 (none) user.info kernel: 802.1Q VLAN Support v1.8 Ben Greear <gr
Jan 1 00:00:14 (none) user.info kernel: All bugs added by David S. Miller <dave
```

On this page, you are allowed to set the log server and view the system log. After enabling the remote log server and enter the IP address of the server, click the **Apply** button, and then the log information can be sent to the remote log server.

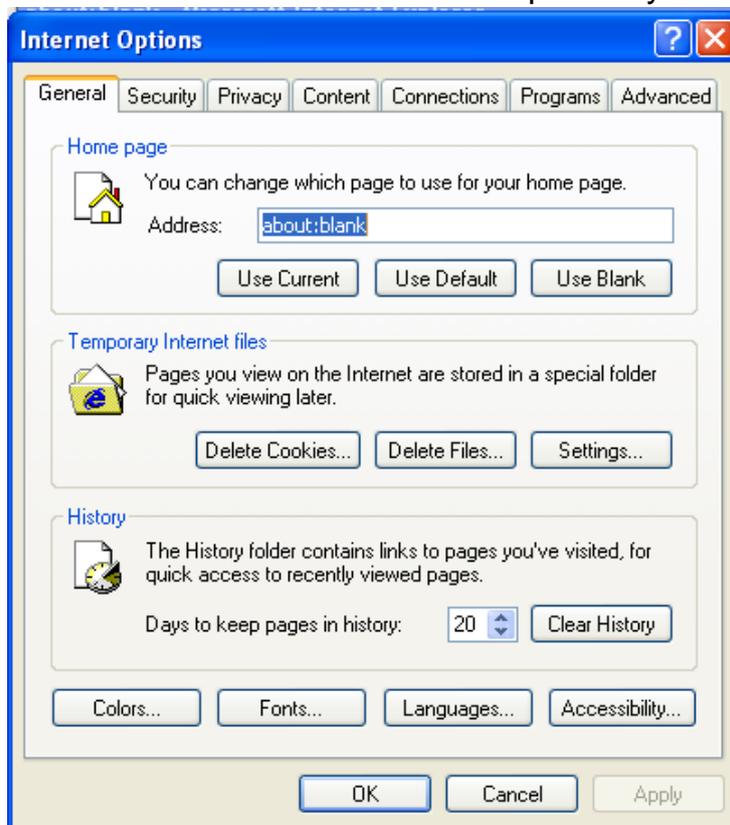
6 Troubleshooting

Why you can not access Web page to configure AP?

(1) Open Web browser (i.e. IE) and select **Tools > Internet Options....**



(2) Click **Delete Cookies...** and **Delete Files...** respectively.



Why you can not establish the network connection?

- Beyond the wireless coverage
 - (1) Place the device near to the client.
 - (2) Try to change the channel setting
- Authentication problem
 - (1) Use the cable to connect the computer to the device.
 - (2) Check the network security setting.
 - (3) Try to reset the device by pressing the **Reset** button.

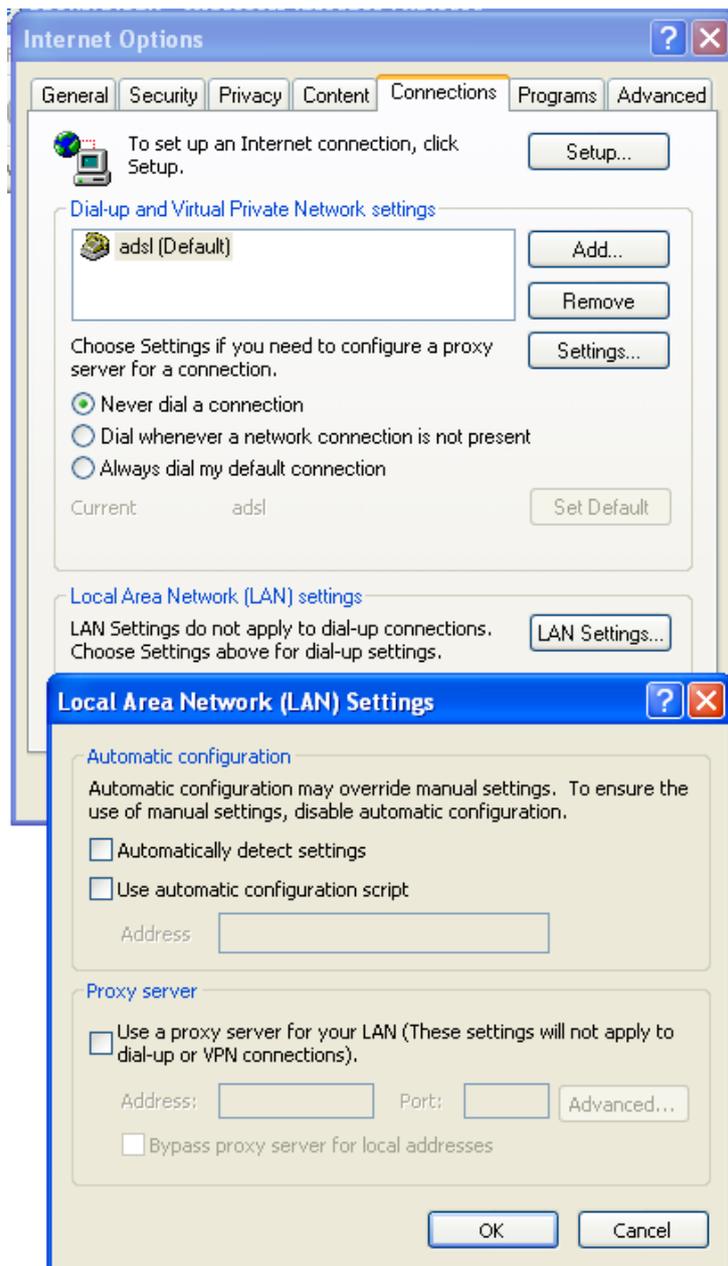
- Can not search the device.
- (1) Try to reset the router and test the device again.
 - (2) Check the setting of the wireless network card.
 - (3) Check the SSID and the encryption setting.

Why you can not access the Internet wirelessly via the device?

- (1) Place the device to the wireless area where user can access the Internet.
- (2) Check whether the wireless network card can connect to the right station.
- (3) Check whether the wireless channel accords with the channel that your country or zone states.
- (4) Check the encryption configuration.
- (5) Check whether your ADSL cable is connected to the correct interfaces.
- (6) Replace a network cable to connect to the device.

Why you can not access the Internet?

- (1) Check whether the LEDs status on the ADSL modem and the wireless device is normal.
- (2) Check whether the WAN indicator is on. If the WAN indicator is off, please check whether the cable connected to the WAN interface is loose.
- (3) When the Link indicator keeps on but does not blink, it indicates that the device has accessed the Internet.
- (4) Reboot your computer.
- (5) Set the device again.
- (6) Check whether the WAN LED is on.
- (7) Check the encryption setting of wireless network.
- (8) Check whether the PC that connects to the device can acquire the IP address via the wireless network or the cable network.
- (9) Check the LAN settings of your Internet options, and do not use a proxy server for your LAN. See the following figure:



getnet
www.getnet.com.tw

EDIMAX Technology Co., Ltd.

www.getnet.com.tw