



Contents

1 Safety Precautions				3	
2	Overview				
	2.1	Prod	uct Introduction	4	
	2.2	Pack	ing list	4	
3	Hard	lware De	escription and Hardware Installation	5	
	3.1	Front	Panel and LED Status	5	
	3.2	Rear	Panel and Interface Description	6	
	3.3	Hard	ware Installation	7	
		3.3.1	System Requirements	7	
		3.3.2	Before You Begin	7	
		3.3.3	Connecting the Device	8	
	3.4	Oper	ation Range	8	
	3.5	Roan	ning	8	
4	TCP	/IP Settir	ngs and Wireless Connection Introduction		
	4.1	TCP/	IP Settings	10	
	4.2	4.2 Wireless Connection Introduction1			
5	Logo	jing In to	the Web Page	19	
6	Web	Configu	ration	21	
	6.1 Setup Wizard				
	6.2	Runn	ing Status	26	
	6.3	Netw	ork Settings	27	
		6.3.1	Operating Mode		
		6.3.2	LAN Interface Settings	29	
		6.3.3	WAN Interface Settings		
		6.3.4	MAC Address Cloning		
	6.4	Wirel	ess Settings	40	
		6.4.1	Basic Settings	41	
		6.4.2	Wireless Security Settings	43	
		6.4.3	Wireless MAC Address Filter	53	
		6.4.4	Advanced Wireless Settings	54	
		6.4.5	Wireless Client List	63	
		6.4.6	WPS Settings	64	

011		We will be the the test will be test	
	6.4.7	WDS Settings	69
6.5	DHCF	P Server	83
	6.5.1	DHCP Service	84
	6.5.2	Static Address Allocation	85
	6.5.3	DHCP Client List	86
6.6	Forwa	arding Rule	87
	6.6.1	Virtual Server	88
	6.6.2	Port Triggering Settings	90
	6.6.3	DMZ Host	92
	6.6.4	UPnP Settings	93
6.7	Secur	ity Options	94
	6.7.1	Security Settings	95
	6.7.2	Advanced Security Settings	96
	6.7.3	LAN Web Management	98
	6.7.4	Remote Web Management	100
6.8	Acces	s Control	101
	6.8.1	MAC/IP/Port Filter Settings	102
	6.8.2	Web URL Filtering	104
6.9	Routir	ng Settings	105
	6.9.1	Static Routing Table	106
6.10	IP Ba	ndwidth Control	107
	6.10.1	IP Bandwidth Control Settings	108
	6.10.2	IP Bandwidth Control List	109
6.11	IP and	d MAC Binding	110
	6.11.1	Static ARP Binding Settings	110
	6.11.2	ARP Mapping Table	111
6.12	Dynar	nic DNS Settings	112
6.13	Syste	m Tools	113
	6.13.1	Network Time Settings	114
	6.13.2	Diagnosis Tools	115
	6.13.3	Software Upgrade	117
	6.13.4	Load Default Settings	118
	6.13.5	Export and Load Settings	119
	6.13.6	Reboot	120
	6.13.7	System Settings	120

	6.13.8	System Log12	1
	6.13.9	Traffic Statistics	3
7	Troubleshooting		4

About User Manual

This user manual mainly describes how to install and configure the wireless router.

Organization

This user manual is organized as follows:

Chapter	Description
Chapter 1 :Safety	Provides safety precaution information.
Precautions	
Chapter 2 :Overview	Provides a general overview of the
	wireless router, and the packing list.
Chapter 3 :Hardware	Mainly describes the front panel and the
Description and Hardware	rear panel of the wireless router and the
Installation	procedures for hardware installation.
Chapter 4 :TCP/IP Settings	Provides the information about how to
and Wireless Connection	configure the TCP/IP settings and how to
Introduction	connect the wireless router wirelessly.
Chapter 5 Logging In to the	Describes how to log in to the wireless
Web Page	router.
Chapter 6 :Web	Mainly describes how to navigate through
Configuration	the Web pages and how to configure the
	parameters.
Chapter 7 : Troubleshooting	Provides the troubleshooting information.

Features

• Support IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.3,

IEEE802.3u, IEEE802.11i, and IEEE802.11e

- Transmission data rate is up to 150 Mbps
- Support WEP and WPA for transmitting data securely
- Support DHCP Server
- Support NetSniper
- Support manually setting static and dynamic routing
- Support firmware version upgrade via Web page
- Support restoring factory default settings
- Support virtual server
- Support DMZ (demilitarized zone)
- Support DNS proxy and forwarding
- Support IP bandwidth settings
- Support MAC and IP filter
- Support authentication modes of wireless security
- Support 4 types of WAN connection modes, including Dynamic IP (DHCP), Static IP, PPPoE, and DHCP+.
- Support remote access control
- Support firewall
- Support system status display
- Support backuping and restoring configuration file
- Support system log

1 Safety Precautions

Before operating the wireless router, read the following precaution information carefully:

- Use the type of power that user manual marks.
- Use the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or the prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid any damage caused by overheating to the device. The long and thin holes on the router are designed for heat dissipation, to ensure that the device works normally. Do not cover these cooling holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where is over damp or watery. Do not spill any liquid on this device.
- Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.
- Do not place this device on an unstable surface or support.

2 Overview

2.1 Product Introduction

The wireless router is a high-performance network access device. It is fully compatible with IEEE802.11b, IEEE802.11g and IEEE802.11n standards. It can provide reliable and convenient access service for the individual user, and SOHO (Small Office, Home Office).

2.2 Packing list

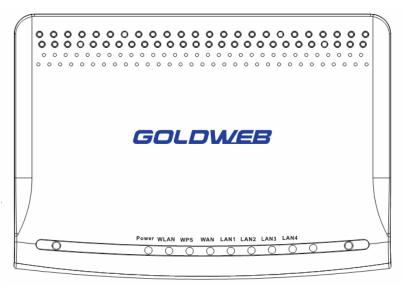
Please check whether your packing list includes the following items:

- wireless router x 1
- Power adapter x 1

3 Hardware Description and Hardware Installation

3.1 Front Panel and LED Status

There are 8 LED indicators on the front panel of the wireless router. By observing their status, you can judge whether the device runs normally.



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

LED	Color	Status	Description
Indicator			
Power	Green	On	Power is on.
	-	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.

GW-WR150N/GW-WR150ND 150Mbps Wireless Router User Manual

WPS	Green	On	Connection succeeds under Wi-Fi Protected Setup.
	Green	Blink	Negotiation is in progress under Wi-Fi Protected Setup.
	-	Off	Wi-Fi Protected Setup is disabled.
WAN	Green	On	Connection succeeds.
	Green	Blink	Data is being transmitted.
	-	Off	No WAN connection.
LAN1/LAN2/	Green	On	LAN connection succeeds.
LAN3/LAN4	Green	Blink	Data is being transmitted.
	-	Off	No LAN connection.

3.2 Rear Panel and Interface Description



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

Interface/Button	Description
Reset	Press Reset gently for 3-6 seconds with a fine needle
	inserted into the hole and then release the button. The
	system reboots and returns to the factory defaults.
Power	Power socket, for connecting the power adapter.
WAN	WAN interface, for connecting WAN or the uplink
	network devices.
LAN1/LAN2/	LAN interfaces, for connecting hub, switch, or
LAN3/LAN4	computer on LAN.
WPS	This button is used for enabling WPS PBC mode. If
	WPS is enabled, press this button, and then AP starts
	to accept the negotiation of PBC mode.

Note:

Do not press **Reset** 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 **Reset** gently for 3-6 seconds with a fine needle inserted into the hole and then release the button. The system reboots and returns to the factory default settings.

Warning:

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

3.3 Hardware Installation

3.3.1 System Requirements

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

- One Ethernet RJ45 cable (10Base-T/100Base-T)
- One wireless router
- A PC is already installed with the TCP/IP protocol and the PC can access the Internet.

3.3.2 Before You Begin

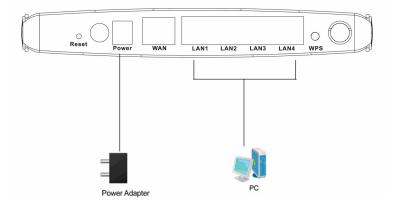
Before you install the device, please pay attention to the following items:

- When the device is connected to a 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.

3.3.3 Connecting the Device

To connect the device, do as follows:

- Step 1 Connect one end of the RJ45 cable to the AP's LAN interface.
- Step 2 Connect the other end of the RJ45 cable to your PC.
- Step 3 Connect the power adapter to the AP's power socket.



3.4 Operation Range

The operation range of AP 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 signal transmission are different. For example, the outdoor straight transmission distance for some devices in the open air is up to 150 meters, and the indoor straight transmission distance is up to 100 meters.

3.5 Roaming

Suppose that several APs run in the same network. Each AP acts as one BSS, and has its coverage range. 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 multiple APs' coverage.

In order to realize the wireless client roaming among different APs, you need to set

the APs properly. Do as follows:

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

4 TCP/IP Settings and Wireless Connection Introduction

Web management tool allows you to configure AP. 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.

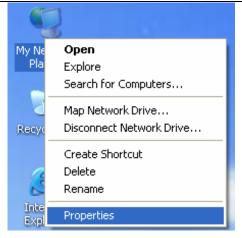
4.1 TCP/IP Settings

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

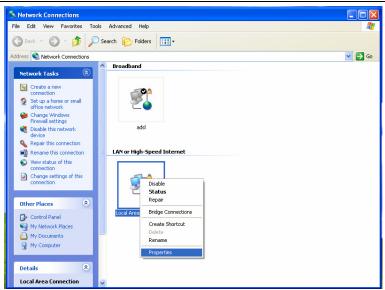
It is recommended you set the network adapter to be **Obtain an IP address automatically**. Your PC acquires IP address, subnet mask, gateway, and DNS address automatically via the AP. If you know the setting of the current LAN interface, you can manually set the TCP/IP properties of the network adapter,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

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

Step 1 Right-click the icon of **My Network Places** (for example, Windows XP) and select **Properties** in the menu. The **Network Connections** page appears.



Step 2 Right-click the network adapter icon and choose **Properties** from 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.*)



Step 3 Double-click the Internet Protocol (TCP/IP) to display the Internet Protocol (TCP/IP) Properties page.

🕹 Local Area Connection Properties 🛛 🔹 💽				
General Advanced				
Connect using:				
Broadcom 440x 10/100 Integrated Cc Configure				
This connection uses the following items:				
 Client for Microsoft Networks Client for Microsoft Networks Client Printer Sharing for Microsoft Networks QoS Packet Scheduler Internet Protocol (TCP/IP) 				
I <u>n</u> stall <u>U</u> ninstall P <u>r</u> operties				
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.				
 Show icon in notification area when connected ✓ Notify me when this connection has limited or no connectivity 				
OK Cancel				

Step 4 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 digit between 2 and 254).

	automatically if your network supports ed to ask your network administrator for
○ Obtain an IP address autom	atically
O Use the following IP address	
IP address:	192.168.1.123
S <u>u</u> bnet mask:	255 . 255 . 255 . 0
Default gateway:	192.168.1.1
 Obtain DNS server address Use the following DNS server Preferred DNS server: Alternate DNS server: 	
	Ad <u>v</u> anced OK Canc

- Step 5 Set the subnet mask and then click **OK** to finish manual setting.
- Step 6 After finishing setting, you may ping the default IP address of the AP, to check whether the current connection between PC and the AP is normal. Click RUN... on the lower left corner of desktop, and then enter ping 192.168.1.1 in the dialog box. See the following figure:

Run	? 🔀
-	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	ping 192.168.1.1
	OK Cancel Browse

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 AP, you should enter the current IP address in the dialog box above.

Step 7 If PC can ping through the default IP address of AP, it indicates that the connection between your PC and the AP is normal. See the following figure:

ex C:\WINDOWS\system32\ping.exe	_ 🗆 ×
	A
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	

4.2 Wireless Connection Introduction

GW-WR150N/GW-WR150ND 150Mbps Wireless Router User Manual By default, the AP function of the wireless router is enabled. User that uses the wireless network adapter can follow the steps below to finish the wireless

connection settings.

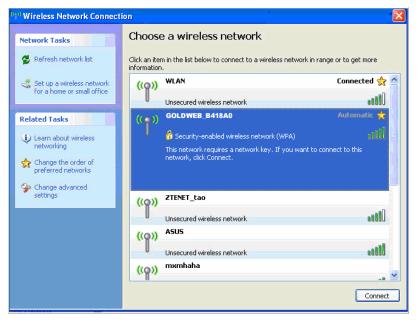
Step 1 Enable your wireless network adapter on your PC, and make sure that the Wireless Zero Configuration tool is available. Right-click the Wireless Network Connection icon and select View Available Wireless Networks.

LAN or High-Spee	d Internet
Not conn 🗶 😹	Network Connection ected, Firewalled Connected, Firewalled
🗡 (မှာ) HED HED	Disable elerated AMD PCN
	View Available Wireless Networks
	Status
	Repair
	Bridge Connections
	Create Shortcut
	Delete
	Rename
	Properties

Step 2 In the Wireless Network Connection page, click Refresh network list and the network list will be refreshed. The default SSID of the wireless router is GOLDWEB_XXXXXX ("XXXXXX" is the end 6 digits of MAC address). Choose the wireless router (e.g. GOLDWEB_B418A0) that you want to connect, and then click the Connect button. The default wireless security mode is Disable, and you can connect the wireless router directly without entering an encryption key. If the wireless router is

encrypted, you need to enter the correct key to connect to the wireless

router.



Step 3 If you are not sure of the available SSID, please log in to the router's Web page, and view the SSID in the **Basic Settings** page of the wireless settings. For more information about the wireless settings, please refer to 6.4 Wireless Settings.

Basic Settings

In this page, you can set the basic network parameters of the wireless network of the router.

Wireless Network	
Wireless Status	wireless enable Display multiple SSID
SSID1	GOLDWEB_B418A0 Hidden Isolated
Mode	11b/g/n mixed mode
Channel	AutoSelect -
Broadcast Network Name (SSID)	C Enable C Disable
SSID internal isolation	C Enable @ Disable
MBSSID AP Isolation	C Enable @ Disable
BSSID	00:1F:A4:B4:18:A0
Frequency Bandwidth	C 20 © 20/40
MCS	Auto
	Save Cancel

Note:

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

5 Logging In to the Web Page

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

Invalid syntax error - Microsoft Internet Explorer													
File	Edit	View	Favorites	Tools	; He	Þ							
G) Back	• 🕤) - 🗙	2		🔎 Search	☆ Favorites	Ø	8-	2	2	1	**
Addre	ess 🧉	http:19	2.168.1.1										

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

GOLDWEB Happily Connecting	
Language: English 💌 Username: admin	
Password: ••••• Login Cancel	

After clicking Login in the login page, you can log in to the Web page of AP.

After logging in to the Web page, you can view, configure and modify the router settings. In order to make the settings and changes take effect, sometimes, you need to reboot the wireless router.

Caution:

If you are managing the wireless router by Web pages, do not cut off the power supply, otherwise, it may damage the device.

6 Web Configuration

6.1 Setup Wizard

After logging in to the Web page, choose **Setup Wizard** on the left pane of the page to display the **Setup Wizard** page.

Setup Wizard

This wizard is used to configure the wireless routing para	his wizard is used to configure the wireless routing parameters, in order to access the Internet.			
You can set basic network parameters of Internet access To continue, click "Next". Otherwise, click "Exit".	in this wizard.			
	Next	Exit		

You can set the basic network parameters for accessing the Internet by this wizard.

If you are not familiar with this product or do not have much network knowledge,

you can follow the on-screen instructions and complete the settings easily.

If you are an expert in wireless network, you can exit the wizard and set the functions of the wireless router in the corresponding pages.

To continue, click Next.

To exit the wizard, click Exit.

After clicking **Next**, the following page appears.

Setup Wizard	
	I network connection modes. Please select an appropriate one according to the actual situation. If you are not familiar with the the recommended mode is "Auto select".
WAN interface Type:	DHCP (Auto Config)
DHCP Mode	Static Mode (fixed IP) DHCP (Auto Config)
Host Name	PPPOE (ADSL)
	Back Next Cancel

This page provides three types of WAN connection types, including Static Mode

(fixed IP), DHCP (Auto Config), and PPPoE (ADSL).

Note:

If you do not insert the network cable into the WAN interface of the wireless router,

the page above will not appear.

• Static Mode (fixed IP)

If you select the Static Mode (fixed IP), the following page appears.

Setup Wizard		
	s of network connection modes. Please select an appropriate one a er, the recommended mode is "Auto select".	according to the actual situation. If you are not familiar with the
WAN interface Type:	Static Mode (fixed IP)	
Static Mode (fixed IP)		
IP Address	172.16.26.34	
Subnet Mask	255.255.254.0	
Gateway	172.16.26.1	
Primary DNS Server	10.28.100.2	
Secondary DNS Server	10.28.100.7	
	Back Next	Cancel

The parameters in this page are described as follows:

Field	Description
IP Address	Enter the WAN IP address provided by the ISP. It is an
	essential parameter, and you cannot leave it to be blank.
Subnet Mask	Enter the subnet mask provided by the ISP. The subnet
	mask may vary according to the network types. Generally, it
	is set to be 255.255.255.0 (C Cat.)

Field	Description
Gateway	Enter the gateway provided by the ISP.
Primary DNS Server	The ISP usually provides at least one DNS address. If It provides two DNS addresses, enter one of them to the field of Secondary DNS Server .
Secondary DNS Server	Enter the DNS server address provided by the ISP.

• DHCP (Auto Config)

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

Setup Wizard				
	s of network connection modes. Plea er, the recommended mode is "Auto		ine according to the ac	tual situation. If you are not familiar with the
WAN interface Type:	DHCP (Auto C	Config) 💌		
DHCP Mode				
Host Name				
	Back	Next	Cancel	

Note:

In the **Running Status** page, you can view the network parameters assigned by the DHCP server, such as the IP address, subnet mask, gateway, and DNS server address.

• PPPoE (ADSL)

If you select the **PPPoE (ADSL)**, the following page appears.

Setup Wizard

Next

Cancel

The parameters in this page are described as follows:

Back

Field	Description
Username	Enter the user name provided by the ISP.
Password	Enter the password provided by the ISP.
Verify Password	Enter the password again.

After setting the WAN connection type, click Next to display the following page.

Setup Wizard

This wizard is used to configure t	he wireless routing parameters, in order to access the Internet.
SSID	GOLDWEB_B418A0
Mode	11b/g/n mixed mode
Wireless Security Options	Disable wireless security WPA-PSK/WPA2-PSK PSK Key 12345678 (8-63 ASCII characters or 8-64 hexadecimal characters) C Do not modify wireless security settings
	Back Next

The parameters in this page are described as follows:

Field	Description
SSID	The maximum character length for SSID is 32

Field	Description
	characters. The legal characters include letter,
	number, underline or the combination of these
	characters.
Mode	Select a proper network mode from the drop-down list.
	 11b/g mixed mode
	• 11b only
	• 11g only
	• 11b/g/n mixed mode (default)
Mode	
Wireless Security Options	• Disable Wireless Security: Enable or
	disable the wireless security.
	• WPA-PSK/WPA2-PSK PSK Key: Enable
	or disable the encryption function. When
	selecting this option, you need to enter a
	key in the field of WPA-PSK/WPA2-PSK
	PSK Key. An encryption key should
	consist of 8-63 ACSII characters or 8-64
	hexadecimal characters.
	 Do not modify wireless security
	settings: When selecting this option, the
	wireless router will keep the previous

GW-WR150N/GW-WR150ND	150Mbps Wireless Router User Manual

Field	Description
	wireless security settings. If the wireless
	security settings have never been
	modified, after selecting this option, it will
	keep the default wireless security settings.

Note:

All the characters on the keyboard are ASCII code. Hexadecimal characters include

the digits 0-9 and the letters such as A, B, C, and D.

After finishing the wireless settings, click **Next** to display the following page.

Setup Wizard		
der to access the Internet.		
s	order to access the Internet. settings, you can access the internet now.	

Click Finish to complete the wizard settings.

6.2 Running Status

Choose Running Status to display the Running Status page.

Runn		

Wireless Router Running Status		
LAN Interface Status		
MAC Address	00:1F:A4:B4:18:A0	
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Wireless Status		
Enabling Status	Disable	
SSID	GOLDWEB_B418A0	
Channel	9	
Node	11b/g/n	
MAC Address		
WAN		
MAC Address	00:1F:A4:B4:18:A0	
IP Address	172.16.26.34	
Subnet Mask	255.255.254.0	
Gateway	172.16.26.1	
DNS	10.28.100.2 10.28.100.7	
WAN Interface Traffic Statistics		
Received/Transmitted Bytes	104318/12030	
Packets	1357	
Running Time	9 mins, 53 secs	

This page displays the information about current running status of the wireless router, including the information about LAN, wireless, and WAN interfaces, and the statistical information of the WAN interface.

6.3 Network Settings

In the **Router** mode, the following figure shows the submenus of the **Network Settings**:

Network Settings	
Operating Mode	
LAN Interface Settings	
WAN Interface Settings	
MAC Address Cloning	

The submenus of Network Settings include Operating Mode, LAN Interface Settings, WAN Interface Settings and MAC Address Cloning.

6.3.1 Operating Mode

Choose **Operating Mode** to display the **Operating Mode** page.

Operating Mode

In this page, you can set up your access to the Internet mode		
C Bridge	Bridge: All Ethernet interfaces and the wireless network interface are connected to a single bridge interface.	
Router	Router: The first Ethernet serves as the WAN interface. Other Ethernet interfaces and the wireless network interface are connected to a single bridge interface, as the LAN interfaces.	
NAT Enabled: Enable Save Cancel		

The AP provides two types of operation modes, including **Bridge** and **Router**. The parameters in this page are described as follows:

Mode	Description
Bridge	In the Bridge mode, the AP acts as a hub.
Router	In the Router mode, the AP allows routing between WAN and
	LAN, or WAN and wireless network.
NAT	This function can only be used only in the Router mode. After
Enabled	NAT is enabled, the device can provide address translation

GW-WR150N/GW-WR150ND 150Mbps Wireless Router User Manual

Mode	Description
	between the interior network and the exterior network for LAN
	and wireless network.

After finishing setting, click **Save** to save the settings.

6.3.2 LAN Interface Settings

Choose Network Settings > LAN Interface Settings to display the LAN Interface

Settings page.

LAN Interface Settings

In this page, you can set the basic network parameters of the LAN interface.	
MAC Address	00:1F:A4:B4:18:A0
IP Address	192.168.1.1
Subnet Mask	255.255.255.0 💌
	Save Cancel

In this page, you are allowed to configure the parameters of the LAN interface. If

necessary, you can change the IP address of the LAN interface according to the

actual network environment.

The parameters in this page are described as follows:

Field	Description
MAC Address	Display the MAC address of the LAN interface. It cannot be
	changed.
IP Address	The IP address for the LAN user to access the wireless router.
	The default value is 192.168.1.1. You can change it if
	necessary.

Field	Description
Subnet Mask	The subnet mask that the wireless router provides to the LAN
	user. You can enter a different subnet mask according to the
	actual network status.

After finishing setting, click Save to save the settings.

Note:

- If you have changed the IP address of the LAN interface, you need to enter the new IP address to log in to the Web page, and the default gateways of all the hosts in LAN must be set to be the new IP address, for accessing the Internet.
- The subnet masks of all the hosts in LAN must be set to be the same as the subnet mask in this page.

6.3.3 WAN Interface Settings

Choose Network Settings > WAN Interface Settings to display the WAN Interface Settings page.

WAN Interface Settings

In this page, you can set the basic network parameters of the WAN interface.		
WAN Interface Connection Type	Dynamic IP(DHCP)	
IP Address	Static IP	
Subnet Mask	PPPoE DHCP+	
Gateway	172.16.26.1	
Packet MTU (byte)	1500 (Default: 1500. Do not modify it unless it is necessary.)	
Manually set the DNS server		
DNS Server		
Secondary DNS Server	(Optional)	
	Save Cancel	

This page is used to configure the WAN connection parameters. This page provides 4 types of WAN interface connection types, including **Dynamic IP (DHCP)**, **Static IP**, **PPPoE**, and **DHCP+**. In this page, you may choose the proper WAN interface connection type and configure the parameters related to the connection type.

• Dynamic IP (DHCP)

If you select **Dynamic IP (DHCP)**, the wireless router acquires the network parameters via the WAN interface, such as the IP address, subnet mask, and gateway. If the ISP does not provide any network parameter, please select this WAN interface connection type.

WAN Interface Settings

In this page, you can set the basic network parameters of the WAN interface.		
WAN Interface Connection Type	Dynamic IP(DHCP)	
IP Address	172.16.26.34	
Subnet Mask	255.255.254.0	
Gateway	172.16.26.1	
Packet MTU (byte)	1500 (Default: 1500. Do not modify it unless it is necessary.)	
Manually set the DNS server		
DNS Server		
Secondary DNS Server	(Optional)	
	Save Cancel	

The parameters in this page are described as follows:

Field	Description
WAN Interface Connection Type	Select Dynamic IP (DHCP) in the drop-down list.
IP Address	Display the IP address assigned by the DHCP server.
Subnet Mask	Display the subnet mask assigned by the DHCP server.
Gateway	Display the gateway assigned by the DHCP server.
Packet MTU (byte)	The default value of MTU (Maximum Transmission Unit) is 1500. Usually, do not change the MTU value. You may consult your ISP whether this value needs to be modified.
Manually set the DNS server	Whether to manually set the DNS server.
DNS Server	Displays the DNS server address provided by the ISP. After enabling Manually set the DNS server , you may set at least one DNS server. When connecting, the wireless router will adopt the DNS server that is set manually first.
Secondary DNS Server	Displays the DNS server address provided by the ISP. After enabling Manually set the DNS server , you may enter the second DNS server if necessary.

After finishing setting, click Save to save the settings.

Static IP

If the ISP provides the information of the WAN interface, please select the **Static IP** connection type. If you are not sure of the detailed settings, please consult your ISP.

WAN Interface Settings

In this page, you can set the basic network parameters of the WAN interface.	
WAN Interface Connection Type	Static IP
IP Address	172.16.26.34
Subnet Mask	255.255.254.0
Gateway	172.16.26.1
Packet MTU (byte)	1500 (Default: 1500. Do not modify it unless it is necessary.)
DNS Server	10.28.100.2
Secondary DNS Server	10.28.100.7 (Optional)
	Save Cancel

Fiel	ld	Description
WAN I	nterface	Select Static IP from the drop-down list.
Connectio	n Type	
IP Address	S	Enter the WAN IP address provided by the ISP. You are not
		allowed to leave it to be blank.
Subnet Ma	ask	Enter the WAN subnet mask provided by the ISP. The subnet
		mask may vary according to the network types. Generally, it is
		set to be 255.255.255.0 (C Cat.)
Gateway		Enter the gateway provided by the ISP. It is the IP address for
		connecting the ISP.

Field		Description
Packet	MTU	The default value of MTU (Maximum Transmission Unit) is
(byte)		1500. Usually, do not change the MTU value. You may consult
		your ISP whether this value needs to be modified.
DNS Server		The ISP usually provides at least one DNS address. If It
		provides two DNS addresses, enter one of them to the field of
		Secondary DNS Server.
Secondary	DNS	Enter the DNS server address provided by the ISP.
Server		

After finishing setting, click **Save** to save the settings.

• PPPoE

If the ISP provides the PPPoE connection type, it also provides the username and the password for you to access the Internet.

WAN Interface Settings		
In this page, you can set the basic network parameters of the WAN interface.		
	N Interface inection Type	PPPoE 💌
PPF	PoE Connection:	
Use	ername	pppoe_user
Pas	sword	•••••
Ser	vice Name:	(Optional)
•	Receive ISP's DNS 🔍	Manually enter DNS
DN	S Server	
Sec	ondary DNS Server	(Optional)
Pac	ket MTU (byte)	1500 (Default: 1500. Do not modify it unless it is necessary.)
Sel	ect the appropriate con	inection mode as required:
$^{\circ}$	Connect on Demand	Automatically connect when access traffic is detected
	Auto Disconnect Wait	ting Time 15 min (0 indicates not to automatically disconnect)
$\overline{\bullet}$	C Auto: Automatically establish the connection while the device is rebooting or the connection is disconnected.	
0	C Scheduled: Automatically connect in a specified period	
	Note: When performing the timing connection function, click System Tools>Time Settings to set the current time.	
	Connection Period: F	rom 0 hour 0 minute 23 hour 59 minute
	Need to support the NetSniper	
		Save Cancel

Field	Description
WAN Interface	Select PPPoE from the drop-down list.
Connection Type	
Username	Enter the user name provided by the ISP.
Password	Enter the password provided by the ISP.
Service Name	Specify the PPPoE server name if there are multiple
	PPPoE servers. It is optional.

Field	Description
Receive ISP's DNS/ Manually enter DNS	 Receive ISP's DNS: Enable or disable this function. After enabling this function, the wireless router automatically acquires the DNS server address by the ISP. Manually enter DNS: Enable or disable this function. After enabling this function, you need to enter at least one DNS address.
DNS Server	Enter the DNS server address.
Secondary DNS Server	Enter the DNS server address. (Optional)
Packet (MTU) (byte)	The default value of MTU (Maximum Transmission Unit) is 1500. It is recommended to keep the default MTU value. You may consult your ISP whether this value needs to be modified.
Select the appropriate connection mode as required:	 The wireless router provides 3 types of connection modes. Connect on Demand: After selecting this option, when there is a network access request from LAN, system automatically establishes the network connection. If there is no any network request from LAN during Auto Disconnect Waiting Time, system will automatically disconnect the connection. For the users who pay the network fee according to the on-line time, it is recommended you had better adopt this connection mode, and it can help you to reduce your network fee. Auto: When selecting Auto, system automatically establishes the connection after startup. In the process of operating the wireless router, the network connection will be disconnected for some external reasons, and then system will try to establish the connection succeeds. If your network service is

GW/WR150N/GW/WR150ND	150Mbps Wireless Router User Manual
GW-WRIDUN/GW-WRIDUND	150100ps Wireless Rouler Oser Mariuar

Field	Description
	monthly payment, it is recommended you use this
	connection mode.
	• Scheduled: When selecting Scheduled, you need
	to set the Connection Period first. System will start
	to establish the connection at the specified time and
	end the connection at the specified end time.
	Selecting this option can control the on-line time of
	user in the internal network.
Auto Disconnect Waiting	If there is no any network request from LAN during Auto
Time	Disconnect Waiting Time, the system automatically
	disconnects the connection for protecting your network
	resources. The default value is 15 minutes. When the
	value is set to be 0, it indicates that the connection will
	not be automatically disconnected. You need to set this
	parameter only in the Connect on Demand mode.
Need to support the	Enable or disable the NetSniper function.
NetSniper	The NetSniper can automatically detect the private proxy
	server system or the illegal routers, and control their IP
	packets.

After finishing the settings, click **Save** to save the settings.

• DHCP+

If the ISP provides the DHCP+ connection type, it also provides the username and the password for you to access the Internet.

WAN Interface Settings

In this page, you can set the basic network parameters of the WAN interface.	
WAN Interface Connection Type	DHCP+
Username	usemame
Password	
IP Address	0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Packet MTU (byte)	1500 (Default:1500. Modification is not recommended.)
Authentication Server	218.29.0.228 (Default: 218.29.0.228.)
	Save Cancel

Field	Description
WAN Interface Connection Type	Select DHCP+ from the drop-down list.
Username	Enter the user name provided by the ISP.
Password	Enter the password provided by the ISP.
IP Address	After the connection succeeds in the DHCP+ mode, this filed displays the IP address that is automatically acquired from the DHCP server.
Subnet Mask	After the connection succeeds in the DHCP+ mode, this filed displays the subnet mask that is automatically acquired from the ISP.
Gateway	After the connection succeeds in the DHCP+ mode, this filed displays the gateway that is automatically acquired from the ISP.
DNS Server/Secondary	After the connection succeeds in the DHCP+ mode, this filed displays the DNS server address that is automatically acquired

Field	Description
DNS Server	from the ISP.
Packet (MTU) (byte)	The default value of MTU (Maximum Transmission Unit) is 1500. Usually, do not change the MTU value. You may consult your ISP whether this value needs to be modified.
Authentication Server	Enter the authentication server address for accessing the network provided by the ISP. If you are not sure of the authentication server address, please consult your ISP.

After finishing the settings, click **Save** to save the settings.

6.3.4 MAC Address Cloning

Choose Network Settings > MAC Address Cloning to display the MAC Address Cloning page.

MAC Address Cloning

In this page, you can set the WAN MAC address of the router.		
Enable	Enable 💌	
MAC Address	Fill my MAC address	
Note: This function applies to computers in the LAN only.		
	Save Cancel	

This page is used to configure the WAN MAC address of the wireless router.

Field/Button	Description
Enable	Enable or disable the MAC address cloning.
MAC Address	Display the MAC address of the WAN interface. Some ISPs require user to bind the MAC address, and they will provide a valid MAC address for user. In that case, you need to enter the MAC address in this field. Do not change the

Field/Button	Description
	MAC address, unless the ISP requires you to do so.
Fill my MAC	Click this button to clone the host MAC address to the field of
address	MAC Address. Do not clone the MAC address, unless the
	ISP requires you to do so.

After finishing the settings, click the **Save** button to save the settings.

Note:

The MAC cloning function is only for the hosts in the LAN.

6.4 Wireless Settings

In the router mode, the following figure shows the submenus of the Wireless Settings:

Wireless Settings
Basic Settings
Wireless Security Settings
Wireless MAC Address Filter
Advanced Wireless Settings
Wireless Client List
WPS Settings
WDS Settings

The submenu items of the Wireless Settings are Basic Settings, Wireless

Security Settings, Wireless MAC Address Filter, Advanced Wireless Settings,

Wireless Client List, WPS Settings, and WDS Settings.

6.4.1 Basic Settings

Choose Wireless Settings > Basic Settings to display the Basic Settings page.

Basic Settings

In this page, you can set the basic network parameters of the wireless network of the router.		
Wireless Network		
Wireless Status	wireless disable Display multiple SSID	
SSID1	GOLDWEB_B418A0 Hidden Isolated	
SSID2	Enable 🗆 Hidden 🗖 Isolated 🗖	
SSID3	Enable 🗆 Hidden 🗖 Isolated 🗖	
SSID4	Enable 🗆 Hidden 🗖 Isolated 🗖	
Mode	11b/g/n mixed mode	
Channel	AutoSelect	
Broadcast Network Name (SSID)	€ Enable C Disable	
SSID internal isolation	C Enable @ Disable	
MBSSID AP Isolation	C Enable @ Disable	
BSSID		
Frequency Bandwidth	C 20 © 20/40	
MCS	Auto	
	Save Cancel	

This page is used to configure the wireless basic parameters.

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

Field	Description		
Wireless Status	Enable or disable the wireless function.		
Display multiple SSID	If it is selected, all SSIDs fields are displayed. If it is not selected, only SSID1 is displayed.		
SSID1-4	The maximum entry length of SSID is 32-character. The legal characters include letter, number, underline or the combination of these characters. The default SSID is NEXUS . You can select to enable, hide, or isolate an SSID by selecting the corresponding check box next to the specific SSID.		
Mode	 Select a proper network mode from the drop-down list. 11b/g mixed mode 11b only 11g only 11b/g/n mixed mode (default) 		
Channel	Select a proper channel from the drop-down list. The default channel is AutoSelect .		
Broadcast Network Name (SSID)	Whether to broadcast SSID. After enabling this function, the wireless router will broadcast its SSID, and the wireless client can scan the SSID.		
SSID internal isolation	Enable or disable the isolation among AP clients. If this function is enabled, the client terminals that connect to the same AP cannot communicate with 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 with each other.		
BSSID	Display the MAC address of the wireless interface.		
Frequency Bandwidth	You may select 20 or 20/40.		
MCS	You may select the MCS value from 0 to 7. The default MCS is Auto .		

After finishing the settings, click the **Save** button to save the settings.

6.4.2 Wireless Security Settings

Choose Wireless Settings > Wireless Security Settings to display the Wireless

Security Settings page.

Wireless Security Settings			
In this page, you can set the security parameters of a wireless network.			
Select SSID			
SSID	GOLDWEB_B418A0		
GOLDWEB_B418A0			
Security Mode	Disable Disable Open Shared WEPAUTO WPA-Enterprise WPA2-PSK WPA2-PSK WPA2-PSK WPA2-PSK WPA2-PSK WPA2-Enterprise Dynamic WEP 802.1X	Cancel	

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

Select SSID

Select SSID	
SSID	GOLDWEB_B418A0 -

SSID: Select a SSID that you want to configure.

• Security Mode

This page provides 10 types of security 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.

- Open Mode

GOLDWEB_B418A0				
Security Mode	Open	•		
Wire Equivalence Protection (WEP)				
Default Key	Key 1 💌			
WEP Keys	WEP Key 1:		Hex 💌	
	WEP Key 2 :		Hex 💌	
	WEP Key 3 :		Hex 💌	
	WEP Key 4 :		Hex 💌	
	Save	Cancel		

The parameters of Open mode are described as follows:

Field	Description
Security	Select the Open mode in the drop-down list.
Mode	
Default Key	Select a key as the default key.
WEP Keys	Set 64-bit or 128-bit key. The key format is Hex or ASCII.
(WEP	
Key1/2/3/4)	

Note:

When selecting the Hex format, you need to set 5-bit or 13-bit hex characters as the WEP key. Hex characters include the digits (0-9), and the letters (A-Z). When selecting the ASCII format, the WEP key should be set to be 10-bit or 26-bit ASCII

characters.

- Shared Mode

GOLDWEB_B418A0				
Security Mode	Shared	•		
	WEP -			
Wire Equivalence Protection (WEP)				
Default Key	Key 1 💌			
WEP Keys	WEP Key 1:		Hex 💌	
	WEP Key 2 :		Hex 💌	
	WEP Key 3 :		Hex	
	WEP Key 4 :		Hex	
	Save	Cancel		

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

Field	Description
Security	Select the Shared mode in the drop-down list. The
Mode	Shared mode only supports WEP.
Default Key	Select a key as the default key.
WEP Keys	Set 64-bit or 128-bit key. The key format is Hex or ASCII.
(WEP	
Key1/2/3/4)	

- WEPAUTO Mode

GOLDWEB_B418A0			
Security Mode	WEPAUTO	•	
Wire Equivalence Prote	ection (WEP)		
Default Key	Key 1 💌		
	WEP Key 1:		Hex
WED Keine	WEP Key 2 :		Hex 💌
WEP Keys	WEP Key 3 :		Hex 💌
	WEP Key 4 :		Hex 💌
	Save	Cancel	

The parameter description of WEPAUTO mode, please refer to the Open mode.

- WPA-Enterprise Mode

GOLDWEB_B418A0			
Security Mode	WPA-Enterprise	•	
WPA			
WPA Algorithms	O TKIP O AES		
Key Renewal Interval	3600	seconds	
Radius Server			
IP Address	0		
Port	1812		
Shared Secret			
Session Timeout	0		
Idle Timeout	0		
	Save		Cancel

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

Field	Description
Security	Select the WPA-Enterprise in the drop-down list.
Mode	

Field	Description
WPA	You may select TKIP or AES .
Algorithms	
Key	Set the key renewal interval. The value 0 indicates that
Renewal	system does not renew the key.
Interval	
IP Address	Enter the IP address of the RADIUS server. RADIUS
	server is used to authenticate the hosts in the wireless
	network.
Port	The port number that the RADIUS server uses. The
	default port number is 1812. You may change it according
	to the server setting.
Shared	Set the shared key for accessing the RADIUS server.
Secret	
Session	If this value is 0, it indicates that there is no session time
Timeout	limit.
Idle Timeout	Set the idle timeout.

- WPA-PSK Mode

GOLDWEB_B418A0			
Security Mode	WPA-PSK	-	
WPA			
WPA Algorithms	O TKIP O AES		
Pass Phrase	12345678		
Key Renewal Interval	3600	seconds	
	Save		Cancel

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

Field	Description	
Security	Select the WPA-PSK mode in the drop-down list.	

Field	Description
Mode	
WPA	Select TKIP or AES.
Algorithms	
Pass	Set 8-bit to 64-bit key in ASCII characters.
Phrase	
Key	Set the key renewal interval. The value 0 indicates that
Renewal	system does not renew the key.
Interval	

- WPA2-Enterprise Mode

GOLDWEB_B418A0		
Security Mode	WPA2-Enterprise	•
WPA		
WPA Algorithms	O TKIP O AES	C TKIP+AES
Key Renewal Interval	3600	seconds
PMK Cache Period	10	minute
Pre-Authentication	Disable O En	nable
Radius Server		
IP Address	0	
Port	1812	
Shared Secret		
Session Timeout	0	
	0	_

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

Field	Description
Security Mode	Select the WPA2-Enterprise in the drop-down list.
WPA Algorithms	You may select TKIP, AES, or TKIP+AES.
Key Renewal	Set the key renewal interval. The value 0 indicates

Field	Description
Interval	that system does not renew the key.
PMK Cache	Set the PMK (Pairwise Master Key) cache period.
Period	PMK scheme allows the roaming users that pass
	through the 802.11X/EAP handshake protocol to
	roam to the previous AP again. PMK can decrease
	the roaming delay and improve the roaming speed.
Pre-Authentication	Enable or disable pre-authentication.
IP Address	Enter the IP address of the RADIUS server. RADIUS
	server is used to authenticate the hosts in the
	wireless network.
Port	The port number that the RADIUS server uses. The
	default port number is 1812. You may change it
	according to the server setting.
Shared Secret	Set the shared key for accessing the RADIUS
	server.
Session Timeout	If this value is 0, it indicates that there is no session
	time limit.
Idle Timeout	Set the idle timeout.

- WPA2-PSK Mode

GOLDWEB_B418A0			
Security Mode	WPA2-PSK	•	
WPA			
WPA Algorithms	O TKIP O AES	C TKIP+AES	
Pass Phrase	12345678		
Key Renewal Interval	3600	seconds	
	Save		Cancel

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

Field	Description
Security	Select the WPA2-PSK in the drop-down list.
Mode	
WPA	You may select TKIP, AES, or TKIP+AES.
Algorithms	
Pass Phrase	Set 8-bit to 64-bit key in ASCII characters.
Key Renewal	Set the key renewal interval. The value 0 indicates that
Interval	system does not renew the key.

- WPA-PSK/WPA2-PSK Mode

GOLDWEB_B418A0		
Security Mode	WPA-PSK/WPA2-PSK	
WPA		
WPA Algorithms	CITKIP CIAES CITKIP+AES	
Pass Phrase	12345678	
Key Renewal Interval	3600 seconds	
	Save Cancel	

The parameter description of **WPA-PSK/WPA2-PSK** mode, please refer to the **WPA2-PSK** mode.

- WPA/WPA2-Enterprise Mode

GOLDWEB_B418A0		
Security Mode	WPA/WPA2-Enterprise	
WPA		
WPA Algorithms	O TKIP O AES O TKIP+AES	
Key Renewal Interval	3600 seconds	
Radius Server		
IP Address	0	
Port	1812	
Shared Secret		
Session Timeout	0	
Idle Timeout	0	
	Save Cancel	

The parameters of WPA/WPA2-Enterprise mode are described as follows:

Field	Description
Security Mode	Select the WPA/WPA2-Enterprise in the drop-down
	list.
WPA Algorithms	You may select TKIP, AES, or TKIP+AES.
Key Renewal	Set the key renewal interval. The value 0 indicates
Interval	that system does not renew the key.
IP Address	Enter the IP address of the RADIUS server. RADIUS
	server is used to authenticate the hosts in the
	wireless network.
Port	The port number that the RADIUS server uses. The
	default port number is 1812. You may change it
	according to the server setting.
Shared Secret	Set the shared key for accessing the RADIUS
	server.
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

GOLDWEB_B418A0		
Security Mode	Dynamic WEP 802.1X	
Radius Server		
IP Address	0	
Port	1812	
Shared Secret		
Session Timeout	0	
Idle Timeout	0	
	Save Cancel	

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

Field	Description
Security Mode	Select the Dynamic WEP 802.1X in the drop-down
	list.
IP Address	Enter the IP address of the RADIUS server. RADIUS
	server is used to authenticate the hosts in the
	wireless network.
Port	The port number that the RADIUS server uses. The
	default port number is 1812. You may change it
	according to the server setting.
Shared Secret	Set the shared key for accessing the RADIUS
	server.
Session Timeout	If this value is 0, it indicates that there is no session
	time limit.
Idle Timeout	Set the idle timeout.

Note:

In order to connect to the wireless router successfully, the wireless settings (e.g.

SSID) and the security settings (e.g. encryption key) of the hosts in the wireless network should be consistent with that of the wireless router.

6.4.3 Wireless MAC Address Filter

The wireless MAC address filtering function is used to allow or reject the hosts in the wireless network to access the WAN, for controlling the on-line permission of the users in the wireless network.

Choose Wireless Settings > Wireless MAC Address Filter to display the Wireless MAC Address Filtering page.

Wireless MAC Address Filtering

In this page, you can set MAC address filtering to control the access of computers to the wireless network.		
Access Policy		
Policy	Disable 💌	
Add MAC	Allow	
	Reject	
	Save Cancel	
MAC Address List		
NO.	MAC Address	
	Delete	

This page is used to allow or reject the wireless clients to access the wireless network of the wireless router.

Field	Description
Policy	The filtering policies include Disable, Allow, and Reject.
	Disable: Disable the wireless MAC address filtering
	function.
	Allow: Allow the wireless clients with the MAC addresses in

Field	Description
	the MAC Address List to access the wireless network of
	the wireless router.
	• Reject : Reject the wireless clients with the MAC addresses
	in the MAC Address List to access the wireless network of
	the wireless router.
Add MAC	Add a MAC address of the wireless client.

After finishing the settings, click the **Save** button to save the settings.

6.4.4 Advanced Wireless Settings

Choose Wireless Settings > Advanced Wireless Settings to display the Advanced Wireless Settings page.

Advanced Wireless Settings

In this page, you can set the advanced settings of the wireless network.

Advanced Wireless paramet	ers
BG Protection Mode	Auto 💌
Beacon Interval	100 ms (range 20 - 999, default 100)
DTIM (Delivery Traffic Indication Message)	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	100 (range 1 - 100, default 100)
Short Preamble	C Enable C Disable
Pkt_Aggregate	C Enable C Disable
DFS RDRegion	ETSI(1-13)
WMM Bandwidth Manageme	nt
WMM Capable	C Enable C Disable
APSD Capability	C Enable
DLS Capable	C Enable C Disable
WMM Parameters	WMM Configuration
Multicast-to-Unicast Convert	er
Multicast-to-Unicast	C Enable C Disable
	Save Cancel

This page allows you to configure the advanced wireless settings.

• Parameter Description

Field	Description
BG Protection Mode	You may select On , Off , or Auto . The default BG protection

Field	Description
	mode is Auto .
Beacon Interval	By default, wireless beacon signal sends data to station
	every other 100 ms. The range is 20~999.
DTIM (Delivery Traffic Indication Message)	The default DTIM is 1ms. The range is 1~255.
Fragment Threshold	Set the fragmentation threshold. Packets larger than the
	size set in this field will be fragmented. Too many data
	packets will lower the wireless network performance. The
	Fragment Threshold value should not be set too low. The
	default value is 2346.
RTS Threshold	Set the RTS (Request to send threshold.) threshold. When
	the packet size is large than the preset RTS size, the
	wireless router will send a RTS to the destination station to
	start negotiation. When receiving the RTS frame, the
	wireless station will send back a CTS frame to the wireless
	router, to indicate that they can communicate with each
	other. The default value is 2347.
TX Power	Set the Tx power of the wireless router. The default value is
	100. The value 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 the

Field	Description
	wireless devices. Short preamble adopts 56-bit synchronization field. The network whose 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.
Pkt_Aggregate	Enable or disable the Pkt_Aggregate function. Pkt_Aggregate can aggregate multiple data packets together for improving the transmission efficiency.
DFS RDRegion	Set the register region. Different register regions limit the ranges of different frequency.
WMM capable	Enable or disable WMM. After enabling WMM, the wireless router can process different types of wireless data according to their priority levels.
APSD Capability	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	After enabling this function, the transmission quality of the wireless multicast stream can be improved.

After finishing the settings, click the **Save** button to save the settings.

Note:

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

WMM Configuration

WMM Access Categories

At present, WMM defines traffic into 4 access categories.

Access Category	Description	802.1d Tags
WMM Voice Priority	Highest priority	7,6
	Allows multiple concurrent VoIP calls, with low latency and toll voice quality	
WMM Video Priority	Prioritize video traffic above other data traffic	5, 4
	One 802.11g or 802.11a channel can support 3-4 SDTV streams or 1 HDTV streams	
WMM Best Effort Priority	Traffic from legacy devices, or traffic from applications or devices that lack QoS capabilities	0, 3
	Traffic less sensitive to latency, but affected by long delays, such as Internet surfing	
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).

- Setting the WMM Parameters

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

Aifsn 3 7 1	CWMin 15 • 15 •	63	Max	Txop	-			Policy
7	15 💌	-	_	0	-			_
		102						
1	7 _		3 💌	0				
	7 💌	15	•	94				
1	3 💌	7	•	47				
Aifsn	CW	/Min	CV	VMax		Тхор		ACM
3	15	-	1023 💌			0		
7	15	-	1023 💌			0		
2	7	•	1	5 💌		94		
2	3	3 🔻		•	47			
Apply		Can	cel		Clos	e		
	Aifsn 3 7 2 2	1 3 Aifsn CW 3 15 7 15 2 7 2 3	1 3 ▼ 7 Aifsn CWMin 3 15 ▼ 7 15 ▼ 2 7 ▼ 2 3 ▼	1 3 7 Aifsn CWMin CV 3 15 102 7 15 102 2 7 11 2 3 7	1 3 7 47 Aifsn CWMin CWMax 3 15 1023 7 15 1023 2 7 15 2 3 7	1 3 7 47 Alfsn CWMin CWMax 3 15 1023 7 15 1023 2 7 15	1 3 7 47 Aifsn CWMin CWMax Txop 3 15 1023 0 7 15 1023 0 2 7 15 94 2 3 7 47	1 3 7 47 Alfsn CWMin CWMax Txop 3 15 1023 0 7 15 1023 0 2 7 15 94 2 3 7 47

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

Note:

The wireless router provides the standard WMM settings. If you want to modify the parameters above, please refer to the WMM settings of your WMM products.

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)
Тхор	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

GW-WR150N/GW-WR150ND 150Mbps Wireless Router User Manual

Field	Description
	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.

Note:

Usually, you do not need to modify the WMM parameters.

• DLS (Direct Link Setup) Configuration

The wireless router 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 wireless router. 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 wireless router.
- Step2 Enable the DLS function in the Advanced Wireless Settings page of the wireless router.

Advanced Wireless Settings

In this page, you can set the advanced settings of the wireless network.

Advanced Wireless paramet	ers
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
DTIM (Delivery Traffic Indication Message)	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	100 (range 1 - 100, default 100)
Short Preamble	C Enable C Disable
Pkt_Aggregate	
DFS RDRegion	ETSI(1-13)
WMM Bandwidth Manageme	nt
WMM Capable	€ Enable C Disable
APSD Capability	C Enable
DLS Capable	C Disable
WMM Parameters	WMM Configuration
Multicast-to-Unicast Convert	er
Multicast-to-Unicast	C Enable
	Save Cancel

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

🔀 RaUI														
	ofile	Letwork	Adv	anced	S	tatist	ics	Qos WMM		Ø WPS	Radi	on/off	About	>
WMM Setup	p Status													_
w/	MM >> Enat	led	Por	wer Save	>> Dis	abled					Direct L	ink >> Enable	d	
	WAMA	Enable												
	v	/MM · Power Sa	ve Enabl	e										
	[AC_BK		AC_BE			AC_VI		AC_VO					
	0	irect Link Setu	ip Enable]										
		NAC Address >	00 1	18 6e	39	ca	81	Timeout	t Value >>	60	sec			
												Ap	ply	
												Tear	Down	
												rear		
														-

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

🔀 RaUI														
	Profile	Letwork	Adva) inced	St	tatisti	cs	Goe WM	,	Ø WPS	Rad	io on/off	About	•
WMM	Setup Status	abled	Pow	er Save :	>> Disa	abled					Direct I	.ink >> Enable	d	
		M Enable												
		WMM - Power Sav	e Enable											
		AC_BK		AC_BE			AC_VI		AC_VO					
		Direct Link Setup	Enable											
		MAC Address >>	00 18	6e	39	ca	81	Time	out Value >:	60	sec			
	(00-1E-E3-00-	61-8A					60				Ар	xly	
												Tear	Down	
														-

6.4.5 Wireless Client List

Choose Wireless Settings > Wireless Client List to display the Wireless Client List page.

Wireless Client list									
In this page, You can check the wireless clients connected to this device									
Wireless Network	Wireless Network								
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC		

In this page, you can view the information of the clients that access the wireless router.

6.4.6 WPS Settings

Choose Wireless Settings > WPS Settings to display the Wi-Fi Protected Setup (WPS) page.

Wi-Fi Protected Setup (WPS)

By entering a personal identification number (PIN) or pressing the button (PBC) to the implemente the Wi-Fi protected setting, enabling you to build secure mechanisms more easily.

WPS Settings Configuration	
WPS settings:	Enable 🔻
	Save
WPS settings list	
WPS Current Status:	Idle
The Configured WPS:	Yes
WPS SSID:	GOLDWEB_B418A0
WPS authentication mode:	Open
WPS encryption type:	None
The Default Key Index of WPS:	1
WPS Key(ASCII)	
PIN(personal identification number):	18027846 Generate Pin
	OOB
WPS mode settings	
WPS mode:	© PIN O PBC
Personal identification number (PIN)	
	Save
WPS setting status	
WSC:Idle	<u>~</u>

In this page, you can configure the WPS settings.

• WPS Settings Configuration

WPS Settings Configuration	
WPS settings:	Enable 💌
	Save

WPS settings: Enable or disable the WPS.

After enabling WPS, you can configure the parameters related to WPS.

WPS Settings List

WPS settings list	
WPS Current Status:	Idle
The Configured WPS:	Yes
WPS SSID:	GOLDWEB_B418A0
WPS authentication mode:	Open
WPS encryption type:	None
The Default Key Index of WPS:	1
WPS Key(ASCII)	
PIN(personal identification number):	18027846 Generate Pin
	OOB

WPS settings list displays the preset WPS information, such as WPS current status, WPS authentication mode, and WPS encryption type.

Click the **OOB** button in the **Wi-Fi Protected Setup (WPS)** page, system displays the WPS default settings. See the following figure:

WPS settings list	
WPS Current Status:	Idle
The Configured WPS:	No
WPS SSID:	default_B418A0
WPS authentication mode:	Open
WPS encryption type:	None
The Default Key Index of WPS:	1
WPS Key(ASCII)	
PIN(personal identification number):	18027846 Generate Pin
	OOB

• WPS Mode Settings

WPS mode settings		
WPS mode:	● PIN C PBC	
Personal identification number (PIN)		
	Save	

WPS modes include PIN and PBC. For more details, please refer to WPS Application.

• WPS Setting Status

WPS setting status	
WSC;Idle	

The figure above displays WPS current status.

• WPS Application

This page provides two WPS modes, including PIN and PBC modes.

At present, WPS supports three types of operation modes, including **Enrollee** mode, **Registrar** mode, and **PBC** mode. **Enrollee** and **Registrar** modes need to apply PIN code negotiation.

- Enrollee Mode

- Step 1 Select the enrollee mode on the wireless client, the software of wireless client will generate a random PIN code, for example, 12345678.
- Step 2 In the **Wi-Fi Protected Setup (WPS)** page, enter the PIN code of wireless client, for example, 12345678.
- Step 3 Click the **Save** button in the **Wi-Fi Protected Setup (WPS)** page to submit the setting.

WPS mode settings	
WPS mode:	● PIN C PBC
Personal identification number (PIN)	12345678
	Save

- Registrar Mode
- Step 1 View the AP PIN in the **Wi-Fi Protected Setup (WPS)** page, for example, 31668729.

WPS settings list	
WPS Current Status:	Idle
The Configured WPS:	Yes
WPS SSID:	GOLDWEB_B418A0
WPS authentication mode:	Open
WPS encryption type:	None
The Default Key Index of WPS:	1
WPS Key(ASCII)	
PIN(personal identification number):	31668729 Generate Pin
	OOB

Step 2 Select the **Registrar** mode on the wireless client and enter the PIN code of the wireless router. See the following figure:

	Rescan Information Pin Code
WPS Profile List	Information
ExRegNW277000	31668729 Renew
-	Registrar 💌
۲ <u>۲</u>	Connect
PIN WPS Associate IE Progress >> 0%	Rotate
PBC WPS Probe IE WPS status is disconnected	Disconnect
Auto	Export Profile

- PBC Mode
- Step 1 In the **Wi-Fi Protected Setup (WPS)** page, select the **PBC** mode, and then click the **Save** button. You may press the **WPS** button on the rear panel.

WPS mode settings	
WPS mode:	
	Save

Step 2 Enable the PBC function on the wireless client. In that case, the wireless router and wireless client will automatically establish connection.

6.4.7 WDS Settings

Wireless Distribution System (WDS) is a system that enables the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required. The notable advantage of WDS over other solutions is that it preserves the MAC addresses of client packets across links between access points.

Choose Wireless Settings > WDS Settings to display the Wireless Distribution

System (WDS) page.

Wireless Distribution System(WDS)

Wireless Distribution System allows you to make a completely wireless infrastructure. The WDS feature allows the access points to be wirelessly connected. Normally used in large, open areas where pulling a wire is restricted or not cost effective and in residential circumstances.

basic wds Settings			
WDS Mode	Disable Disable Lazy Mode Bridge Mode Repeater Mode	Cancel	
	Repeater Mode		

This page provides three types of WDS modes, including Lazy Mode, Bridge Mode, and Repeater Mode. You may also disable WDS.

- Lazy Mode
- Parameter Description

Wireless Distribution System(WDS)

Wireless Distribution System allows you to make a completely wireless infrastructure. The WDS feature allows the access points to be wirelessly connected. Normally used in large, open areas where pulling a wire is restricted or not cost effective and in residential circumstances.

basic wds Settings				
WDS Mode	Lazy Mode	•		
Entity Model	ССК 💌			
WDS 1				
Encryption Type	NONE	•		
Encryption key				
WDS 2				
Encryption Type	NONE	•		
Encryption key				
WDS 3				
Encryption Type	NONE	•		
Encryption key				
WDS 4				
Encryption Type	NONE	•		
Encryption key				
	Save		Cano	cel

The parameters of Lazy Mode are described as follows:

Field	Description
WDS Mode	Select the Lazy Mode in the drop-down list.
Entity Model	The physical modes in the drop-down list include CCK,
	OFDM, and HTMIX
Encryption	The encryption types you can select include NONE, WEP
Туре	64bits, WEP 128bits, WPA-PSK (TKIP), and WPA2-PSK
	(AES).
Encryption	Set the encryption key.
Key	

• Lazy Mode Configuration

In the lazy mode, the wireless router automatically connects to the WDS devices that use the same SSID, channel, encryption mode, and the physical mode. You do not need to manually enter other MAC addresses of the peer routers.

To configure the Lazy Mode, do as follows:

- Step 1 In the Wireless Distribution System (WDS) page, set the WDS mode to be Lazy Mode, and set the entity model and encryption type to accord with the peer router (A router that needs to connect to the this wireless router by WDS). After finishing the settings, click the Save button to save the settings. The wireless router will work in the Lazy mode.
- Step 2 Enter the **Wireless Security Settings** page, and set the security mode of the wireless router to accord with the peer router.

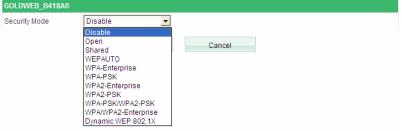
Wireless Security Settings

In this page, you can set the security parameters of a wireless network.

Select SSID

SSID

GOLDWEB_B418A0



- Bridge Mode
- Parameter Description

Wireless Distribution System(WDS)

Wireless Distribution System allows you to make a completely wireless infrastructure. The WDS feature allows the access points to be wirelessly connected. Normally used in large, open areas where pulling a wire is restricted or not cost effective and in residential circumstances.

basic wds Settings			
WDS Mode	Bridge Mode		
Entity Model	ССК 💌		
WDS 1			
Encryption Type	NONE	•	
Encryption key			
Wireless Access Node MAC Address			
WDS 2			
Encryption Type	NONE	•	
Encryption key			
Wireless Access Node MAC Address			
WDS 3			
Encryption Type	NONE	-	
Encryption key			
Wireless Access Node MAC Address			
WDS 4			
Encryption Type	NONE	-	
Encryption key			
Wireless Access Node MAC Address			
	Save		Cancel

The parameters of Bridge Mode are described as follows:

Field	Description
WDS Mode	Select the Bridge Mode in the drop-down list.
Entity Model	The physical modes in the drop-down list include CCK,
	OFDM, and HTMIX.

Field	Description	
Encryption Type	The encryption types you can select include NONE, WEP	
	64bits, WEP 128bits, WPA-PSK (TKIP), and WPA2-PSK	
	(AES).	
Encryption Key	Set the encryption key.	
Wireless Access	The MAC address of another wireless router that	
Node MAC	connects to this wireless router by WDS.	
Address		

GW-WR150N/GW-WR150ND 150Mbps Wireless Router User Manual

Bridge Mode Configuration

In the bridge mode, you can use the wireless router to connect to other routers, 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 wireless router.

- Step 1 In the Wireless Distribution System (WDS) page, select the WDS mode to be Bridge Mode. Set the entity model and encryption type to accord with the peer router, and then enter the MAC address of the peer router. After finishing the settings, click the save button to save the settings. The wireless router will work in the Bridge mode.
- Step 2 Choose Wireless Settings > Wireless Security Settings to display the Wireless Security Settings page. Set the security mode of the wireless router to accord with the peer router.

Wireless Security Settings

In this page, you can se	et the security parameters of a wireless network.
Select SSID	
SSID	GOLDWEB_B418A0
GOLDWEB_B418A0	
Security Mode	Disable Disable Open Shared WEPAUTO WPA-Enterprise WPA2-Enterprise WPA2-PSK WPA2-PSK WPA2-PSK WPAPSKWPA2-PSK WPAWPA2-Enterprise Dynamic WEP 802.1X

- Repeater Mode
- Parameter Description

Wireless Distribution System(WDS)

Wireless Distribution System allows you to make a completely wireless infrastructure. The WDS feature allows the access points to be wirelessly connected. Normally used in large, open areas where pulling a wire is restricted or not cost effective and in residential circumstances.

basic wds Settings				
WDS Mode	Repeater Mode 💌			
Entity Model	ССК 🔻			
WDS 1				
Encryption Type	NONE	-		
Encryption key]	
Wireless Access Node MAC Address				
WDS 2				
Encryption Type	NONE	r		
Encryption key]	
Wireless Access Node MAC Address				
WDS 3				l
Encryption Type	NONE	•		
Encryption key				
Wireless Access Node MAC Address				
WDS 4				
Encryption Type	NONE	-		
Encryption key				
Wireless Access Node MAC Address				
	Save		Cancel	1

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

- Repeater Mode Configuration

In the Repeater mode, you can use the wireless router to connect to the primary

router, for extending the wireless coverage.

Step 1 Choose Wireless Settings > Basic Settings to display the Basic Settings page.

Basic Settings

In this page, you can set the basic network parameters of the wireless network of the router.			
Wireless Network			
Wireless Status	wireless disable Display multiple SSID		
SSID1	default_B418A0 Hidden 🗆 Isolated 🗆		
Mode	11b/g/n mixed mode		
Channel	AutoSelect		
Broadcast Network Name (SSID)	AutoSelect 1 Disable 2		
SSID internal isolation	3 4 Disable		
MBSSID AP Isolation	5 Disable 6		
BSSID	7		
Frequency Bandwidth	8 9 0		
MCS	10		
	12 13 Save Cancel		

- Step 2 In this page, set the channel of the wireless router to accord with the peer router.
- Step 3 In the Wireless Distribution System (WDS) page, set the WDS mode to be Repeater Mode, set the entity model and encryption type to accord with the peer router, and then enter the MAC address of the peer AP. After finishing the settings, click the Save button to save the settings. The wireless router will work in the Repeater mode.
- Step 4 Choose Wireless Settings > Wireless Security Settings to display the Wireless Security Settings page.

Wireless Security Settings

In this page, you can set the security parameters of a wireless network.			
Select SSID			
SSID	GOLDWEB_B418A0 -		
GOLDWEB_B418A0			
Security Mode	Disable Disable Open Shared WEPAUTO WPA-Enterprise WPA2-PSK WPA2-PSK WPA2-PSK WPA2-PSK WPAWPA2-Enterprise Dynamic WEP 802.1X		

Step 5 In this page, set the security mode of the wireless router to accord with the peer router.

Note:

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

Note:

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

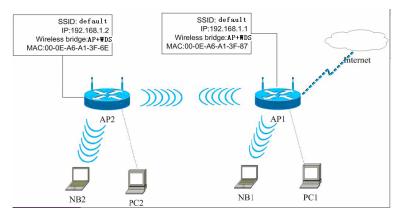
Do not set all the WDS APs to be **Lazy Mode**, please ensure that at least one WDS AP acts as Root Bridge and enter the MAC address of the wireless router to the other routers.

For better compatibility, please try to adopt the products with the same model to connect to the wireless router.

• Establishing a Network by WDS Bridge Mode

GW-WR150N/GW-WR150ND 150Mbps Wireless Router User Manual The following description shows how to use the WDS bridge mode 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, and 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	₩DS 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

- Configuring AP1

Step 1 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.

Step 2 In the Wireless Distribution System (WDS) page, set the WDS mode to be Bridge Mode, and enter the MAC address of the AP2.

Wireless Distribution System(WDS)

Wireless Distribution System allows you to make a completely wireless infrastructure. The WDS feature allows the access points to be wirelessly connected. Normally used in large, open areas where pulling a wire is restricted or not cost effective and in residential circumstances.

basic wds Settings			
WDS Mode	Bridge Mode 💌		
Entity Model	CCK -		
WDS 1			
Encryption Type	NONE		
Encryption key			
Wireless Access Node MAC Address	00:0E:A6:A1:3F:6E		

Step 3 Choose wireless Settings > Basic Settings to display the Basic Settings page. In this page, set the SSID of AP1. AP1 and AP2 must use the same SSID and channel.

Basic Settings

In this page, you can set the basic network parameters of the wireless network of the router.

Wireless Network	
Wireless Status	wireless enable Display multiple SSID
SSID1	default Hidden 🗆 Isolated 🗆
Mode	11b/g/n mixed mode
Channel	6
Broadcast Network Name (SSID)	€ Enable C Disable
SSID internal isolation	C Enable
MBSSID AP Isolation	C Enable C Disable
BSSID	00:1F:A4:B4:18:A0
Frequency Bandwidth	C 20 @ 20/40
MCS	Auto
Extension Channel	2 💌
	Save Cancel

Step 4 Enter the **Wireless Security Settings** page, and disable the security mode.

Wireless Security Settings

In this page, you can set the security parameters of a wireless network.			
Select SSID			
SSID	GOLDWEB_B418A0 -		
GOLDWEB_B418A0			
Security Mode	Disable Disable Open Shared WEPAUTO WPA-Enterprise WPA2-PSK WPA2-PSK WPA2-PSK WPA2-PSK WPAWPA2-Enterprise Dynamic WEP 802.1X		

Step 5 Choose Network Settings > LAN Interface Settings to display the LAN Interface Settings page. Set the IP address of AP1 to be 192.168.1.1 and then click the Save button to save the settings.

LAN Interface Settings

In this page, you can set the basic network parameters of the LAN interface.				
MAC Address	00:0E:A6:A1:3F:87			
IP Address	192.168.1.1			
Subnet Mask 255.255.255.0 -				
	_	Save	Cancel	

- Configuring AP2

Step 1 Choose Network Settings > LAN Interface Settings to display the LAN Interface Settings page. Set the IP address of AP2 to be 192.168.1.2.

LAN Interface Settings

In this page, you can set the basic network parameters of the LAN interface.			
MAC Address	00:0E:A6:A1:3F:6E		
IP Address	192.168.1.2		
Subnet Mask	255.255.255.0 💌		
	Save Cancel		

Step 2 In the **Wireless Distribution System (WDS)** page, set the WDS mode to be the **Bridge Mode** and enter the MAC address of the AP1. Then click the **Save** button to save the settings.

Wireless Distribution System(WDS)

Wireless Distribution System allows you to make a completely wireless infrastructure. The WDS feature allows the access points to be wirelessly connected. Normally used in large, open areas where pulling a wire is restricted or not cost effective and in residential circumstances.			
basic wds Settings			
WDC Mode	Pridee Hade		

WDS Mode	Bridge Mode
Entity Model	ССК •
WDS 1	
Encryption Type	NONE
Encryption key	
Wireless Access Node MAC Address	00:0E:A6:A1:3F:87

6.5 DHCP Server

The following figure shows the submenus of the DHCP Server.

DHCP Server
DHCP Service
Static Address Allocation
DHCP client list

The submenus of the DHCP Server include DHCP Service, Static Address Allocation, and DHCP client list.

6.5.1 DHCP Service

The built-in DHCP server can automatically assign the network parameters such as the IP address, to the hosts in the LAN. User does not need to manually set the IP address, subnet mask, gateway, and DNS server.

Choose DHCP Server > DHCP Service to display the DHCP Service page.

DHCP Service

Each PC's protocol that can be automatically assigned by the built-in DHCP server of the wireless router in the TCP/IP network.			
DHCP Server	C Disable @ Enable		
Start Address of Address Pool	192.168.1.2		
End Address of Address Pool	192.168.1.254		
Lease Time	86400 sec(The default value is 864 00)		
GateWay	192.168.1.1 (Optional)		
Primary DNS Server	192.168.1.1 (Optional)		
Secondary DNS Server	192.168.1.1 (Optional)		
	Save Cancel		

This page is used to configure the DHCP server.

The parameters in this page are described as follows:

Field	Description			
	•			
DHCP Server	Enable or disable the DHCP server. When disabling the DHCP			
	server, you do not need to set the other parameters in this			
	page.			
Start Address of	The starting IP address that the DHCP server automatically			
Address Pool	assigns to the hosts in the LAN.			
End Address of	The end IP address that the DHCP server automatically assigns			
Address Pool	to the hosts in the LAN.			
Lease Time	The lease time is the valid time of the IP address that the DHCP			
	server assigns to the hosts. During the valid period of the IP			
	address, the DHSP server will not assign this IP address to			
	other hosts.			
Gateway	Enter the IP address of the LAN interface. The default gateway			
	is 192.168.1.1. It is optional.			
Primary DNS	Enter the primary DNS server address (optional). If you are not			
Server	sure of the DNS server address, please consult your ISP.			
Secondary DNS	Enter the Secondary DNS server address (optional). If you are			
Server	not sure of the DNS server address, please consult your ISP.			

After finishing setting, click the Save button to save the settings.

Note:

If you want to use the DHCP function of the wireless router, you need to set the **Internet Protocol (TCP/IP)** to be **Obtain an IP address automatically**.

6.5.2 Static Address Allocation

The static address allocation function of the wireless router can reserve the static IP addresses for the computers with the specific MAC addresses. When a computer whose MAC address is in the allocation table of static address requests the DHCP server for an IP address, the DHCP server assigns the reserved IP address to the computer.

Choose DHCP Server > Static Address Allocation to display the Static Address

Allocation page.

Static Address Allocation

In this page, you can set static address allocation of the DHCP server.(Max rule number 10)					
Set rules	Set rules				
	IP Address				
	MAC Address	(eg XX:XX:XX:XX:XX:XX)			
	Save	Cancel			
NO.	IP Address	MAC Address	Delete		
Delete					

The paramters in this page are described as follows:

Filed	Description
IP Address	Set the IP address that is reserved for a
	host on the LAN side.
MAC Address	Enter the MAC address of the host on
	the LAN side.

After finishing setting, click the Save button to save the settings.

6.5.3 DHCP Client List

Choose DHCP Server > DHCP Client list to display the DHCP Clients list page.

DHCP Clients list					
In this page, you can view all DHCP clients information.					
Host Name	MAC Address	IP Address	Lease Time		
Refresh					

In this page, you can view all the network information of the hosts assigned by the

DHCP server in the LAN, such as the host name, MAC address, and IP address.

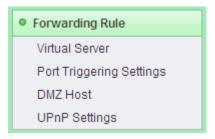
Click the **Refresh** button to refresh the client list.

The parameters in this page are described as follows:

Field	Description
Host Name	Display the host name.
MAC Address	Display the MAC address of the host.
IP Address	Display the IP address assigned by the DHCP server.
Lease Time	Display the lease time of the IP address. Before the lease time of
	the IP address is over, the client software will automatically apply
	for the lease time.

6.6 Forwarding Rule

The following figure shows the submenus of the Forwarding Rule.



The submenus of the Forwarding Rule include Virtual Server, Port Triggering Settings, DMZ Host, and UPnP Settings.

6.6.1 Virtual Server

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

Choose Forwarding Rule > Virtual Server to display the Virtual Server page.

Virtual Server

Virtual server defines the mapping between the WAN service port and LAN network server. All access to the WAN service port is redirected to the LAN network server with a specified IP address.

Virtual Server	Setting			
Virtual Server S	etting Disable 💌			
IP Address]		
Port Range	-			
Protocol	TCP&UDP 💌			
Comment		(Max rule number 10)		
		Save	Cancel	
NO.	IP Address	Port Range	Protocol	Comment
		Delete		

In this page, you are allowed to add or delete a virtual server.

The parameters of Virtual Server are described as follows:

Field	Description
Virtual Server Setting	Enable or disable the virtual server settings.
IP Address	Enter the IP address of the host that provides
	virtual service in the LAN.
Port Range	Set the service port range that the wireless
	router provides to the WAN. The WAN user
	acquires the service via the port. The port
	range format is "the starting port - the end
	port".
Protocol	Select the protocol for the virtual service. You
	may select TCP, UDP or TCP&UDP.
Comment	Enter the comment about the virtual server.

After finishing setting, click the Save button to save the settings.

6.6.2 Port Triggering Settings

Some applications need multiple connections, such as network game, video conference, and IP phone. Because of firewall, these applications cannot work under simple NAT mode, but port forwarding can realize that. When an application generates a connection to the triggered port, all the corresponding ports will be opened, for establishing connection and providing service.

Choose Forwarding Rule > Port Triggering Settings to display the Port Triggering Settings page.

Port Triggering Settings

Some applications require that specific ports in the Router's firewall be opened for access by remote parties. A maximum 10 entries can be configured.								
	Application	1	Trigger			Open		
serial numbers	Name protocol		Port range			Portr	Port range	
		protocol	Start	end	protocol	Start	end	
That have options to:								
Increase the application of rules								
increase the application of rules								

In this page, you are allowed to view the preset rules, add or delete a rule, and enable or disable a selected rule.

Click the **Increase the application of rules** button to display the following page.

Port Triggering Settings

Some applications require that specific ports in the Router's firewall be opened for access by remote parties. A maximum 10 entries can be configured.

	Application	Trigger		Open			
serial numbers	Name	protocol	Port range		a rata a al	Port range	
			Start	end	protocol	Start	end
That have options to:		Enable Disable Delete reset					

Increase the application of rules

Application Name:			
œ	Please select one of Applications	Select One	
0	Custom application name:		

Start Trigger Port	End Trigger Port	Trigger Protocol	A range of ports can be opened from after Trigger	A range of ports can be opened to after Trigger	Open ports Protocol
		TCP			TCP 💌
		TCP			TCP 💌
		TCP 💌			TCP 💌
		TCP 💌			TCP 🔻
		TCP			TCP 💌
		TCP			TCP 💌
		TCP			TCP 💌
		TCP			TCP 🔻
		Save/Apply	Cancel		

The parameters in this page are described as follows:

Field	Description		
Application Nome	It provides two options according to the		
Application Name	added rules.		

Field	Description
	 Please select one of applications: If you select one of applications in the drop-down list, system will automatically configure the Start Trigger Port, End Trigger Port, Trigger Protocol and so on. Custom application name: if you select this option, you need to manually set the parameters such as the Start Trigger Port, End Trigger Port, End Trigger Port, and Open Ports Protocol.
Start Trigger Port	The start port number that LAN user uses to trigger the open port.
End Trigger Port	The end port number that LAN user uses to trigger the open port.
Trigger Protocol	Select the application protocol. You may select TCP/UDP, TCP, or UDP.
A range of ports can be opened from after Trigger	The start port number that is opened to WAN.
A range of ports can be opened to after Trigger	The end port number that is opened to WAN.
Open ports Protocol	Select the proper protocol that is opened to WAN. You may select TCP/UDP, TCP, or UDP.

After finishing setting, click the **Save/Apply** button to save and apply the settings.

6.6.3 DMZ Host

DMZ allows all the ports of a PC in 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 and the host can realize bidirectional limitless communication with the Internet users and servers.

Choose Forwarding Rule > DMZ Host to display the DMZ Host page.

DMZ Host

In this page, you can configure the DMZ host in your computer				
DMZ				
DMZ Status	Disable -			
IP Address of the DMZ Host				
Save	Cancel			

The parameters of DMZ Host are described as follows:

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

After finishing the settings, click the **save** button to save the settings.

6.6.4 UPnP Settings

The hosts can generate the request for port conversion via the UPnP (Universal Plug and Play) protocol, so that the external hosts can access the resources on the internal hosts. For example, MSN Messenger on Windows ME and Windows XP systems can make use of the UPnP protocol to make the limited NAT function back to normal when using audio and video call.

Choose Forwarding Rule > UPnP Settings to display the UPnP Settings page.

UPnP Settings

In th	In this page, you can choose whether to open the UPnP function					
UPnl	Status: Disable 💌	Save				
UPnP Settings List						
ID	Application Remarks	External Port	Protocol Type	Internal Port	IP Address	Status

This page is used to enable or disable the UPnP settings, view the preset the UPnP rules, and delete the selected rules.

Note:

Only when the applications support UPnP protocol, can you use this function.

UPnP function needs operation system support such as Windows ME, Windows XP, and Windows Vista, and application software support.

6.7 Security Options

The following figure shows the submenus of the Security Options.



The submenus of the Security Options include Security Settings, Advanced Security Settings, LAN Web Management, and Remote Web Management.

6.7.1 Security Settings

Choose Security Options > Security Settings to display the Security Settings page.

Secu	ritv	Settir	nas
occu		ocun	'gu

In this page, you can set to enable or disable each basic security option.			
SPI(Stateful Packet Ins	SPI(Stateful Packet Inspection)		
SPI Firewall	C Enable @ Disable		
Virtual Private Network	(VPN)		
PPTP Pass-through	• Enable C Disable		
L2TP Pass-through			
IPSec Pass-through			
Application Layer Gateway (ALG)			
FTP ALG	Enable C Disable		
SIP ALG			
	Save Cancel		

In this page, you are allowed to set Stateful Packet Inspection (SPI), Virtual Private

Network (VPN), and Application Layer Gateway (ALG).

The parameters in this page are described as follows:

Field	Description
Stateful Packet	When the SPI firewall is enabled, only the users in the internal
Inspection (SPI)	network generate the requests, and then the connection is
	established. In addition, all the requests from the external network
	will be rejected by the SPI firewall.
	When the SPI firewall is disabled, all the requests form the internal
	network and external network can generate the connections,
	which will make the hosts in the internal network be exposed to
	the external network. Therefore, disabling the SPI firewall will
	cause the security problem.
	It is recommended you enable the SPI firewall.

Field	Description
Virtual Private	VPN provides the secure communication method for the remote
Network (VPN)	computers via the WAN. If the hosts in the internal network need
	to use the VPN protocols such as PPTP, L2TP, and IPSec to
	connect to the remote VPN network, you should enable the
	corresponding passthrough function.
Application	ALG provides network address and port conversion for some
Layer Gateway	application layer protocols such as FTP, and SIP that adopt
(ALG)	"control/data" mode when passing through the NAT gateway. It is
	recommended you enable the ALG functions.

After finishing setting, click the **Save** button to save the settings.

6.7.2 Advanced Security Settings

The goal of DoS (Denial of service) attack is using a large quantity of illusive information to exhaust the resources of the destination host. The destination host is forced to process the illusive traffic, which affects the processing of the legal traffic. If the DoS attack is from the multiple source addresses, it is also called DDoS (Distribution Denial of service) attack. Generally, all the source addresses of the DoS attack are fraudulent.

Choose Security Options > Advanced Security Settings to display the Advanced Security Settings page.

Advanced Security Settings

In this page, you can set the advanced options of security protection. (The right threshold min is 50)		
Anti DoS Attack	C Disable 🕫 Enable	
Enable filtering ICMP-FLOOD attack		
ICMP-FLOOD Packet Threshold (5-3600)	packets/s	
Enable filtering UDP-FLOOD attack		
UDP-FLOOD Packet Threshold (5-3600)	packets/s	
Enable filtering TCP-SYN-FLOOD attack		
TCP-SYN-FLOOD Packet Threshold (5-3600)	packets/s	
Deny the PING packet from the WAN interface		
Save	Cancel	

In this page, you are allowed to set the advanced options of security protection.

In this page, you should enable the Anti DoS Attack first, and then you are allowed

to set the parameters in this page.

The parameters in this page are described as follows:

Field	Description
Anti DoS Attack	Enable or disable the anti DoS attack. After enabling this
	function, you are allowed to set the following options.
Enable filtering	Enable or disable filtering ICMP-FLOOD attack.
ICMP-FLOOD	
attack	
ICMP-FLOOD	After enabling the filtering ICMP-FLOOD attack, if the ICMP
Packet Threshold (5-3600)	packet number reaches the preset threshold value in the
(0-0000)	specified interval, the measure for preventing ICMP-FLOOD
	takes effect.

C\M_\MP150N/C\M_\MP150ND	150Mbps Wireless Router User Manual
GW-WRIDUN/GW-WRIDUND	100100000 WITELESS ROULET USET Martual

Field	Description
Enable filtering UDP-FLOOD attack	Enable or disable filtering UDP-FLOOD attack.
UDP-FLOOD Packet Threshold (5-3600)	After enabling the filtering UDP -FLOOD attack, if the UDP packet number reaches the specified threshold value in the specified interval, the measure for preventing UDP -FLOOD takes effect.
Enable filtering TCP-SYN-FLOOD attack	Enable or disable filtering TCP-SYN-FLOOD attack.
TCP-SYN-FLOOD Packet Threshold (5-3600)	After enabling the filtering TCP-SYN-FLOOD attack, if the TCP-SYN packet number reaches the specified threshold value in the specified interval, the measure for preventing TCP-SYN-FLOOD takes effect.
Deny the PING packet from the WAN interface	After enabling this function, the computers in the WAN cannot PING through the wireless router.

After finishing setting, click the **Save** button to save and apply the settings.

6.7.3 LAN Web Management

Choose Security Options > LAN Web Management to display the LAN Web Management page.

LAN Web Management

© Allow all hosts in the LAN to access the Web management page			
	address in the list to access the Web management page		
< Allow only wate	address in the list to access the web management page		
MAC Address 1			
MAC Address 2			
MAC Address 3			
MAC Address 4			
	Save Cancel		

In this page, you can set whether the hosts in the LAN are allowed to access the

Web management page.

The parameters in this page are described as follows:

Parameter	Description
Allow all hosts in the LAN to access the	Whether allow all hosts in the LAN to
Web management page	access the Web management page
Allow only MAC addresses in the list to	Whether allow only MAC addresses in
access the Web management page	the list to access the Web management
	page. After enabling this function, add
	the MAC addresses to the list.
MAC Address1, 2, 3, 4	Enter the MAC address in the fields of
	MAC Address1, 2, 3, 4.

After finishing setting, click the **Save** button to save and apply the settings.

Note:

If you select the option "Allow only MAC addresses in the list to access the Web

management page", but not add the MAC Address of management PC to the list, you will not be able to manage the wireless router via the current PC after clicking the **Save** button. In that case, if you want to manage the wireless router again, please press the **Reset** button of the wireless router to restore the factory default settings.

6.7.4 Remote Web Management

Choose Security Options > Remote Web Management to display the Remote Web Management page.

Remote Web Management

In this page, you can set the Web management port of the router and the IP address of the computer in the WAN.		
Enable Remote Web Management:		
Web Management Port:	80	
IP Address of Remote Web Management:	255.255.255.255	
	Save Cancel	

In this page, you can set whether the users are allowed to manage the wireless router remotely via the WAN. This feature allows you to perform the management tasks from the remote hosts.

The parameters in this page are described as follows:

Field	Description
Enable Remote	Enable or disable remote Web management.
Web Management	
Web Management	The Web management port for accessing the Web page of the
Port	wireless router.
IP Address of	The IP address of the computer that are allowed to access the
Remote Web	Web page of the wireless router to perform the remote Web
Management	management.

After finishing setting, click the **Save** button to save and apply the settings.

Note:

The default Web management port is 80. If you change the default Web management port, you have to log in to the Web page by "IP address: port". You need to reboot the wireless router to make the settings take effect.

The default IP address for remote management is "0.0.0.0". By default, all the computers in the WAN can not access the Web page of the wireless router to perform the remote Web management. If you change the IP address for remote management, for example, the default IP address is changed to be "202, 96,12,8", only the hosts with the specified IP address (e.g. "202, 96,12,8") are allowed to access the Web page. If you change the IP address for remote management to be "255.255.255.255", in the case, all the hosts in the WAN can access the Web page of the wireless router to perform the remote Web management.

6.8 Access Control

The following figure shows the submenus of the Access Control.



The submenus of the Access Control include MAC/IP/Port Filter Settings, and Web URL Filtering.

6.8.1 MAC/IP/Port Filter Settings

Choose Access Control > MAC/IP/Port Filter Settings to display the MAC/IP/Port Filter Settings page.

MAC/IP/Port filter settings

In th	In this page, You may setup the filter rules, maximum is 10.								
Basi	c Settings								
MAC/IP/Port Filtering Disable 🗸									
Default Policy The packet which don't match with any rules would be:									
Save Cancel									
Current IP/Port Filtering Rules									
No.	Source Mac address	Dest IP Address	Source IP Address	Protocol	Dest. Port Range	Src Port Range	Action	Comment	Time
Others would be accepted -						-			
Delete Selected Cancel									

In this page, you are allowed to set the MAC/IP/Port Filtering rules and vierw the preset rules.

The paramters in this page are described as follows:

Field	Description		
MAC/IP/Port	Enable or disable MAC/IP/Port filtering. The default setting is		
Filtering	Disable.		
Default Policy	• Accepted: When selecting this option, the wireless router wi		
	accept all the packets that do not match any rule.		
	• Dropped: When selecting this option, the wireless router will		
	reject all the packets that do not match any rule.		

After enabling the MAC/IP/Port filtering, click the Save button to display the

following page for adding a new rule.

IP/Port Filter Settings				
Access Control List	Custom ACL			
Source Mac address				
Dest IP Address				
Source IP Address				
Protocol	•			
Dest. Port Range				
Src Port Range	-			
Comment				
schedule planning(days-week	I All I Monday I Tuesday I Wednesday I Thursday I Friday I Saturday I Sunday			
schedule planning(hour) All Period of time . (HH)				
Action Drop 💌				
Max rule number 10.				
	Save Cancel			
Current IP/Port Filtering Rules				
No. Source Mac De Add	Protocol Action Comment Time			
Others would be accepted -				
	Delete Selected Cancel			

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

The parameters for adding a new rule (e.g. Custom ACL) are described as follows:

Field	Description
Access Control list	Select a filter service in the drop-down list.
Source MAC Address	The MAC addresses included in the data packets.

Field	Description	
Dest IP Address	The destination IP address.	
Source IP Address	The source IP address.	
Protocol	The protocol types of data packets include TCP, UDP, and ICMP.	
Dest Port Range	The destination port range is 1~65535.	
Src Port Range	The source port range is 1~65535.	
Comment	Comment about the rule.	
Schedule Planning (days-week)	Set the day when filter takes effect.	
Schedule Planning (Hour)	Set the time when filter takes effect.	
Action	Enable or disable the rule.	
	• Accept: Enable the rule.	
	• Drop : Disable the rule.	

After finishing setting, click the **Save** button to save and apply the settings.

Note:

When the hosts in the LAN match the MAC address or IP address, the rules of

Custom ACL take effect.

In this page, you can set up to 32 rules.

6.8.2 Web URL Filtering

Choose Access Control > Web URL Filtering to display the Web URL Filtering page.

Web URL Filtering

In this page, you is ten)	I can add or delete URL filtering rules system to restrict access to inappropriate Web page URL(The max
The current sys	tem's website at URL filtering rules:
NO.	URL
	Delete
Add URL filter ru	ules
URL:	
	Add Cancel

Thisp age is used to prevent the LAN users from accessing some Websites in the WAN.

Enter the URL that needs to be filtered and then click the **Add** button to add a new rule.

If you want to delete a rule, select the rule, and then click the **Delete** button to delete the rule.

6.9 Routing Settings

The following figure shows the submenus of the Routing Settings.



The submenu of the Routing Settings only includes Static Routing Table.

6.9.1 Static Routing Table

Static routing is a kind of special routing. Applying the proper static routing rules in network can reduce the problems of routing selection and the overload of data stream, and increase the transport speed of data packets. You can create a routing rule by setting the destination IP address, subnet mask, and gateway. The destination IP address and subnet mask can determine a destination network or a host, and then the wireless router will transmit the data packets to the destination network or the host via the gateway.

Choose Routing Settings > Static Routing Table to display the Static Routing

Table page.

Static Routing Table

Curr	ent Routing table in th	ne system:							
No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	239.255.255.250	255.255.255.255	0.0.0.0	5	0	0	0	br0	
2	192.168.1.0	255.255.255.0	0.0.0.0	1	0	0	0	br0	

In this page, you can add or delete a routing rule, for limiting the LAN users to access some WAN websites.

Click the Add button to display the following page.

Add a routing rule	
Destination	
Host/Net	Host 💌
Gateway	
Interface	LAN
Comment	
	Save Cancel

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

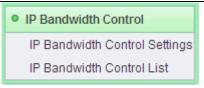
Field	Description
Destination	The destination address of the routing rule.
Host/Net	You may select Host or Net.
Gateway	The IP address that the routing rule passes.
Sub	When the range is Net , you can set this option.
Netmask	
Gateway	The IP address that the routing rule passes.
Interface	The local legal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

After finishing setting, click the Save button to save the settings.

If you want to delete a self-defined rule, select the rule, and then click the **Delete** button to delete the rule.

6.10 IP Bandwidth Control

The following figure shows the submenus of the IP Bandwidth Control.



The submenus of the IP Bandwidth Control include IP Bandwidth Control Settings and IP Bandwidth Control List.

6.10.1 IP Bandwidth Control Settings

Choose IP Bandwidth Control > IP Bandwidth Control Settings to display the IP

Bandwidth Control Settings page.

IP Bandwidth Cont	rol Settings
In this page, you can enable	or disable IP bandwidth control.
Enable IP bandwidth control	
Total Uplink Bandwidth	Kbps
Total Downlink Bandwidth	Kbps
	Save Cancel

After enabling IP bandwidth control, you can set the following parameters.

Field	Description
Enable IP	Enable or disable IP bandwidth control.
bandwidth control	
Total Uplink	Set the total uplink bandwidth.
Bandwidth	
Total Downlink	Set the total downlink bandwidth.
Bandwidth	

After finishing setting, click the **Save** button to save the settings.

Note:

In order to make QoS achieve the best result, please consult your ISP about the total bandwidth of upstream and downstream.

6.10.2 IP Bandwidth Control List

Choose IP Bandwidth Control > IP Bandwidth Control List to display the IP Bandwidth Control List page.

IP Bandwidth Control List

ID	ID Remarks		Uplink Bandwidth (Kbps)			Downlink B	andwidth (Kbps)	Enable		Delete
U			Min	Ma	ах	Min Max		Enable	Edit	Delete
				The li	st is ei	mpty.				
			Ad	d		Delete				
				-						
Add	or edit the IP bandwidth	n control	rules							
•	Enable									
	IP address range			-						
	Protocol	ALL	•							
	Uplink Bandwidth	Min		Kbps	Max		Kbps			
	Downlink Bandwidth	Min		Kbps	Max		Kbps			

In this page, you can view the preset IP bandwidth control rules, add or delete the rules.

The parameters in this page are described as follows:

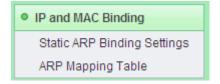
Field	Description
Enable	Enable or disable the rule.
IP address	Enter the address range of the internal hosts. When this field is

Field	Description
range	blank or the value is "0.0.0.0", it indicates this value is invalid.
Protocol	Select the protocol type that the transmission layer adopts. You may select All (match randomly), TCP or UDP in the drop-down list.
Uplink Bandwidth	Set the minimum and maximum uplink bandwidth.
Downlink Bandwidth	Set the minimum and maximum downlink bandwidth.

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

6.11 IP and MAC Binding

The following figure shows the submenus of the IP and MAC Binding.



The submenus of the IP and MAC Binding include Static ARP Binding Settings and ARP Mapping Table.

6.11.1 Static ARP Binding Settings

ARP binding is a valid method for preventing ARP cheating by binding the host IP address and the corresponding MAC address together. Setting the static ARP binding entry can protect the network security of the users in the internal network. When a host sends the ARP request to the wireless router, the wireless router will check the

GW-WR150N/GW-WR150ND 150Mbps Wireless Router User Manual static ARP binding list according to the IP address of the host. If the host MAC address matches the MAC address in the list, the wireless router will accept the request; otherwise, it rejects the request.

Choose IP and MAC Binding > Static ARP Binding Settings to display the Static

ARP Binding Settings page.

Static ARF Binding Settings				
In this page, you can s	et the rule of mapping between the MAC address and IP address of a single computer.			
IP/MAC Binding	C Disable @ Enable			
IP/MAC Binding Settin	gs			
IP Address				
MAC Address				
	Add Cancel			

In this page, you are allowed to enable or disable the IP/MAC binding, and set the IP/MAC binding rule.

The parameters in this page are described as follows:

Field	Description
IP Address	Enter the host IP address for binding.
MAC Address	Enter the MAC address for binding.

After finishing setting, click the Add button to add a new static ARP binding rule.

6.11.2 ARP Mapping Table

Choose IP and MAC Binding > ARP Mapping Table to display the ARP Mapping Table page.

ARP Mapping Table			
In this page, you can set the rules of mapping between MAC addresses and IP addresses of computers.			
MAC address and IP ac	ddress mapping list		
No.	IP Address	Mac Address	
1 🗆	172.36.8.2	09:43:76:A3:46:16	

In this page, you are allowed to view the preset ARP mapping rules or delete the preset rules.

6.12 Dynamic DNS Settings

DDNS is mainly realized the resolution between the fixed DNS and dynamic IP address. For the users using the dynamic IP addresses, when acquiring the new IP addresses after accessing the Internet, the DDNS software will send the IP address to the DDNS server provided by the DDNS provider, and refresh the DDNS database. When other users in the Internet access the DNS, the DDNS server will return the correct IP address.

Choose Dynamic DNS Settings to display the Dynamic DNS Settings page.

Dynamic DNS Settings

In this page, you may configure Dynamic DNS parameters				
Dynamic DNS service settings				
Dynamic DNS service website	Disable			
UserName				
PassWord				
Dynamic DNS service address				
	Save Cancel			

In this page, you are allowed to modify the DDNS settings.

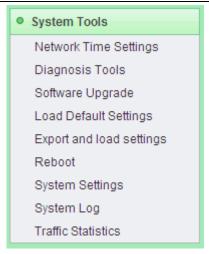
The paramteres in this page are described as follows:

Field	Description
Dynamic DNS	You may select Dyndns.org, freedns.afraid.org,
service website	www.zoneedit.com, and www.no-ip.com in the drop-down list.
UserName	Enter your DDNS username.
Password	Enter your DDNS password.
Dynamic DNS service address	Enter the domain name of the DDNS.

After finishing setting, click the **Save** button to save the settings.

6.13 System Tools

The following figure shows the submenus of the **System Tools**.



The submenus of the System Tools include Network Time Settings, Diagnosis Tools, Software Upgrade, Load Default Settings, Export and load settings, Reboot, System Settings, System Log and Traffic Statistics.

6.13.1 Network Time Settings

Choose System Tools > Network Time Settings to display the Network Time Setting page.

Network Time	Setting		
In this page, you can s	set the network time of system.		
Network Time Setting	1		
Current Time	ent Time Fri Jan 1 03:01:41 UTC 1971 Synchronize with the host		
Time Zone	(GMT+08:00) The coast of China, Hong Kong 🔍		
	192.43.244.18		
Network time server	ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw		
	Save	Cancel	

This page is used to set the network time of the wireless router.

Field	Description		
Current Time	Display the current system time.		
Synchronize with	Click the Synchronize with the host button, and then the		
the host	wireless router can synchronize its time with your PC.		
Time Zone	Select your proper time zone.		
Network time server	Enter the URL of the network time server. After setting the		
	URL of the network time server, the wireless router can		
	synchronize its time with the time server.		

The parameters in this page are described as follows:

After finishing setting, click the **Save** button to save the settings.

6.13.2 Diagnosis Tools

Choose System Tools > Diagnosis Tools to display the Diagnosis Tools page.

Diagnosis Tools

In this page, you can use the PING or Tracert function to diagnose the connection status of the router.

Parameter Settings		
Select	• Ping	O Tracert
IP Address/Domain Name		
Ping Packet Total	4	(1-50)
Ping Packet Size	64	(8-1472)
Ping Timeout	10	(10-100, Unit: seconds)
Tracert Hops	20	(1-30)
Diagnosis Result		
		A
5	Start Diagnos	is Cancel

In this page, you can check the connection status between the wireless router and

other hosts (including the network devices) by $\ensuremath{\mathsf{Ping}}$ or $\ensuremath{\mathsf{Tracert}}$ function.

The parameters in this page are described as follows:

Field	Description
Select	Select Ping or Tracert to check the connection status of the

Field	Description		
	wireless router.		
	• Ping: Ping is used to check whether the wireless router		
	has connected to the host successfully or whether the		
	connection is delayed.		
	• Tracert: Tracert is used to check the number of the		
	routers that the wireless router passed through when		
	connecting to the host.		
IP Address/Domain	The IP address or domain name of the host.		
Name			
Ping Packet Total	The Ping packet number of the Ping operation. The		
	recommended value is 4.		
Ping Packet Size	The Ping packet size of the Ping operation. The		
	recommended value is 64.		
Ping Timeout	Set the Ping timeout. If the preset interval is over, and no		
	echo is sent back, it indicates that the Ping operation fails.		
Tracert Hops	Set the tracert hops. It is the maximum router number		
	between the wireless router and the host.		

After finishing setting, click the **Start Diagnosis** button to save and apply the settings, and the diagnosis result is displayed in the field of **Diagnosis Result**.

6.13.3 Software Upgrade

Choose System Tools > Software Upgrade to display the Software Update page.

Software Update

Upgrade the	Wireless router's Software to obtai	in new functionality.		
Upload the So Please keep p Caution! A cor	oftware will takes about 3 minutes. power on and be patient during upg rrupted image or power broken off (
Software Up	date			
Location: Browse				
		Update		

If you want to update the software of the wireless router, click the **Browse...** button to choose the correct software, and then click the **Update** button. System begins to update the software.

After finishing the updating process, system reboots and automatically enters the Web page.

Note:

Updating the software will make the wireless router return to the factory default settings. In order to avoid the settings loss, please save the settings before updating the software.

During updating, do not cut off the power or press the Reset button.

6.13.4 Load Default Settings

Choose System Tools > Load Default Settings to display the Load default settings page.

Load default settings			
In this page, you can r	In this page, you can reset the router to factory defaults.		
Load default settings			
Load default settings	Load default settings		

In this page, click the **Load default settings** button, and then system returns to the factory default settings.

6.13.5 Export and Load Settings

By exporting the configuration file, you can save the settings of the wireless router to your PC. By backuping the original settings before updating the software, you can avoid data loss of the original settings. You can also load the saved or a new configuration file.

Choose System Tools > Export and Load Settings to display the Export and Load Settings page.

Export and load settings

In this page, you can back up the existing configuration file, you can also load an existing configuration file to change the configuration.

Export Settings	
Export Button	Save

Warning! To upgrade the incorrect configuration file will lose your settings.

Import Settings			
Bet File Locations Browse			
	Save	Cancel	

This page is used to save and load a configuration file. The parameters in this page are described as follows:

Field	Description	
Export Button	Click the Save button to select the path for saving the settings,	

GW-WR150N/GW-WR150ND 150Mbps Wireless Router User Manual

Field	Description	
	and then save the settings to your PC.	
Set File Locations	Click the Browse button to select the settings on your PC, and then click the Save button to load the settings to the wireless router.	

Note:

After loading a new configuration file, the original settings on the wireless router will lose. Therefore, please backup the original settings before loading the new configuration file. If you load the incorrect configuration file, you may import the original settings on your PC.

While loading the configuration file, do not power off the wireless router, otherwise, it may damage the device.

6.13.6 Reboot

Choose System Tools > Reboot to display the Reboot page.



In this page, click the **reboot** button to reboot the wireless router.

6.13.7 System Settings

Choose System Tools > System Settings to display the System Settings page.

System Settings

In this page, you can set the system administrator with the password, network time, Dynamic Domain Name Service.

Account Management		
Account	admin	
Enter the new password		
Re-enter password	•••••	
	Save Cancel	

This page is used to set the administrator password.

Field	Description	
Account	Display the username.	
Enter the new password	Enter the new password.	
Re-enter the new password	Enter the new password again.	

After finishing setting, click the Save button to save the settings.

Note:

If you forget the password, you can press the **Reset** button for 3-6 seconds, and then the wireless router returns to the factory default settings. The default username and the password are **admin**, respectively.

For the sake of the data security, it is strong recommended you change the default username and password.

6.13.8 System Log

Choose System Tools > System Log to display the System Log page.

n this page, you can ch	neck the system log of the device.		
Enable remote System			
Enable remote system			
P Address			
	Save		
Jan 100:	00:05 11AP syslog.info syslogd started: BusyBox v1.12.1 00:05 11AP user.warn kernel: GDMA1_IAC_ADRL: 0x00000000		
	00:05 11AP user.warn kernel: Ralink APSoC Ethernet Driver Initilization. v2.0 64 n/ 00:05 11AP user.warn kernel: GDMA1 MAC ADRH : 0x0000001f		
	00:05 11AP user.warn kernel: GDMA1_MAC_ADRL : 0xa4b418a0		
	00:05 11AP user.alert kernel: PROC INIT OK!		
	00:05 11AP user.info kernel: PPP generic driver version 2.4.2		
	00:05 11AP user.info kernel: PPP BSD Compression module registered		
	00:05 11AP user.info kernel: PPP MPPE Compression module registered 00:05 11AP user.info kernel: NET: Registered protocol family 24		
	00:05 11AP user info kernel: block2mtd: ver		
	00:05 11AP user.info kernel: sion \$Revision: 1.1.1.1 \$		
Jan 100:	00:05 11AP user.warn kernel: Netfilter messages via NETLINK v0.30.		
	00:05 11AP user.warn kernel: ip_conntrack version 2.4 (128 buckets, 1024 max) - 2		
	00:05 11AP user.warn kernel: ip_conntrack_rtsp v0.6.21 loading		
Jan 1 00:00:05 11AP user.debug kernel: net/ipv4/netfilter/ip_conntrack_rtsp.c: init: port #0: 5! Jan 1 00:00:05 11AP user.warn kernel: ip_nat_rtsp.v0.6.21 loading			
Jan 1 00:00:05 TTAP user.warn kernel: ip_riat_itsp v0:0.21 loading Jan 1 00:00:05 TTAP user.warn kernel: ip_conntrack_pptp version 3.1 loaded			
Jan 1 00:00:05 11AP user.warn kernel: ip_contrack_ppp version 3.1 roaded			
	00:05 11AP user.warn kernel: ip_conntrack_l2tp version 3.1 loaded		
Jan 1 00:00:05 11AP user.warn kernel: ip_nat_pptp version 3.0 loaded			
	00:05 11AP user.warn kernel: ip_nat_ipsec loaded		
Jan 1 00:00:05 11AP user.warn kernel: ip_tables: (C) 2000-2006 Netfilter Core Team, Type=			
Jan 1 00:00:05 11AP user.warn kernel: ipt_time loading Jan 1 00:00:05 11AP user.info kernel: TCP cubic registered			
Jan 1 00:00:05 11AP user.warn kernel:>luotao ipport netspy test Driver>			
	00:05 11AP user.info kernel: NETSPY IPPORT proc module 2.1 initialized		
Jan 1 00:00:05 11AP user.info kernel: NET: Registered protocol family 1			
	00:05 11AP user.info kernel: NET: Registered protocol family 17		
	00:05 11AP user.info kernel: 802.1Q VLAN Support v1.8 Ben Greear <greearb@car< td=""></greearb@car<>		
	00:05 11AP user.info kernel: All bugs added by David S. Miller <davem@redhat.cor< td=""></davem@redhat.cor<>		
	00:05 11AP user.warn kernel: VFS: Mounted root (squashfs filesystem) readonly.		
	00:05 11AP user.info kernel: Freeing unused kernel memory: 112k freed 00:05 11AP user.warn kernel: Algorithmics/MIPS FPU Emulator v1.5		
	00:05 11AP user.err kernel: devots: called with bogus options		
4			

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

6.13.9 Traffic Statistics

Choose System Tools > Traffic Statistics to display the Traffic Statistics page.

Traffic Statistics

In this page, you can check the wireless router statistics.

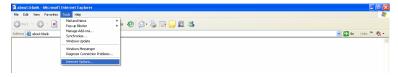
Memory	
Total Memory Capacity:	13900 kB
The remaining amount of memory:	3680 kB
WAN / LAN	
The packet numbers that the wide area network receives:	0
The data amount that the wide area network receives:	0
The packet numbers that the wide area network transmits:	534
The data amount that the wide area network transmits:	317196
The packet numbers that the local area network receives:	8579
The data amount that the Local area network receives:	719774
The packet numbers that the local area network transmits:	12136
The data amount that the local area network transmits:	9568743
All of the interface	
Name	eth2
Rx Packet	14458
Rx Byte	1226944
Tx Packet	18547
Tx Byte	10318445
Name	lo
Rx Packet	0
Rx Byte	0
Tx Packet	0
Tx Byte	0
Name	eth2.1
Rx Packet	8581
Rx Byte	754190

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

7 Troubleshooting

Why the Web page cannot be accessed for configuring the AP?

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



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

Internet Options		
General Security Privacy Content Connections Programs Advanced		
Home page		
Address: about:blank		
Use Current Use Default Use Blank		
Temporary Internet files Pages you view on the Internet are stored in a special folder for quick viewing later.		
Delete Cookies) Delete Files) Settings		
History The History folder contains links to pages you've visited, for quick access to recently viewed pages.		
Days to keep pages in history: 20 📚 Clear History		
Colors Fonts Languages Accessibility		
OK Cancel Apply		

Why the network connection cannot be established?

- Beyond the wireless coverage
 - (1) Place AP near to the client.
 - (2) Try to change the channel setting
- Authentication problem

- (1) Use the cable to connect PC to AP.
- (2) Check the network security setting.
- (3) Try to reset the device by pressing **Reset**.
- Can not search the router.
 - (1) Try to reset the router and test AP again.
 - (2) Check the setting of the wireless network card.
 - (3) Check the SSID and the encryption setting.

Why does wireless Internet access via the device fail?

- (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 base.
- (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 does the Internet access fail?

- (1) Check whether the LEDs status on the ADSL modem and the wireless router 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 router has accessed the Internet.
- (4) Reboot your computer.
- (5) Set the AP 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 router 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:

nternet Options	? 🗙			
General Security Privacy Content Connections	Programs Advanced			
To set up an Internet connection, click Setup.	Setup			
Dial-up and Virtual Private Network settings				
adsl (Default)	Add			
	Remove			
Choose Settings if you need to configure a proxy server for a connection.	Settings			
 Never dial a connection 				
O Dial whenever a network connection is not pres	ent			
 Always dial my default connection 				
Current adsl	Set Default			
LAN Settings do not apply to dial-up connections. LAN Settings Choose Settings above for dial-up settings.				
	· · ·			
Automatic configuration Automatic configuration may override manual se	ttings. To ensure the			
use of manual settings, disable automatic config				
Automatically detect settings				
Use automatic configuration script				
Address				
Proxy server				
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).				
Address: Port: Advanced				
Bypass proxy server for local addresses				
OK Cancel				

Shenzhen Landing Electronics Co.,Ltd Address: 3F Block A,BaiyingBuilding,No.1019 Nanhai Road, Nanshan District,Shenzhen,Guangdong, China Post Code:518067 E-Mail: sales@goldwebcn.com Website: http://www.goldwebcn.com