AN-N20-01

VivoCam Agent Wireless Router

User Manual

Version 0.1

Date: December 05th , 2016

Contents

Overview 3
About this Product 3
Key Features 3
What's in the Box? 4
Package Contents 4
LED Indicators 4
The Real Panel 4
To Be Started 6
System Requirements 6
Operation Mode 6
Connecting as Gateway Mode 6
Connecting as Bridge Mode 7
Connecting as Wireless ISP Mode 8
Quick Setup Wizard 9
Login to the Web Management Interface 9
Setup Wizard for Gateway Mode 9
Setup Wizard for Bridge Mode 12
Setup Wizard for Wireless ISP Mode 13
Wireless Settings 15
Basic Settings 15
Advanced Settings 17
Encryption 19
Access Control 22
Site Survey 24
WPS 26
Schedule 31
TCP/IP Settings 33
LAN Interface 33
WAN Interface 35
Firewall 41
Port Filtering 41
IP Filtering 41
MAC Filtering 42
Port Forwarding 43
URL Filtering 44
DMZ 45

VLAN 46
QoS 47
Route Setup 49
Router Management 51
Current Status 51
Statistics 51
DDNS 52
Time Zone Setting 52
System Log 53
Upgrade Firmware 54
Save/Reload Settings 54
Admin Password 55
Logout 56
Troubleshooting 57
Specifications 58
Glossary 59
Appendix A: TCP/IP Settings 61

Overview

About this Product

This is a wireless router with 2T2R MIMO technology providing an excellent network solution for home, SOHO and hotspot users. It complies with standards IEEE 802.11n with data rate up to 300 Mbps, and IEEE 802.11b/g with maximum data rate of 54 Mbps. It can also interoperate with all the 11/54 Mbps wireless (802.11n/b/g) products.
The router allows multiple users to share one broadband connection, as well as secures your private network. With its built-in five ports switch and wireless AP, LAN users can share files, printers, or playing network games.
To provide a secure wireless network, this router supports wireless data encryption with 64/128-bit WEP, WPA and WPA2. Network Address Translation (NAT) Firewall is also support to shield your communications and network from hackers and wireless eavesdroppers.

Key Features

- Main chip: Realtek RTL8196E-VE3 + RTL8192ER
- Provide one 10/100Mbps Ethernet ports (WAN port)
- Provide four 10/100Mbps Ethernet ports (LAN port)
- Comply with IEEE 802.11n and IEEE802.11b/g wireless standards
- 2.4GHz 2T2R 2T2R frequency band
- High speed transfer rate up to 2.4GHZ 300Mbps
- Support auto-MDI/MDI-X, backpressure and flow control
- Support IEEE802.1x port-based and MAC-based network access control
- Support wireless security for WEP, WPA TKIP and WPA2 AES PSK and pair-wise key authentication services
- Support Static IP, DHCP Client, PPPoE, Firewall and NAT IP Sharing
- Support MAC Clone function
- Support Multiple APs (up to 4 AP SSIDs)
- Support Wireless auto-channel selection
- Support WPS supported in AP and client mode
- Provide 1 x WPS button / 1x RESET button
- Support Auto IP
- Support WPS2.0

What’s in the Box?

Package Contents

Your package contains the following items:

- One Wi-Fi Router
- User Manual

Note:

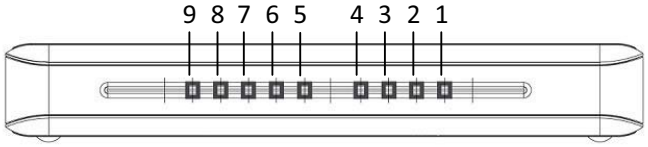
Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor immediately.

Conventions

The router mentioned in this guide stands for W635/W235/CA900-41PA1 without any explanation.

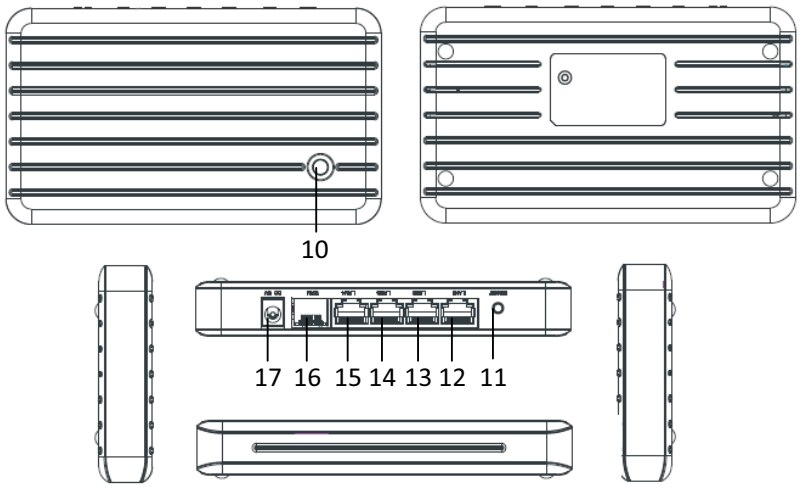
LED Indicators

The front panel of this wireless router contains four status lights as below. You can use the status lights to verify various conditions.



No.	LED	Light Status	Description
1	PWR	Lit	The product is powered on.
		Off	The product is powered off.
2	WPS / RESET	Lit	The reset function is starting.
		Blink	The WPS function is in operation.
		Off	The product is operating normally.
3, 4	2.4G WLAN	Blink	The wireless network band is working.
		Off	The wireless network band isn’t working.
5-8	LAN 1-4	Lit / Blink	A device is linked to the LAN port.
		Flashing	Data is being sent or received over the LAN port.
		Off	No link is detected on the LAN port.
9	WAN	Lit / Blink	A device is linked to the WAN port.
		Flashing	Data is being sent or received over the WAN port.
		Off	No link is detected on the WAN port.

The Real Panel



No.	Name	Description
10	**Reset Button**	Hold down this button for 5 seconds or more to start the reset function.
11	**WPS Button**	Hold down this button for about 1 second to start the WPS function.
12-15	**LAN Port**	The port connects to a modem/router/access point.
16	**WAN Port**	The ports connect to local computers by LAN cables.
17	**DC IN Jack**	The jack connects the power adapter.

To Be Started

System Requirements

- Each computer with a 802.11n/b/g wireless adapter for wireless connection
- Available Internet connection for accessing
- A web browser such as Internet Explorer 5.0 or higher

Operation Mode

This product provides three working modes: Gateway, Bridge and Wireless ISP mode.

- **Gateway Mode**

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

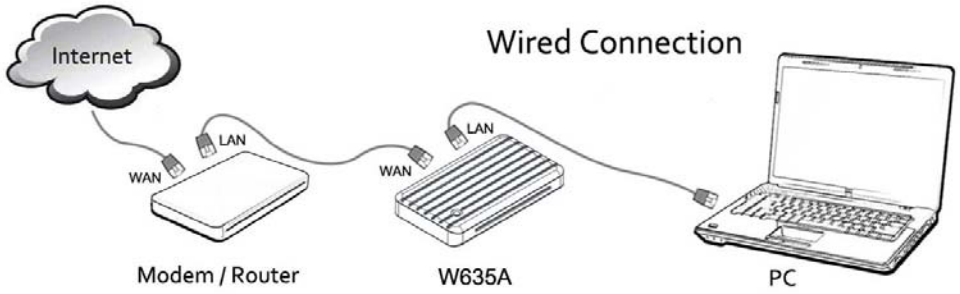
- **Bridge Mode**

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

- **Wireless ISP Mode**

In this mode, all Ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. You can connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Connecting as Gateway Mode



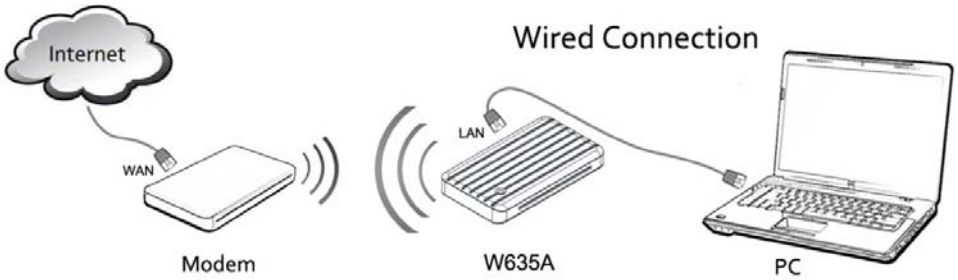
1. Power on the router, and connect your computer to it.
   Wired connection: Connect the router's LAN port to your computer's Ethernet port by a LAN cable.
   Wireless Connection: Connect to the SSID of the router wirelessly by the encryption or WPS.
2. Connect the product's WAN port to the LAN port of the modem or the other router with a LAN cable.
3. The router's default mode is Gateway mode and WAN access type is DHCP client, if you want to change the mode or WAN access type, please set the router following the chapter **Wizard Setup**.

Connecting as Bridge Mode

1. Power on the router, and connect your computer to it by a LAN cable. If the router is already working in Bridge mode, you need to set TCP/IP properties manually on your computer as the steps in **Appendix A: TCP/IP Settings** to connect to the router.

2. Connect the router to the access point following the chapter **Wizard Setup**. When the setup finished, disconnect the LAN connection between the router and computer.

Connecting as Wireless ISP Mode



1. Power on the router, and connect your computer to it.
   Wired connection: Connect the router's LAN port to your computer's Ethernet port by a LAN cable.
   Wireless Connection: Connect to the SSID of the router wirelessly by the encryption or WPS.
2. Power on the wireless modem which can access to Internet.
3. Connect the product to the wireless modem following the chapter **Wizard Setup**.

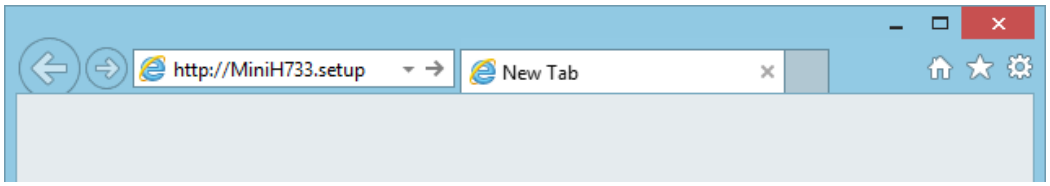
Quick Setup Wizard

The Setup Wizard will help you getting online in several minutes by configuring the basic functions of the wireless router.

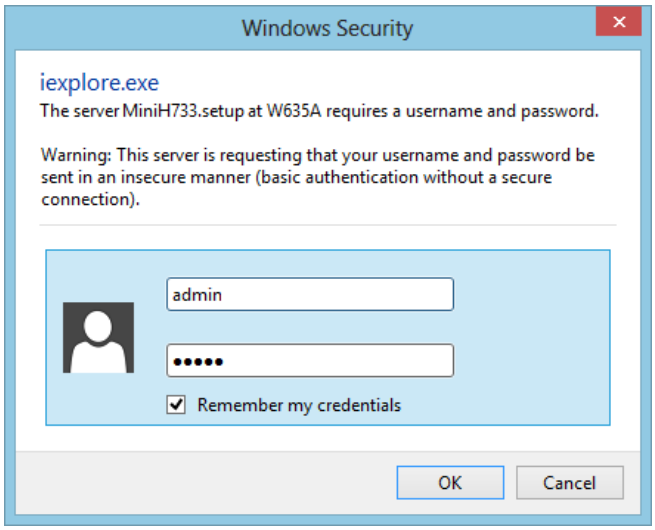
Login to the Web Management Interface

Use a LAN cable to connect a LAN port of router and the Ethernet port of computer, and don't connect the WAN port of router to another router or modem.
If the network is recognized, open a web browser; otherwise you need to set TCP/IP properties manually on your computer as the steps in **Appendix A: TCP/IP Settings**.

Type the URL "http://MiniH733.setup" to access this product's home page.



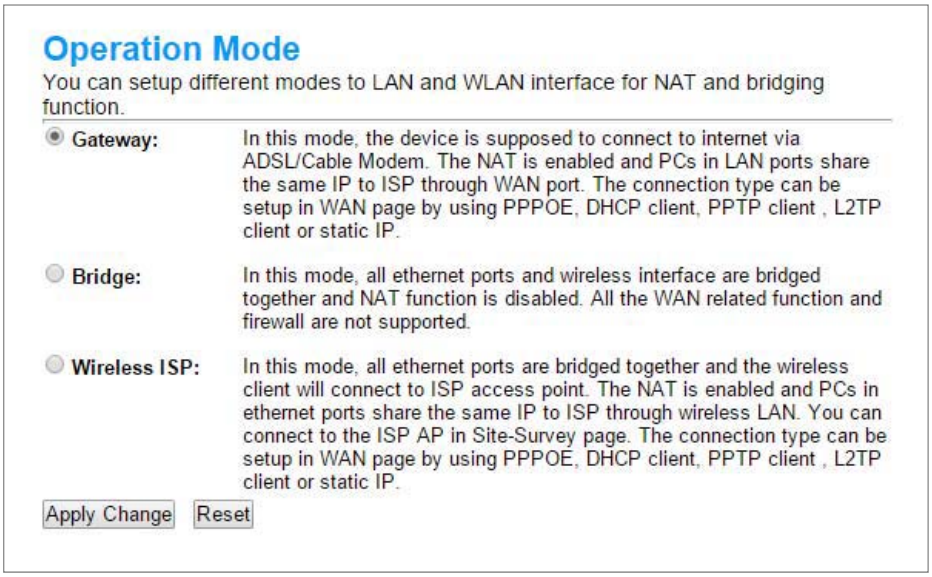
You will see a login window after pressing Enter. Login it with "admin" for both username and password.



Setup Wizard for Gateway Mode

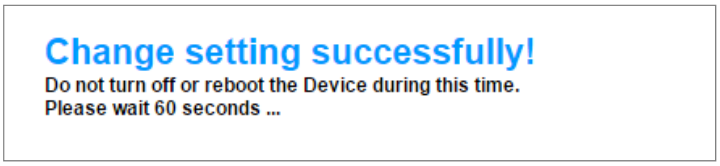
Step 1.

Select "Operation Mode" on the left menu.
Select "Gateway Mode" and click "Apply Change".



Step 2.

Wait 60 seconds for rebooting finished to apply the Gateway mode.

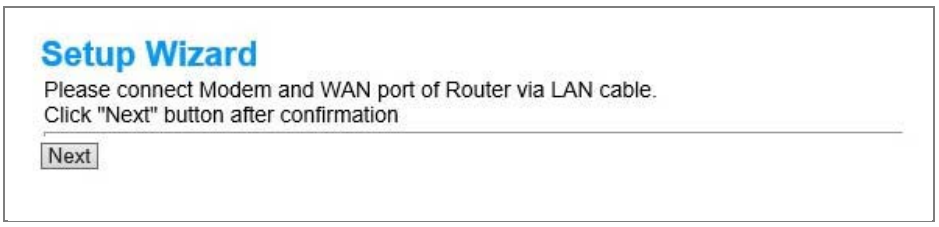


Step 3.

Set the WAN access type following the chapter **WAN Interface**. After set the WAN access type, allow to reboot the router.

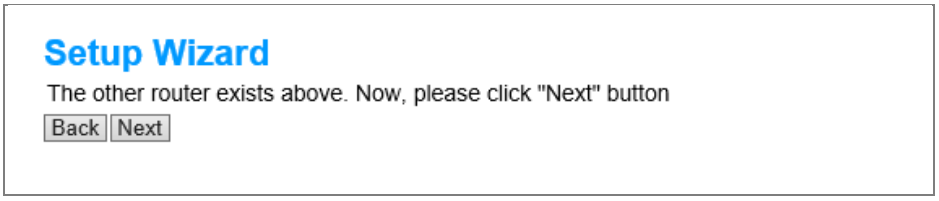
Step 4.

Select “Run Setup Wizard” on the left menu.
Follow the prompt to connect the modem to the WAN port of router, and then click “Next” button.



Step 5.

If the WAN port connection is OK, the prompt will tell you “The other router exists above”, and then you can click “Next”; otherwise the prompt will show error message, you need to check the WAN port connection again.



Step 6.

Wait 40 seconds for confirming the connection.

Step 7.

When the webpage jumps to “Access Point Status” page and WAN IP has been got (See in “WAN Configuration”), the setup is successful.

Wireless Set Up (Router Mode)

Access Point Status

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

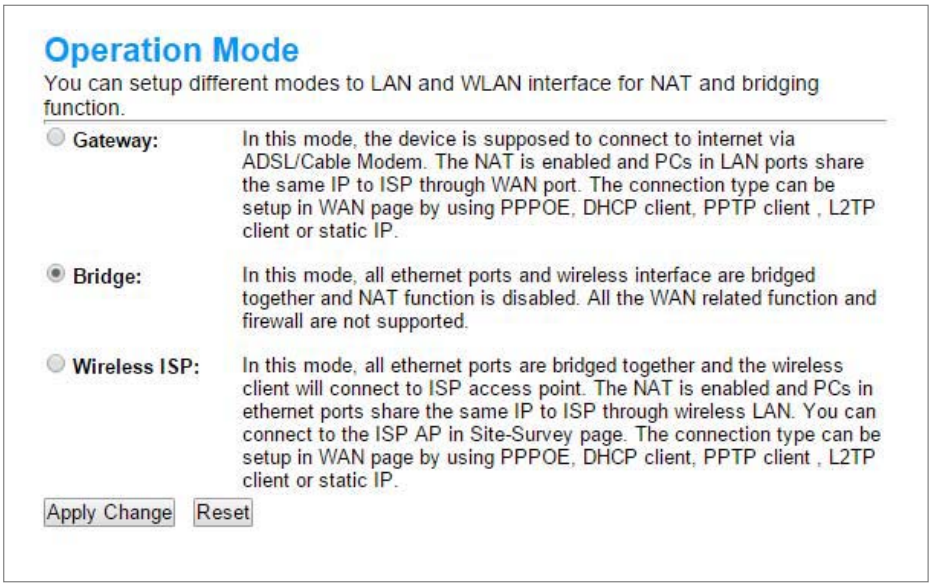
System	
Uptime	0day:0h:3m:8s
Firmware Version	vA.01
Build Time	Tue Oct 20 11:38:36 CST 2015
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	MiniRouter
Channel Number	6
Encryption	Disabled
BSSID	00:e0:4c:81:96:c1
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.100.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.100.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:96:c1
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:96:c9

You can keep the wired connection to router, or connect to the SSID of the router wirelessly by the encryption or WPS on your computer to access to Internet.

Setup Wizard for Bridge Mode

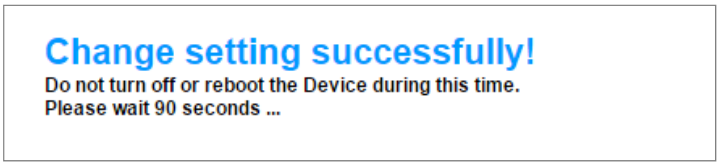
Step 1.

Select “Operation Mode” on the left menu.
Select “Bridge Mode” and click “Apply Change”.



Step 2.

Wait 90 seconds for rebooting finished to apply the Bridge mode.



Step 3.

To connect the router to the access point by a LAN cable, please plug the end of the LAN cable into the WAN port of router.
To connect the router to the access point wirelessly, please following the chapter **Site Survey**.

Step 4.

After connected to the access point, the LAN connection from the router to computer becomes invalid, please disconnect it and finish the setup.
Then you can connect to the SSID of the router wirelessly by the encryption or WPS on your computer to access to Internet.

Setup Wizard for Wireless ISP Mode

Step 1.

Select “Operation Mode” on the left menu.
Select “Wireless ISP Mode” and click “Apply Change”.

- **Mode**

This item is used to select the wireless LAN mode to AP or Client.

- **Network Type**

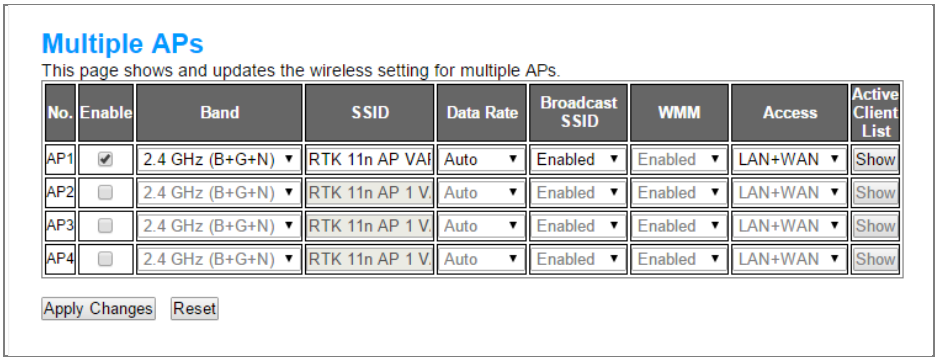
This item is used to select the network type to Infrastructure or Ad-Hoc when the wireless LAN mode is Client.

- **SSID**

SSID is a special name used to identify a wireless network from the other. You need to connect to this product wirelessly by the SSID.
The default SSID of this product is "MiniH7332g-XX" (for 2.4G band, "XX" is the last two characters of product WAN MAC address).
You can set an easily recognizable name no longer than 32 characters.

- **Multiple AP**

This product provides 4 multiple SSIDs for isolating the clients.
Click “MultipleAP” button to enter the settings of AP 1 to 4.



Check the “Enable” box, and then you can configure band, name, data rate, visibility, and access type of the AP.

- **Channel Width**

This option provides 20MHz/40MHz in 2.4GHz band and to 20MHz/40MHz/80MHz in 2.4GHz band select as your channel width.

- **Control Sideband**

This option is used to select upper/lower sideband and it is only available at 40MHz channel width of 2.4GHz band.

- **Channel Number**

Channel number can be manually set to a specific number.
The range of available channel number will be different in different bands.

Band	Range
2.4GHz (20MHz)	1 - 11
2.4GHz (40MHz)	Upper Side: 1-9, Lower Side: 5-11

- **Broadcast SSID**

This function is used to set whether to broadcast the SSID or not. If this option is disabled, the SSID will be hidden. When you want to connect to the hidden SSID, you need to add it manually on your computer.

- **WMM**

WMM function is used to give video/audio data a higher priority than the common data over wireless communications.

- **Data Rate**

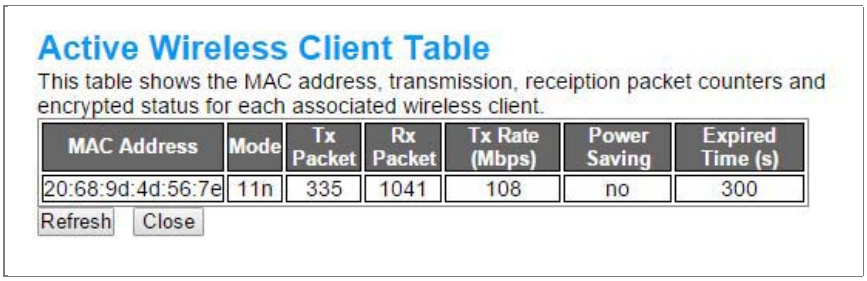
There are various wireless data rate provided for 802.11b/g/n standards.

Band	Data Rate
2.4GHz (B)	1, 2, 5.5, 11Mbps
2.4GHz (G)	6, 9, 12, 18, 24, 36, 48, 54Mbps
2.4GHz (N)	MCS0-15, up to 300Mbps

Please select the data rate you need or retain it auto as default.

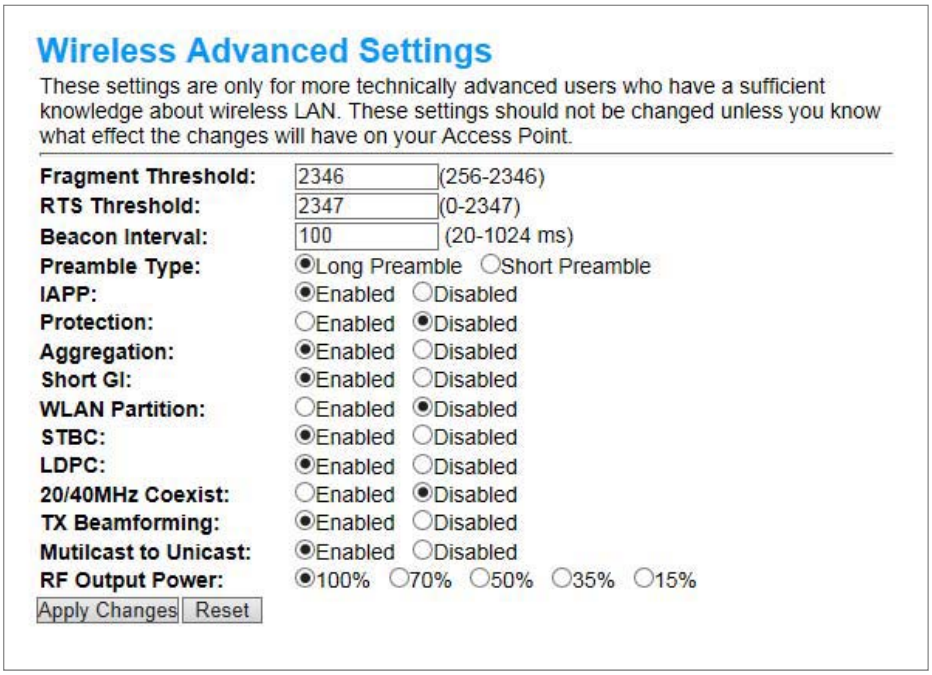
- **Associated Clients**

Click the “Show Active Clients” button, and then you will see the wireless clients connected to the SSID and status of them in the table.



Advanced Settings

In “Wireless Settings” > “Advanced Settings” option of this product’s web management interface, the advanced parameters for wireless LAN can be configured. After setting the parameters, please click “Apply Changes” button and reboot the product.



*It's recommended to keep the default values unless you know exactly the effect will be brought to this product when changing the parameters.

- **Fragment Threshold**

This value determines the maximum size of a data packet. The packets which are larger than this size will be fragmented.
If the wireless connection experienced packet errors frequently, you may slightly adjust the fragmentation threshold within the range of 256 to 2346.

- **RTS Threshold**

Request to Send (RTS) Threshold determines the size of the data packet that the low level RF protocol issues to an RTS packet
If the wireless connection is frequently disconnected by a long-distance connection to the AP, you may set it lower within the value range of 0 to 2347.

- **Beacon Interval**

The beacons are the packets sent by the router to synchronize a wireless network. The time interval of the beacons can be set in the range of 20 to 1024ms.

- **Preamble Type**

The preamble type defines the length of CRC blocks in the frames over the wireless communications. You may select "Short Preamble" when there is a large network-flow.

- **IAPP**

Inter-Access Point Protocol (IAPP) is used to provides wireless access point communications among multivendor systems

- **Protection**

This function provides wireless protection mechanism.

- **Aggregation**

This function is used to reduce the blocking in a large data transfer by aggregating multiple packets to a large packet.

- **Short GI**

This function is used to increase the data capacity by reducing the Guard Interval (GI) time.

- **WLAN Partition**

This function is used to prevent wireless clients from communicating with each other.

- **STBC**

Space-time block codes (STBC) function is used to improve system capacity and spectral efficiency.

- **LDPC**

Low-density parity-check (LDPC) code is used to transmit a message over a noisy transmission channel.

- **20/40MHz Coexist**

This function is used select whether the channel width of 20MHz and 40MHz can be mixed using.

- **TX Beamforming**

TX Beamforming is used to control sensor arrays for directional signal transmission.

- **Multicast to Unicast**

This option is used to change network transmission type to Unicast from Multicast.
Multicast is group communication where information is addressed to a group of destination computers simultaneously.
Unicast transmission is the sending of messages to a single network destination identified by a unique address.

- **RF Output Power**

Radio Frequency (RF) Output Power is used to control the signal strength of the wireless network. It can be decreased from 100% to 70%, 50%, 35% or 15%.

Encryption

The encryption function protects your wireless network from invasion.
It's strongly recommended to enable the encryption function. If this function is disabled, the router will be accessible by any client without password and the data transmission will be unsafe without encryption.
To set an encryption:

Step 1.

In "Wireless Settings" > "Encryption" option of this product's web management

interface, select the SSID you want to set an encryption for.

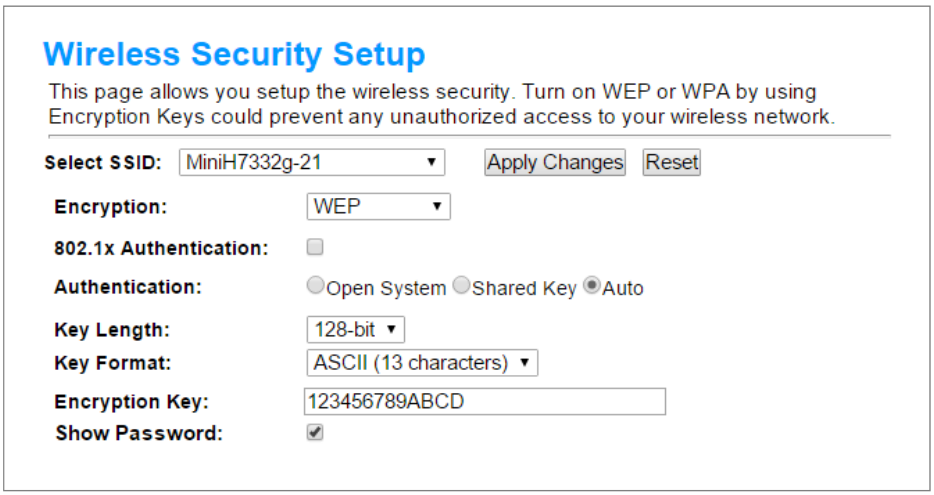
Step 2.

Select an encryption type from WEP, WPA2 and WPA-Mixed.

Step 3.

Select authentication mode, cipher suite (for WPA2/WPA-Mixed encryption), management frame protection (for WPA2 encryption), key format, and input the key. When input is completed, enable “Show Password” option to check the key.

WEP Encryption



802.1x Authentication:

802.1x Authentication provides an authentication for wireless local area networks (WLANs), which allowing a user to be authenticated by a central authority.

The WLAN client needs to use Remote Authentication Dial in User Service (RADIUS) server for authentication.

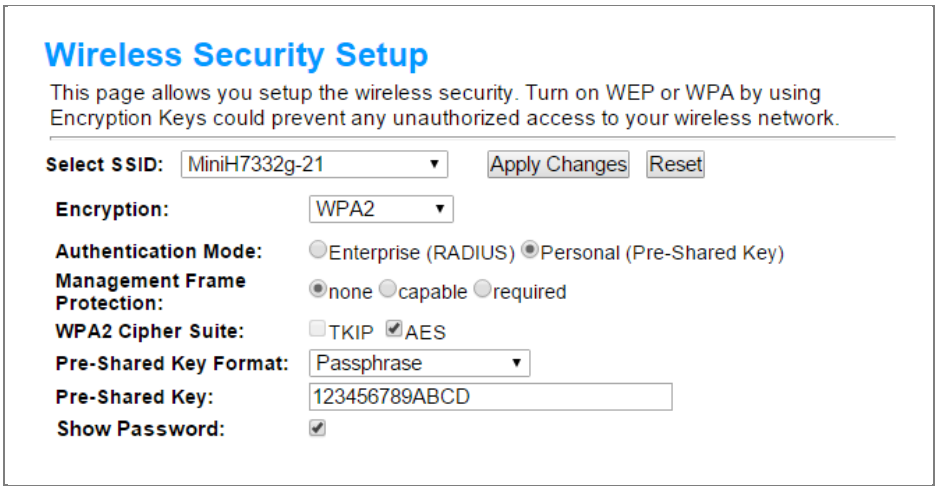
Authentication:

- Open System: The WLAN client can authenticate with the access point and then attempt to associate. If the client want to transmit data with access point, he must send the correct keys.
- Shared Key Authentication: The WLAN client needs to send the correct key to the router for authentication.

Key Length & Format:

Key Length	Key Format	Description
64-bit	ASCII (5 characters)	The key length must be 5 characters.
	Hex (10 characters)	The key length must be 10 characters.
128-bit	ASCII (13 characters)	The key length must be 13 characters.
	Hex (26 characters)	The key length must be 26 characters.

WPA2/WPA-Mixed Encryption



Authentication:

- Enterprise (RADIUS) Authentication: The WLAN client needs to use Remote Authentication Dial in User Service (RADIUS) server for authentication.
- Personal (Pre-Shared Key) Authentication: The WLAN client needs to send the pre-shared key to the router for authentication.

Management Frame Protection (for WPA2 encryption):

- Capable: In this mode, an AP will advertise that it can protect management frames. If a client that supports management frame protection attaches to the network, the AP will encrypt management traffic to it.
- Required: In this mode, an AP advertises not only that it can protect management frames, but also that clients must support the capability to use the network. If a client is unable to support management frame protection, it will not be allowed to connect to the network.

Cipher Suite:

- TKIP: Temporal Key Integrity Protocol (TKIP) is a suite of algorithms that works as a "wrapper" to WEP, which allows 40 and 128 bits key lengths.
- AES: Advanced Encryption Standard (AES) offers a higher level of security than TKIP, which allows 128, 192 and 256 bits key lengths.

Key Format:

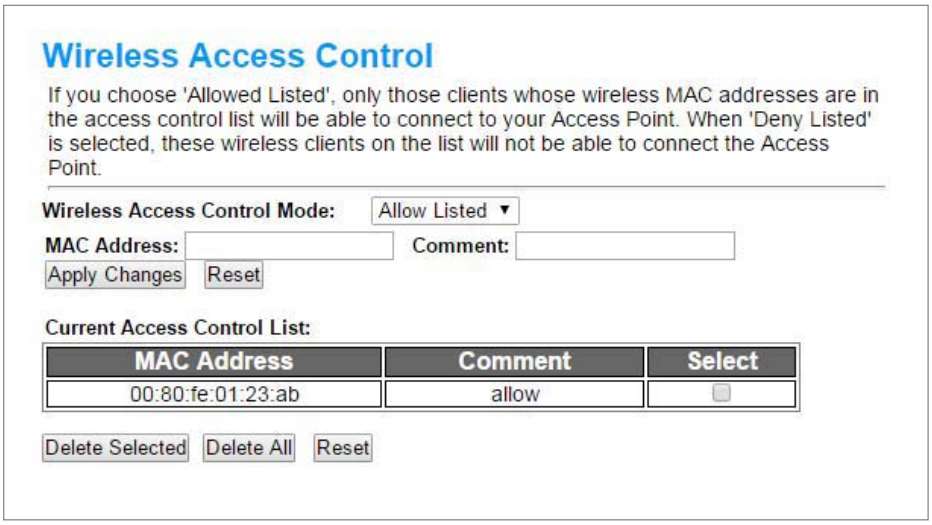
Key Format	Description
Passphrase	The key length must be between 8-63 characters.
Hex (64 characters)	The key length must be 64 characters.

Step 4.

Click “Apply Changes” button and reboot the product. After the product restarts, you can reconnect to the SSID by the key you set.

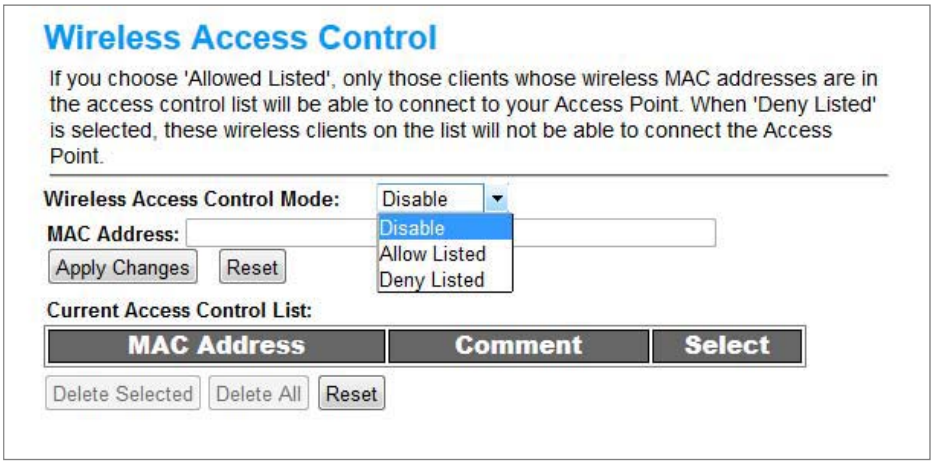
Access Control

To restrict the wireless connections, you can set up a control list in this page.



Step 1.

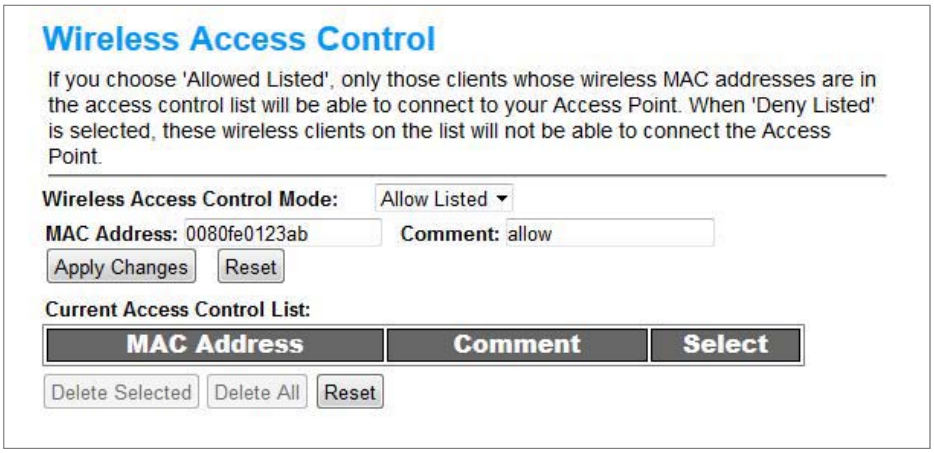
In “Wireless Settings” > “Access Control” option of this product’s web management interface, select “Wireless Access Control Mode” to “Allow Listed” or “Deny Listed”.



When “Allow listed” is selected, only the registered MAC addresses can access to this product; when “Deny Listed” is selected, the registered MAC addresses cannot access to this product.

Step 2.

Input the allowed/denied MAC address following the example format (0080fe0123ab) in “MAC address” input filed, and you can also input some description in “Comment” input filed.

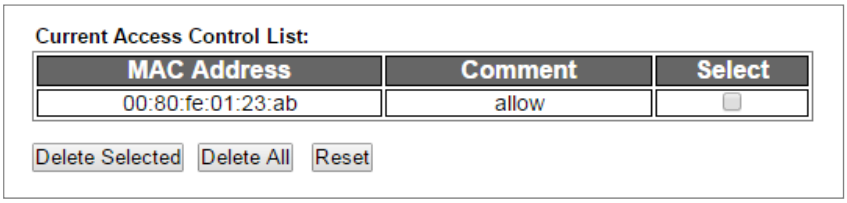


When input is completed, click “Apply Changes” button to save it.
If you are adding the first MAC into allow list, a prompt "If ACL allow list turn on; WPS2.0 will be disabled" will pop up, click "OK" to ensure that.

Step 3.

If you need to add more allowed/denied MAC addresses, click “Reboot Later” button and repeat Step 2.

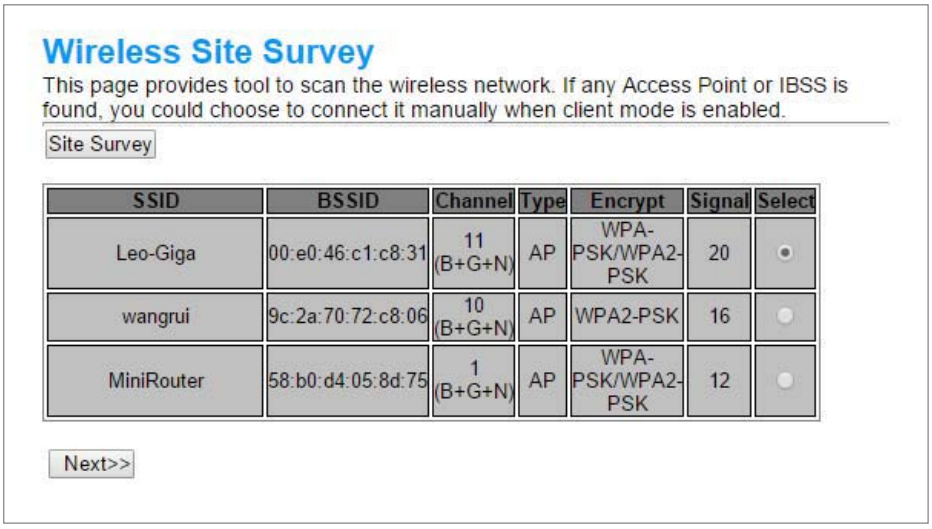
The form “Current Access Control List” will show the MAC addresses you have added.



When a MAC address need to remove control, you can delete it from the form and click “Apply Changes” button.
When all the addresses are added, click “Reboot Now” to restart the product.

Site Survey

The Site Survey function is used to scan the available wireless networks for the router to connect.
Site Survey function is only supported in Bridge and Wireless ISP mode.



Step 2.

Fill in the encryption information of the SSID you selected in the previous step. Confirm the encryption information is right and then click “Connect” button.

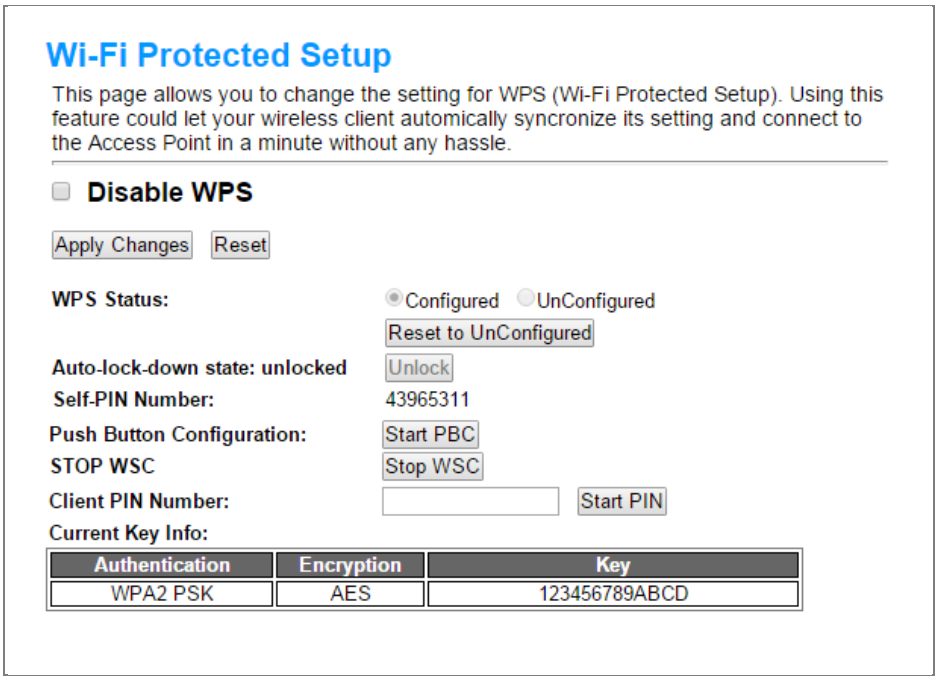
Step 3.

Wait a few time until the router is successfully connected to the SSID, and then reboot the product.

WPS

Wi-Fi Protected Setup (WPS) is used to simplify the security setup and management of Wi-Fi networks. This router supports two methods for WPS: Personal Identification Number (PIN) and Push Button Communication (PBC).

You need to set an encryption for the router before using the WPS function.

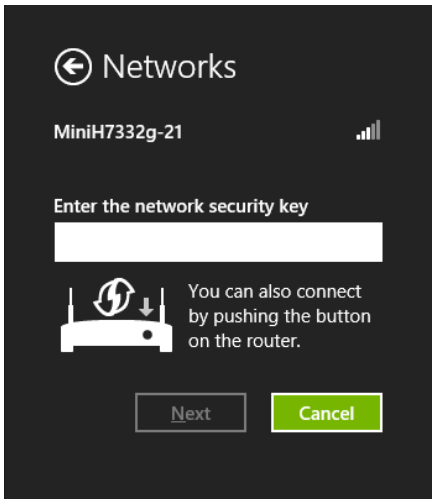


If you want to disable WPS function, select the checkbox of "Disable WPS", and then click "Apply Changes" button and reboot the product.

Connecting computer to router

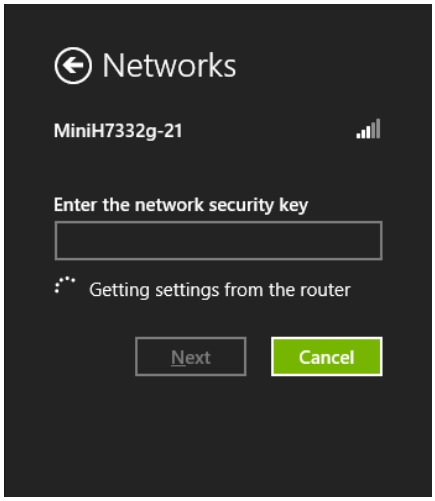
Step 1.

Connect to the SSID of the router wirelessly on your computer.
If WPS function is support on your computer, the connection will prompt to push router's button like picture below.



Step 2.

Push the WPS button at the lower right side of the product' top for more than 1 second until the WPS indicator starts to blink, you will see the connection is building.



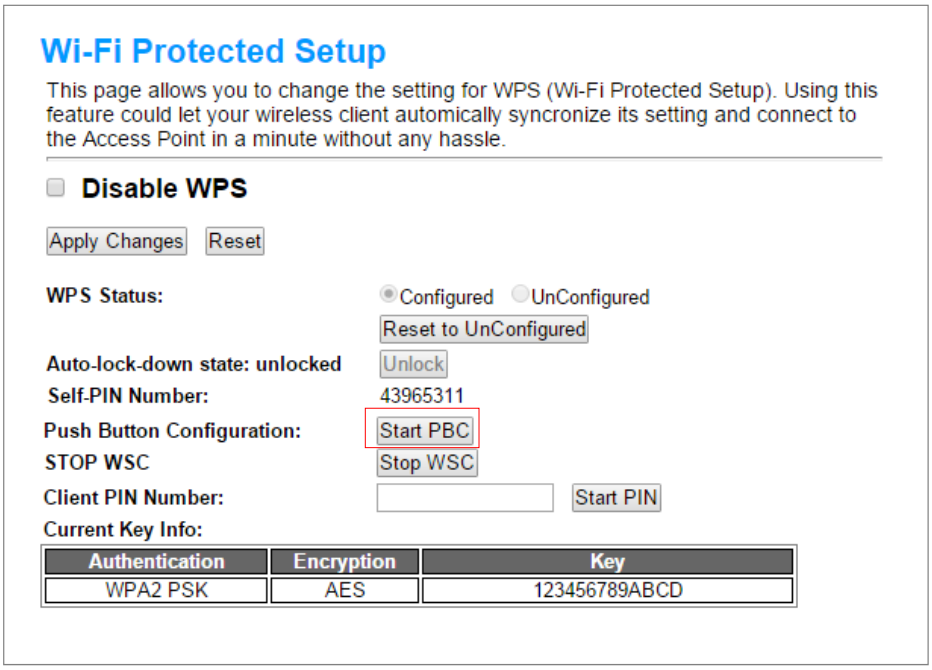
Step 3.
Wait until the connection created.

Connecting as the other router's client

Method 1: WPS Connection

Step 1.
Push the WPS button on your AP device in 2 minutes.

Step 2.
In "Wireless Settings" > "WPS" option of this product's web management interface, click "Start PBC" button; or directly push the WPS button at the lower right side of the product' top for more than 1 second. The WPS indicator on the product will start to blink.



If you want to cancel WPS, click "Stop WSC" button.

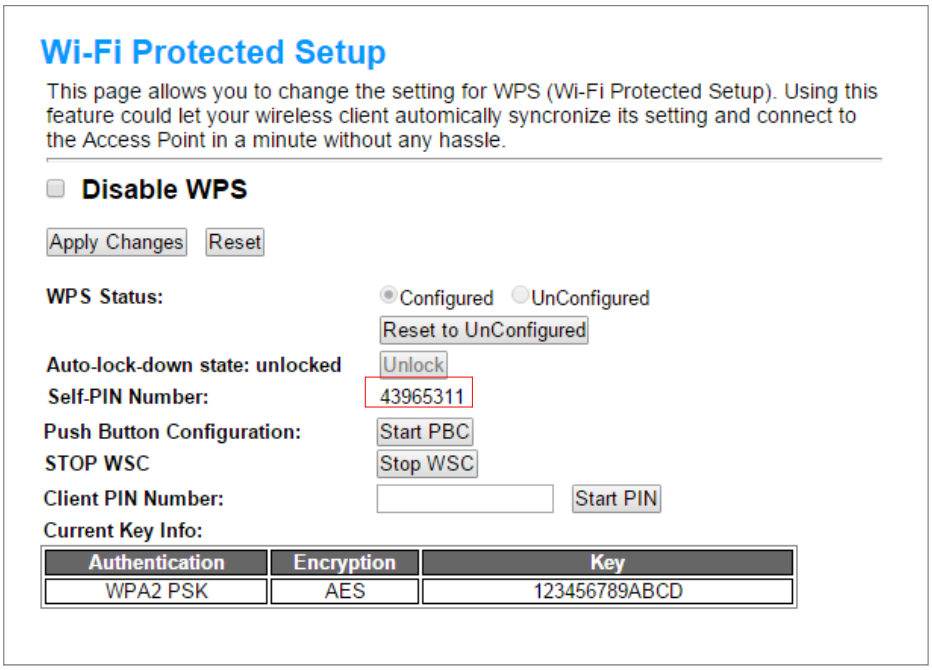
Step 3.

Wait until the WPS indicator stops blinking. At this time, the connection has been created automatically.

Method 2: PIN Connection

Step 1.

In “Wireless Settings” > “WPS” option of this product’s web management interface, find the code of “Self-PIN Number”.



Step 2.

In the WPS settings of AP website, input the PIN code of this product into the PIN setting field, and then start the PIN connection in the AP.

Step 3.

After AP starts PIN connection, the WPS indicator on this product will start to blink. When the connection is successfully created, the WPS indicator will stop blinking.

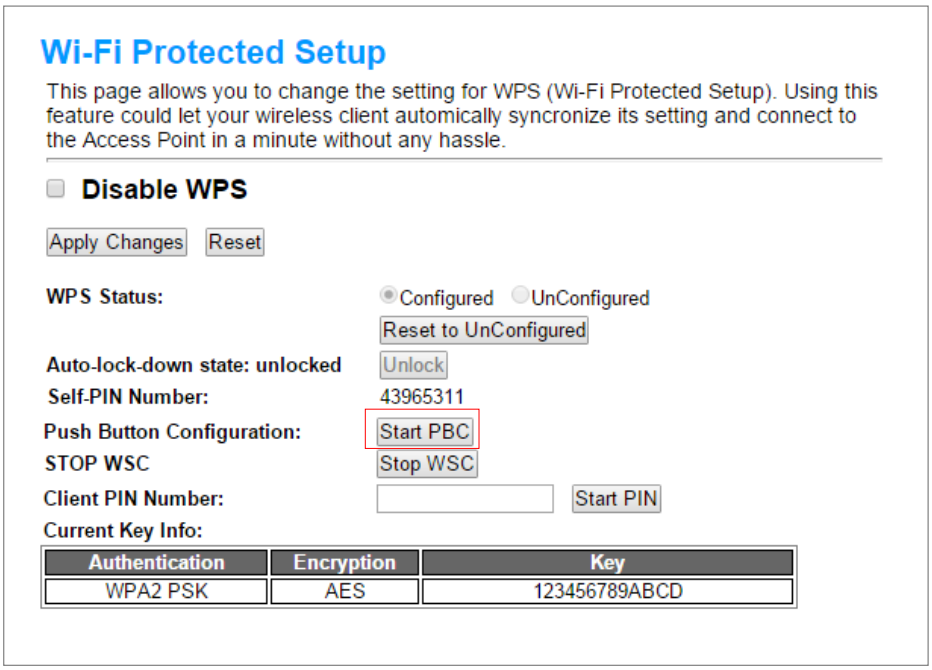
After the product restarts, you can connect to the extended wireless network (default renamed as AP SSID plus "-EXT") on your computer to access to Internet.

Connecting as the other router's AP

Method 1: WPS Connection

Step 1.

In "Wireless Settings" > "WPS" option of this product's web management interface, click "Start PBC" button; or directly push the WPS button at the lower right side of the product' top for more than 1 second. The WPS indicator on the product will start to blink.



If you want to cancel WPS, click "Stop WSC" button.

Step 2.

Push the WPS button on your client device in 2 minutes.

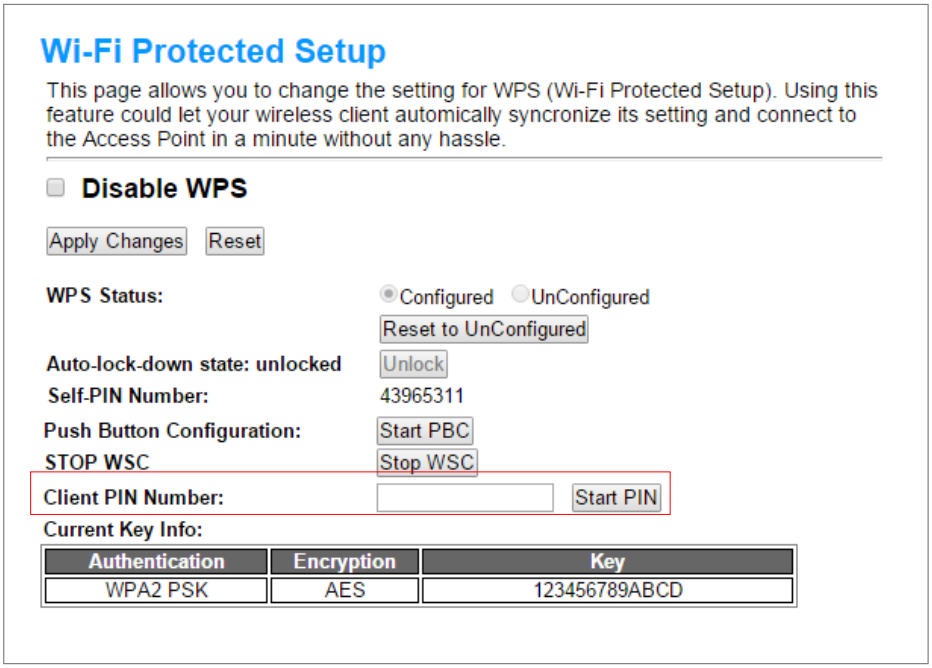
Step 3.

Wait until the WPS indicator stops blinking. At this time, the connection has been created automatically.

Method 2: PIN Connection

Step 1.

In “Wireless Settings” > “WPS” option of this product’s web management interface, input the PIN code of the client device into “Client PIN Number” input field, and then click “Start PIN” button beside.



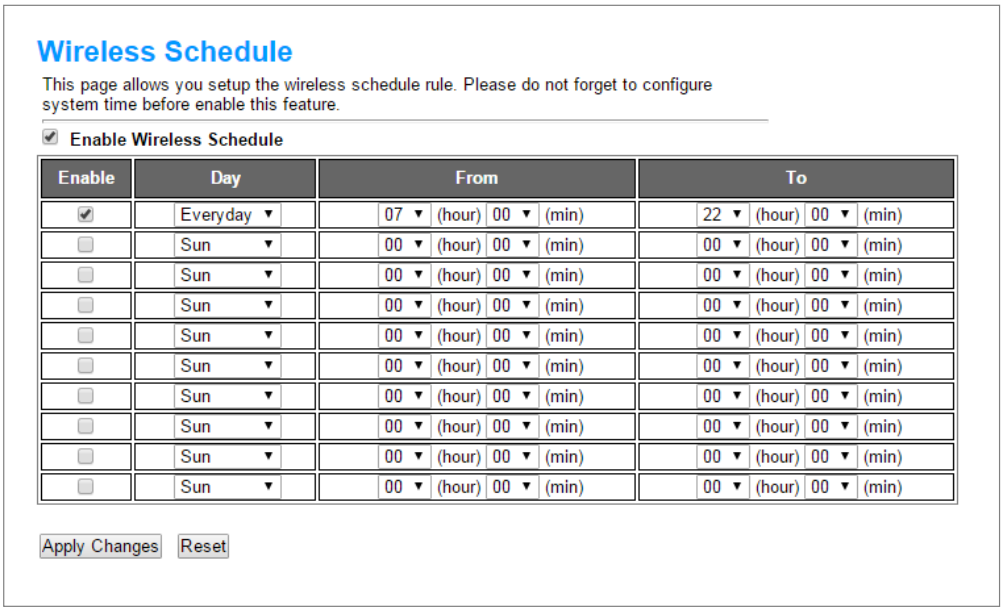
Step 2.

After starting PIN connection, the WPS indicator on this product will start to blink. When the connection is successfully created, the WPS indicator will stop blinking.

After the product restarts, you can connect to the extended wireless network (default renamed as “MiniH7332g-XX-EXT” for 2.4G band, "XX" is the last two characters of product WAN MAC address) on your computer to access to Internet.

Schedule

You can make your wireless schedule rule to control the work time of the router.



Step 1.

In “Wireless Settings” > “Schedule” option of this product’s web management interface, select the checkbox of "Enable Wireless Schedule".

Step 2.

Select a checkbox of column "Enable", and then select days and start/end time for schedule.

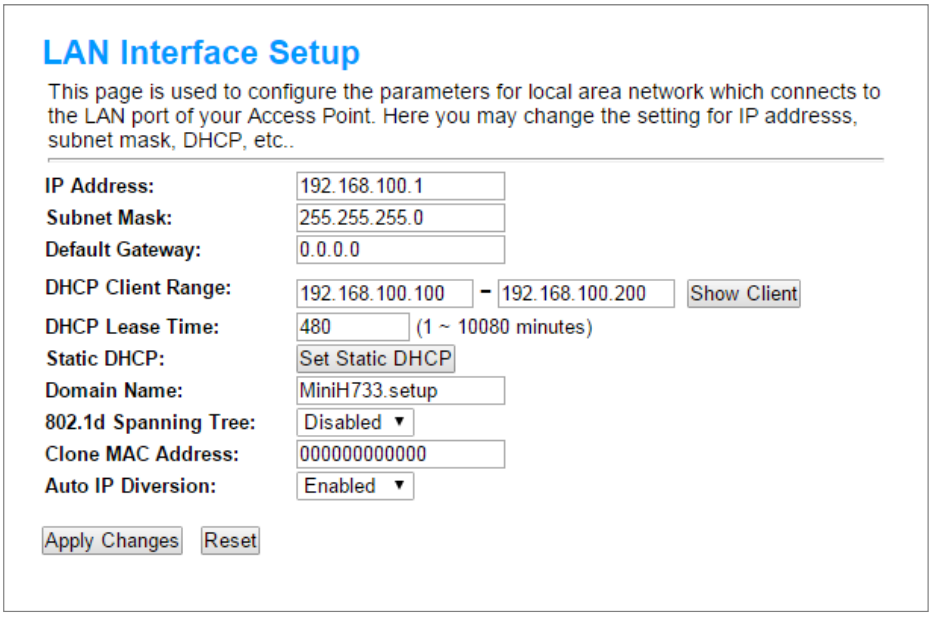
Step 3.

If you want to add more schedules, repeat step 2. At last click "Apply Changes" button and reboot the product to bring the schedule into effect.

TCP/IP Settings

LAN Interface

In “TCP/IP Settings” > “LAN Interface” option of this product’s web management interface, you can configure the parameters for LAN interface.

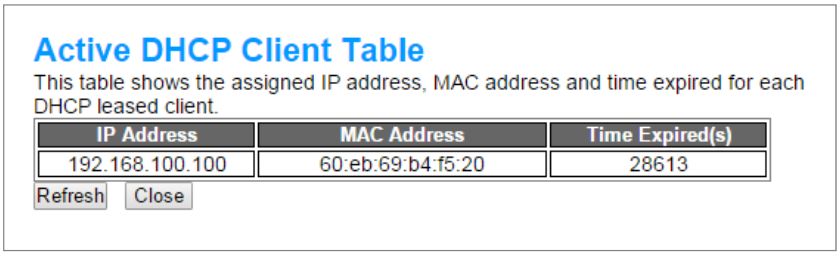


In Router mode, you can set IP address, subnet mask and default gateway manually, and configure DHCP settings for the LAN Interface.

DHCP Settings:

- **Set DHCP Client Range**

The range which used to assign IP addresses to DHCP Clients should be set in the same network segment as LAN IP address.
Click “Show Client” button, you can see the DHCP clients which are connected to this product, and check the IP addresses of the clients whether in the set range.

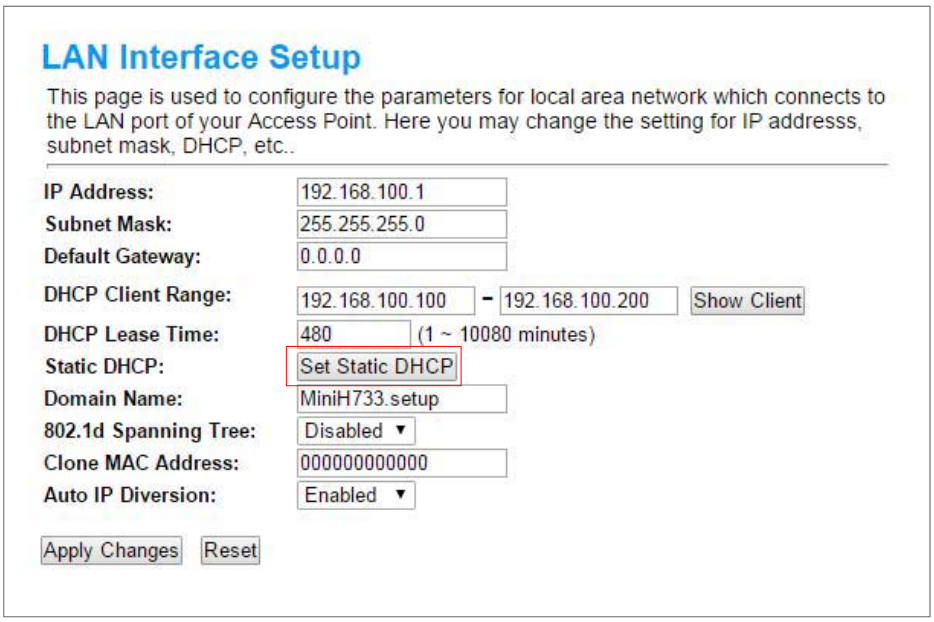


- **Set DHCP Lease Time**

DHCP lease time is used to limit the usage time of an IP address for a DHCP client. When the time is exceeded, the DHCP server will release the IP.
You can set the lease time within the range of 1 to 10080 minutes.

- **Set Static DHCP**

Static DHCP is used to assign an available static IP to a DHCP client. Click “Set Static DHCP” button then you will enter the static DHCP settings.



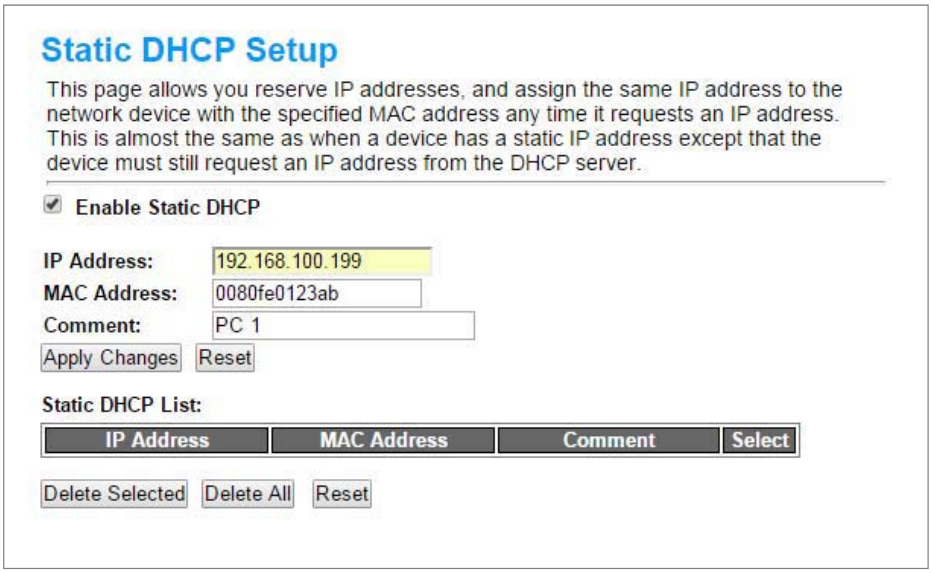
To use the Static DHCP function**:**

Step 1.

Enable “Enable Static DHCP” option.

Step 2.

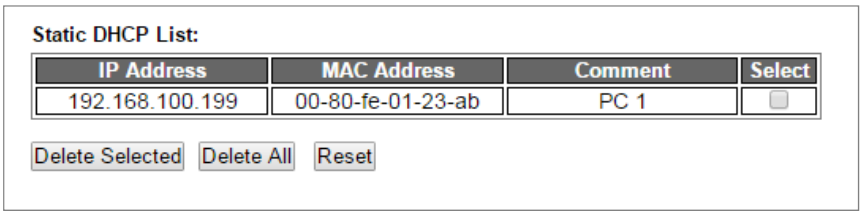
Input the IP address which will be assigned to a client in “IP address” input filed, and the MAC address of the client following the example format (0080fe0123ab) in “MAC address” input filed, and you can also input some description in “Comment” input filed.



When input is completed, click “Apply Changes” button to save it.

Step 3.

If you need to add more IP addresses for different clients, click “Reboot Later” button and repeat Step 2.
The form “Static DHCP List” will show the IP addresses you have added. When an IP address needs to be removed, you can delete it from the form and click “Apply Changes” button.



When all the IP addresses are added, restart the product to bring the settings take effect.

- **Domain Name**

Domain name is used to provide an easy way to access the web management interface.

- **802.d Spanning Tree**

The Spanning Tree Protocol is a network protocol that ensures a loop-free network while providing redundant connections.

- **Clone MAC Address**

This function is used to provide Internet capabilities for multiple computers through the router.
When you were required to register a MAC address by the ISP in order to access the Internet, actually you want multiple computers to join the network, you can assign the MAC address you have registered to the router by coping it to the “Clone MAC Address” field.

- **Auto IP Diversion**

This function is used to solve the conflict for IP addresses when WAN and LAN interfaces in the same subnet.

WAN Interface

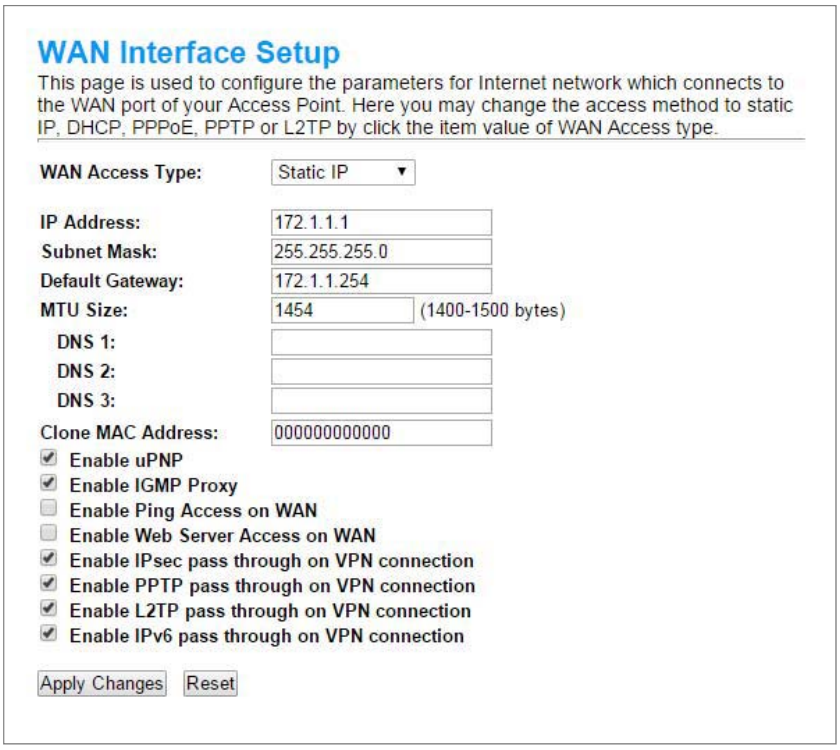
In “TCP/IP Settings” > “WAN Interface” option of this product’s web management interface, you can configure the parameters for WAN Interface.
WAN Interface settings is only supported in Router mode.

- **Set WAN Access Type**

There are three WAN access types provided: Static IP, DHCP Client and PPPoE.

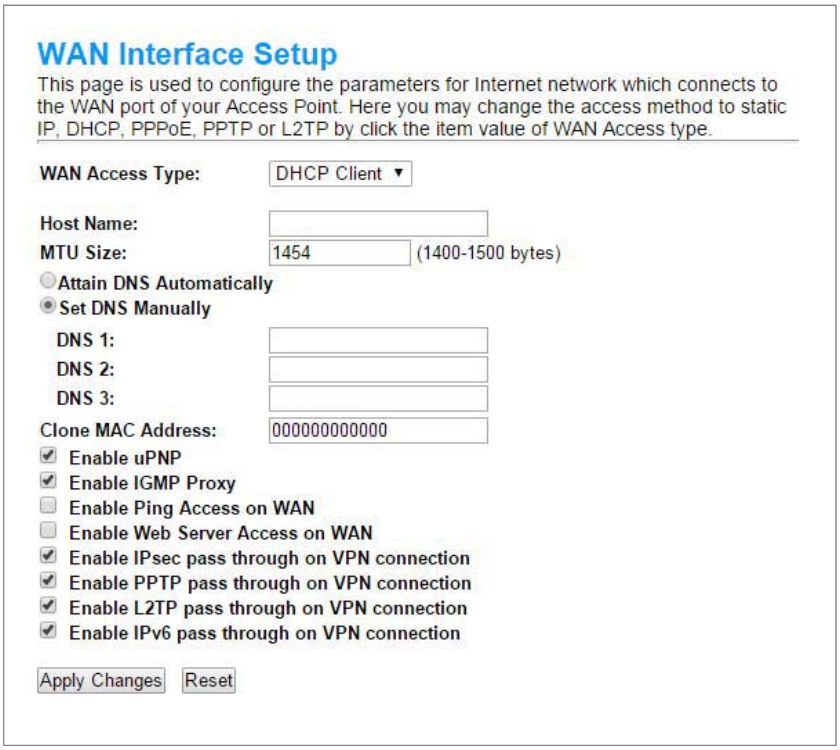
Type 1: Static IP

Select “Static IP” in the drop-down list of “WAN Access Type”, and input the static IP address, subnet mask and default gateway that provided by ISP.



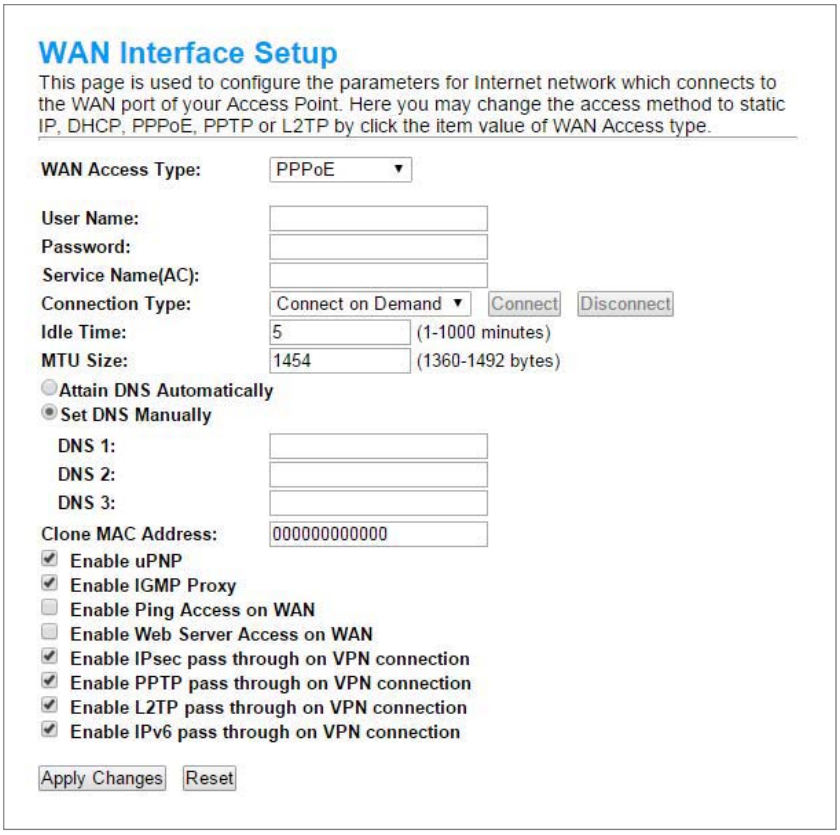
Type 2: DHCP Client

Select “DHCP Client” in the drop-down list of “WAN Access Type”, and set the DNS and host name for the product if the using Internet service has been configured with a host name.



Type 3: PPPoE

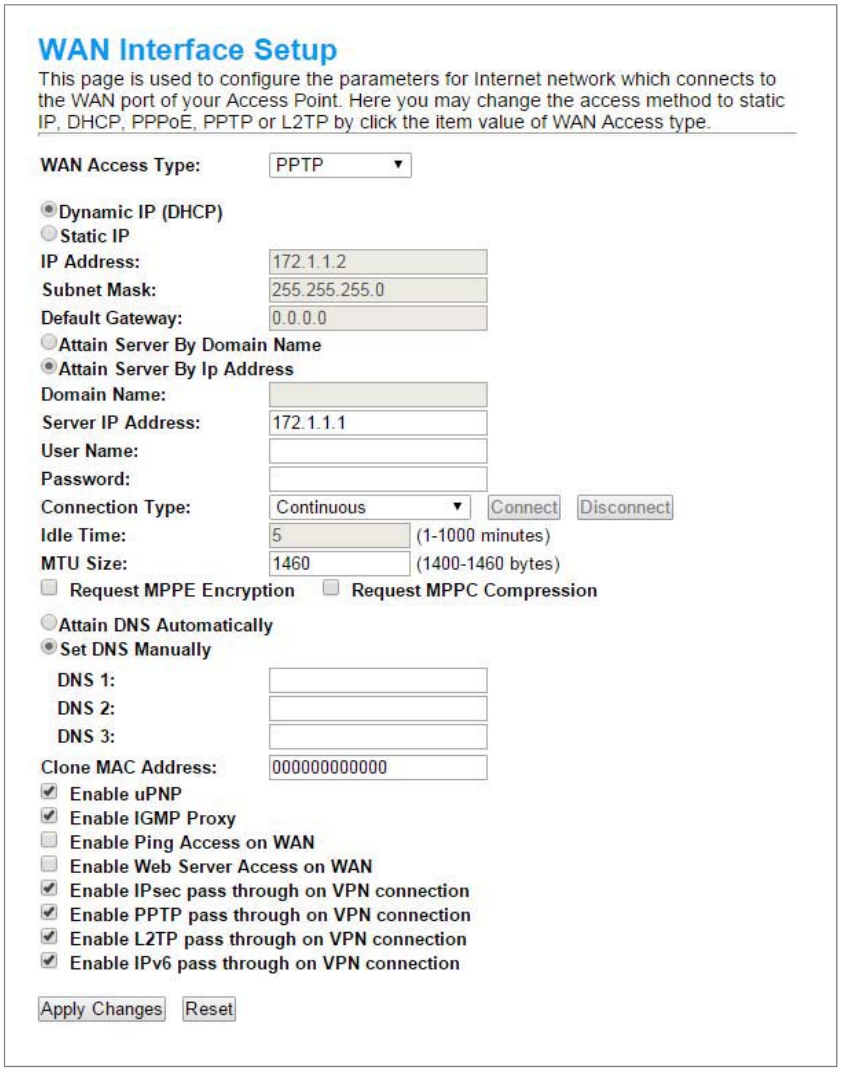
Select “PPPoE” in the drop-down list of “WAN Access Type”, and input the user name, password, and service name provided by ISP.



Type 4: PPTP

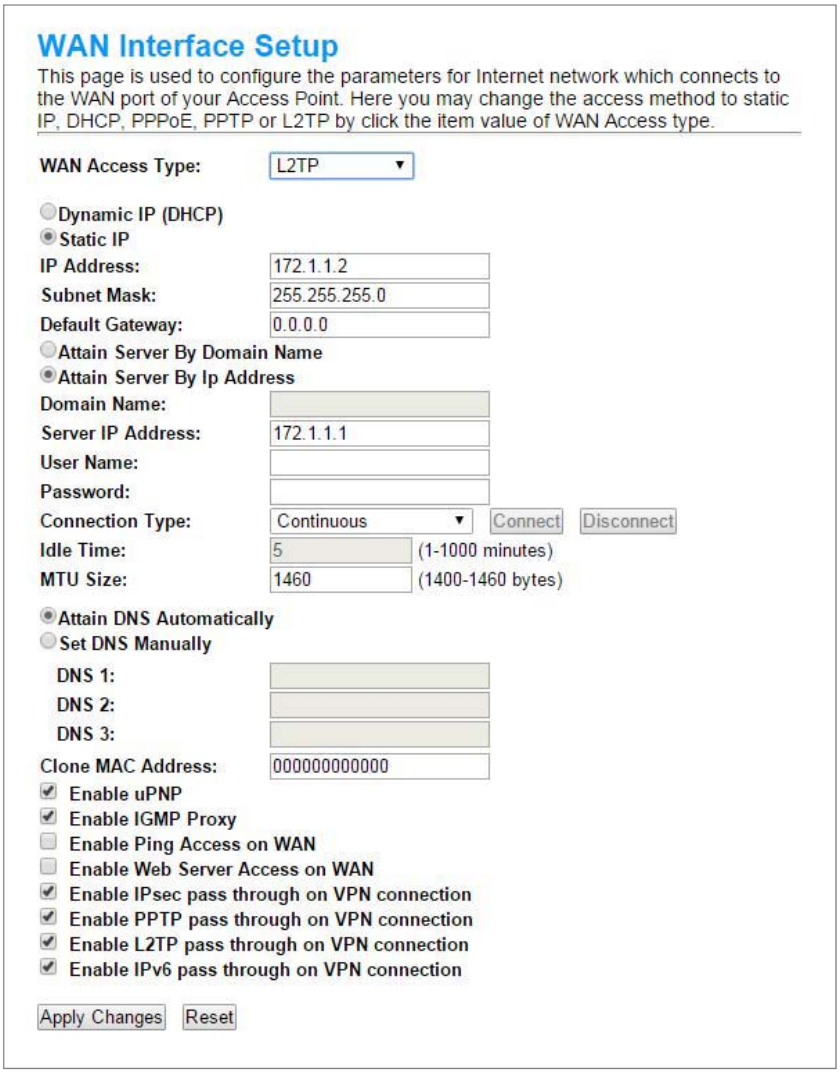
Select “PPTP” in the drop-down list of “WAN Access Type”, select client attaining type (DHCP/Static IP) and server attaining type (Domain Name/IP Address). Client Static IP and Server IP information were provided by ISP.

Microsoft Point-to-Point Encryption (MPPE) and Microsoft Point-to-Point Compression (MPPC) options are provided for the PPTP connection to transfer encrypted and compressed data grams over point-to-point links.



Type 5: L2TP

Select “L2TP” in the drop-down list of “WAN Access Type”, select client attaining type (DHCP/Static IP) and server attaining type (Domain Name/IP Address). Client Static IP and Server IP information were provided by ISP.



- **Connection Type**

Connection type is default set to "Continuous" for reconnecting automatically when the network is dropped, it can be changed to "Connect on Demand" or "Manual". "Connect on Demand" is for automatic reconnection with an idle time between 1 to 1000 minutes for demand. When the connection type is selected to this option, you can set the idle time in the “Idle Time” input field.
"Manual" is for manual connection by clicking “Connect” button to start a connection and clicking “Disconnect” button to disconnect.

- **Set MTU Size**

Maximum Transfer Unit (MTU) determines the largest size of datagram that can be transmitted. You can set the MTU size in the available range.

WAN Access	Range (bytes)	Default (bytes)
Static IP	1400 - 1500	1454
DHCP Client	1400 - 1500	1454
PPPoE	1360 - 1492	1454

PPTP	1400 - 1460	1460
L2TP	1400 - 1460	1460

- **DNS**

Domain Name Server (DNS) is a network system used to translate names into IP addresses.
Select “Attain DNS automatically" if you are provided with dynamic DNS by ISP, or select "Set DNS Manually" and input the DNS provided by ISP.

- **Clone MAC Address**

This function is used to provide Internet capabilities for multiple computers through the router.
When you were required to register a MAC address by the ISP in order to access the Internet, actually you want multiple computers to join the network, you can assign the MAC address you have registered to the router by coping it to the “Clone MAC Address” field.

- **Enable UPnP**

This function is used to support Universal Plug and Play (UPnP) devices.

- **Enable IGMP Proxy**

This function is used to intercept Internet Group Management Protocol (IGMP) packets between the repeater and clients to setup a multicast group.

- **Enable Ping Access on WAN**

This function is used to allow access Ping on WAN interface.

- **Enable Web Server Access on WAN**

This function is used to allow clients to access to this product’s web management interface from WAN interface.

- **Enable IPsec pass through on VPN connection**

This function is used to allow Internet Protocol Security (IPsec) packets from VPN connection pass through the repeater.

- **Enable PPTP pass through on VPN connection**

This function is used to allow Point to Point Tunneling Protocol (PPTP) packets from VPN connection pass through the repeater.

- **Enable L2TP pass through on VPN connection**

This function is used to allow Layer 2 Tunneling Protocol (L2TP) packets from VPN connection pass through the repeater.

- **Enable IPv6 pass through on VPN connection**

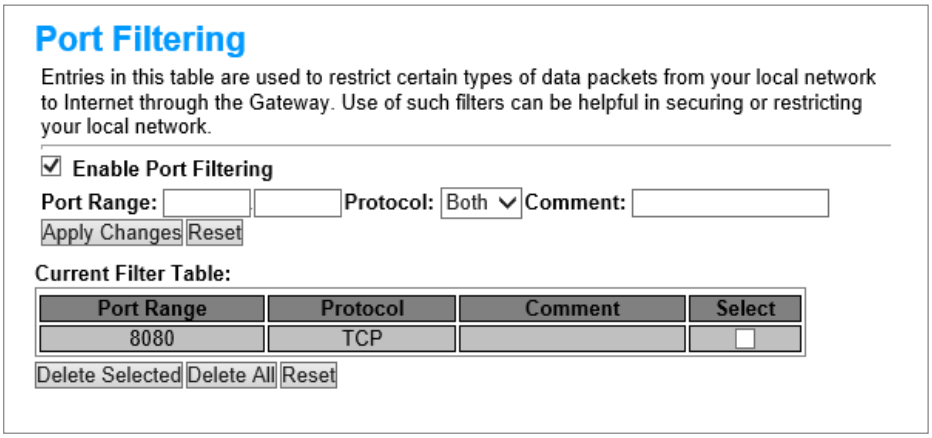
This function is used to allow Internet Protocol Version 6 (IPv6) packets from VPN connection pass through the repeater.

Firewall

Firewall is a network security tool that protects the computer from network attacks. Firewall function is only supported in Router mode.

Port Filtering

This function is used to restrict the data pass through the ports in a specified range.



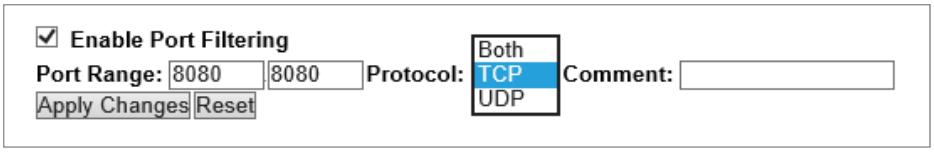
To use Port Filtering function:

Step 1.

In “Firewall” > “Port Filtering” option of this product’s web management interface, select the checkbox of "Enable Port Filtering".

Step 2.

Input the range for the ports that you want to restrict data pass through, and select filtering on TCP or UDP traffic or both.



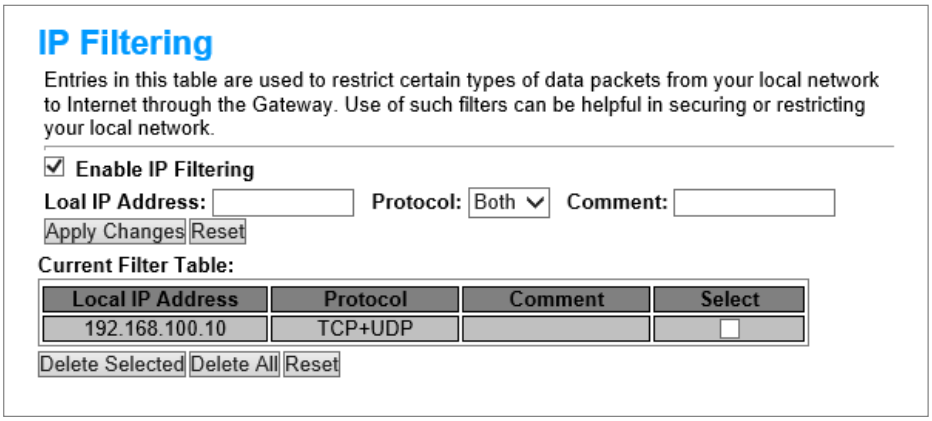
After set the port, click “Apply Changes” button to save it.

Step 3.

If you need to add more ports, click “Reboot Later” button and repeat Step 2.
The form “Current Filter Table” shows the filtered ports you have added. When you want to remove a port, you can delete it from the form and click “Apply Changes” button.
When all the ports are added, click “Reboot Now” to restart the product.

IP Filtering

This function is used to restrict the data pass through a specified IP address.



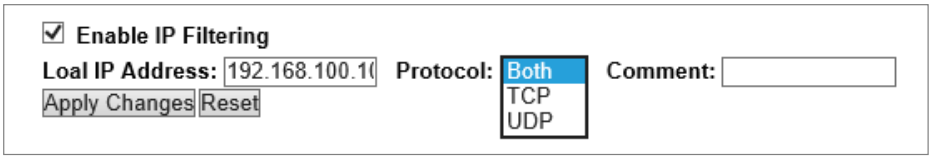
To use IP Filtering function:

Step 1.

In “Firewall” > “IP Filtering” option of this product’s web management interface, select the checkbox of "Enable IP Filtering".

Step 2.

Input the IP address that you want to restrict data pass through, and select filtering on TCP or UDP traffic or both.



After set the IP address, click “Apply Changes” button to save it.

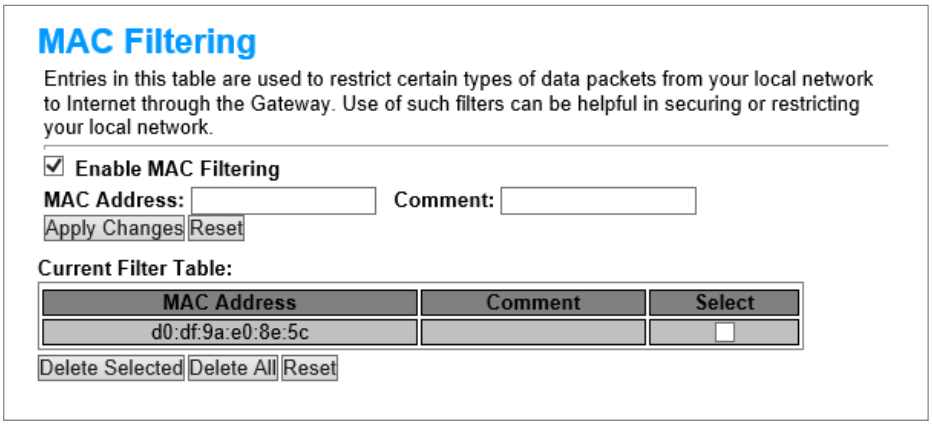
Step 3.

If you need to add more IP addresses, click “Reboot Later” button and repeat Step 2. The form “Current Filter Table” shows the filtered IP addresses you have added. When you want to remove an IP address, you can delete it from the form and click “Apply Changes” button.

When all the IP addresses are added, click “Reboot Now” to restart the product.

MAC Filtering

This function is used to restrict the data pass through the device with a specified MAC address.



To use MAC Filtering function:

Step 1.

In “Firewall” > “MAC Filtering” option of this product’s web management interface, select the checkbox of "Enable MAC Filtering".

Step 2.

Input the MAC address of the device that you want to restrict data pass through following the example format (0080fe0123ab), and select filtering on TCP or UDP traffic or both.

After set the MAC address, click “Apply Changes” button to save it.

Step 3.

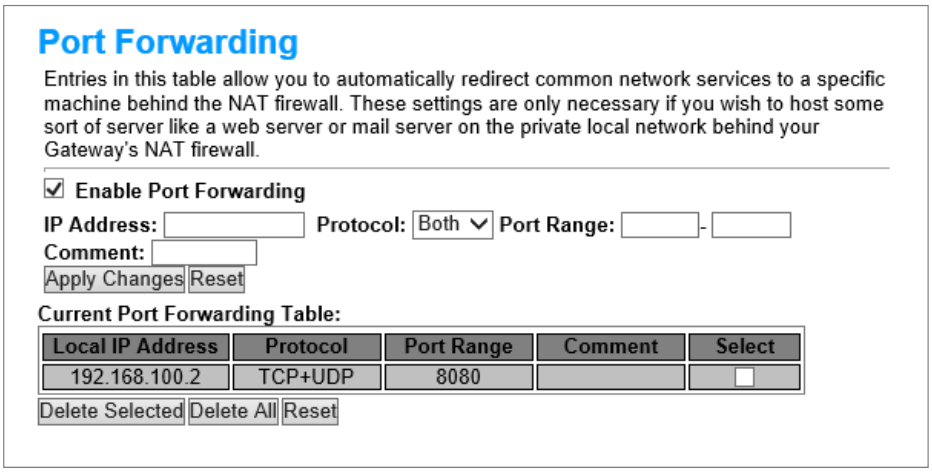
If you need to add more MAC addresses, click “Reboot Later” button and repeat Step 2.

The form “Current Filter Table” shows the filtered MAC addresses you have added. When you want to remove an MAC address, you can delete it from the form and click “Apply Changes” button.

When all the MAC addresses are added, click “Reboot Now” to restart the product.

Port Forwarding

This function is used to forward the visitors to the device with a specified IP when they visit through a specified port.



To use Port Forwarding function:

Step 1.

In “Firewall” > “Port Forwarding” option of this product’s web management interface, select the checkbox of "Enable Port Forwarding".

Step 2.

Input the IP address and the range for the ports that you want to make a port forwarding, and select forwarding on TCP or UDP traffic or both.

After set the port forwarding rule, click “Apply Changes” button to save it.

Step 3.

If you need to add more port forwarding rules, click “Reboot Later” button and repeat Step 2.

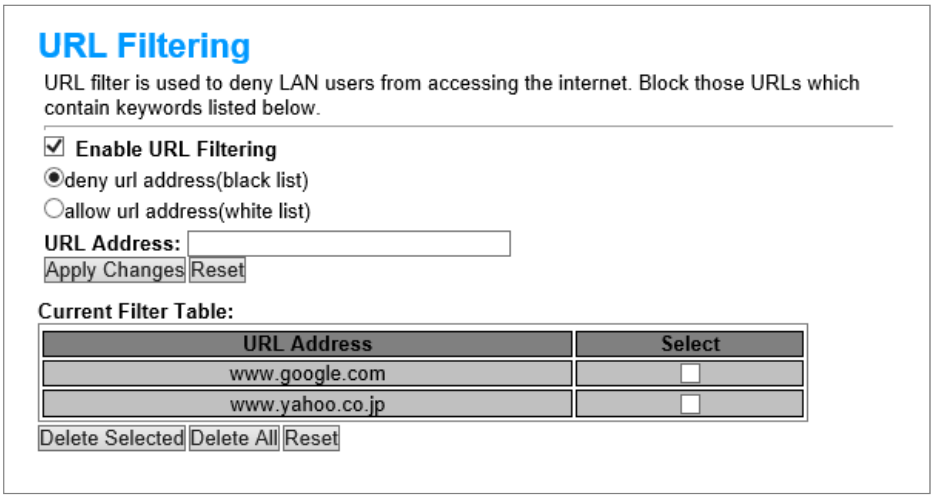
The form “Current Filter Table” shows the port forwarding rules you have added.

When you want to remove a port forwarding rule, you can delete it from the form and click “Apply Changes” button.

When all the port forwarding rules are added, click “Reboot Now” to restart the product.

URL Filtering

URL Filtering function is used to restrict the data pass through a specified URL address.



To use URL Filtering function:

Step 1.

In “Firewall” > “URL Filtering” option of this product’s web management interface, select the checkbox of "Enable URL Filtering".

Step 2.

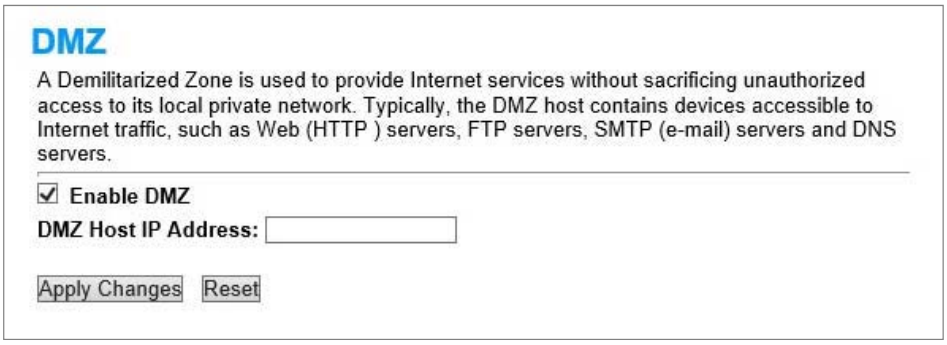
Select “deny url address” and input the URL address to deny data pass through it, or select “allow url address” and input the URL address to allow data pass through it. After set the URL, click “Apply Changes” button to save it.

Step 3.

If you need to add more URLs, click “Reboot Later” button and repeat Step 2.
The form “Current Filter Table” shows the filtered URLs you have added. When you want to remove an URL, you can delete it from the form and click “Apply Changes” button.
When all the URLs are added, click “Reboot Now” to restart the product.

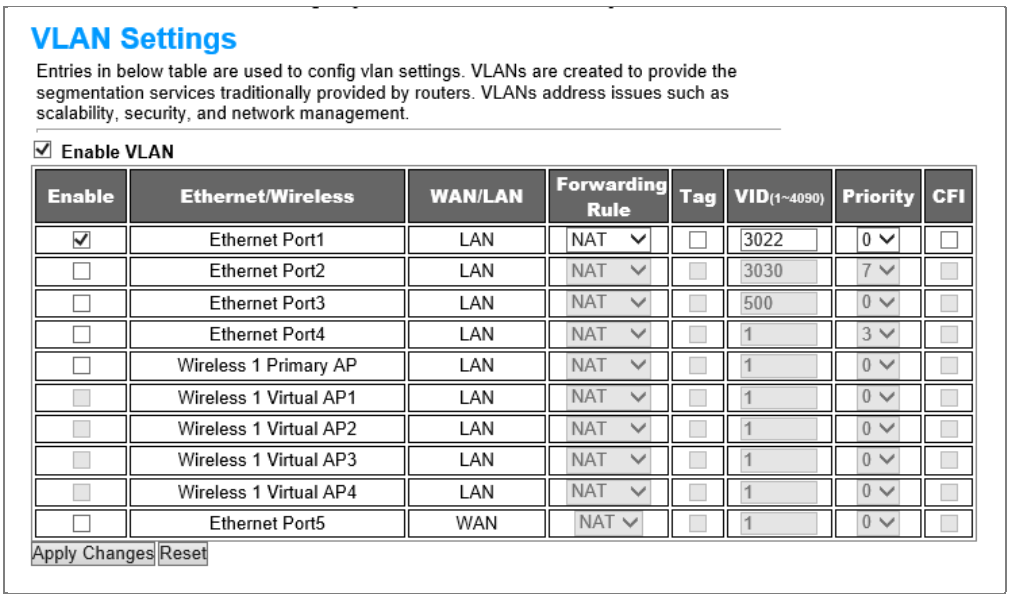
DMZ

The Demilitarized Zone (DMZ) function is used to forward the visitors to a specified device when they visit the router from WAN.
To use DMZ function:
In “Firewall” > “DMZ” option of this product’s web management interface, select the checkbox of “Enable DMZ”, and input the IP address of the DMZ host, then click “Apply Changes” button and reboot the product.



VLAN

Virtual Local Area Network (VLAN) is created to provide the segmentation services traditionally provided by routers.
To use VLAN function:
In “Firewall” > “VLAN” option of this product’s web management interface, select the checkbox of “Enable VLAN”, and then set the VLAN for the ports.
After setting the parameters, please click “Apply Changes” button and reboot the product.



VLAN Settings

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

☑ Enable VLAN

Enable	Ethernet/Wireless	WAN/LAN	Forwarding Rule	Tag	VID(1~4090)	Priority	CFI
☑	Ethernet Port1	LAN	NAT	☐	3022	0	☐
☐	Ethernet Port2	LAN	NAT	☐	3030	7	☐
☐	Ethernet Port3	LAN	NAT	☐	500	0	☐
☐	Ethernet Port4	LAN	NAT	☐	1	3	☐
☐	Wireless 1 Primary AP	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP1	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP2	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP3	LAN	NAT	☐	1	0	☐
☐	Wireless 1 Virtual AP4	LAN	NAT	☐	1	0	☐
☐	Ethernet Port5	WAN	NAT	☐	1	0	☐

Apply Changes Reset

- **Ethernet/Wireless**

This item lists the available ports including virtual APs.

- **WAN/LAN**

This item marks the ports as WAN or LAN.

- **Tag**

This item is used to set a tag for the VLAN.

- **VID**

VLAN Identifier (VID) is used to identify the VLAN to which the frame belongs. It can be set in the range from 0 to 4090.

- **Priority**

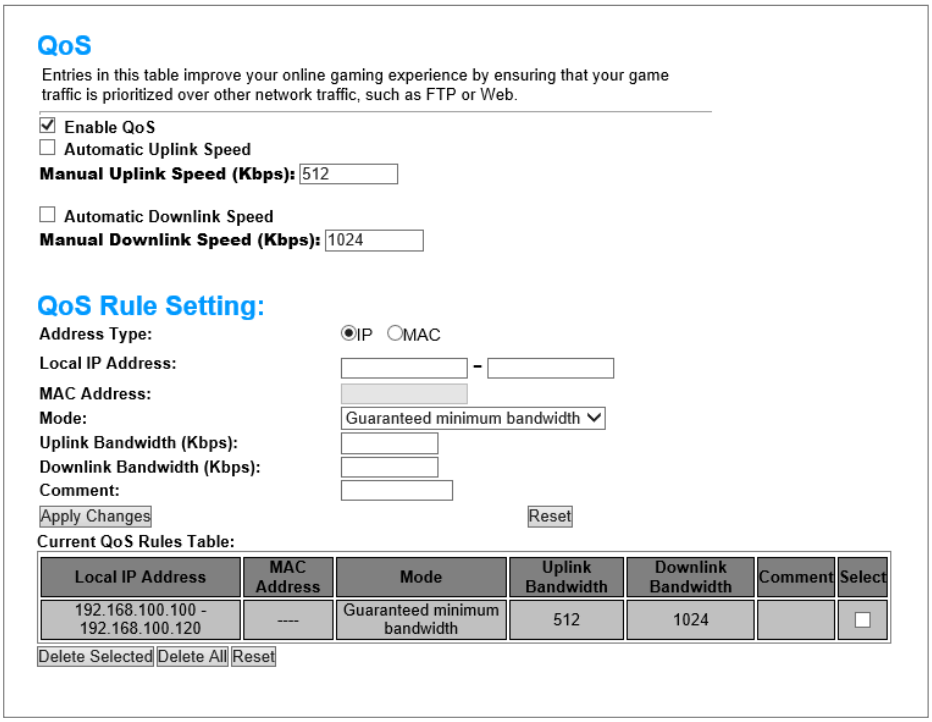
This item indicates the frame priority level which can be used for the prioritization of traffic. It can be set in the range from 0 to 7.

- **CFI**

Canonical Format Indicator (CFI) specifies whether or not the MAC addresses are encapsulated in standard format when packets are transmitted across different medium.

QoS

Quality of Service (QoS) is a service that used to improve the quality of network communication by setting rules.
QoS function is only supported in Router mode.



To set a QoS rule:

Step 1.

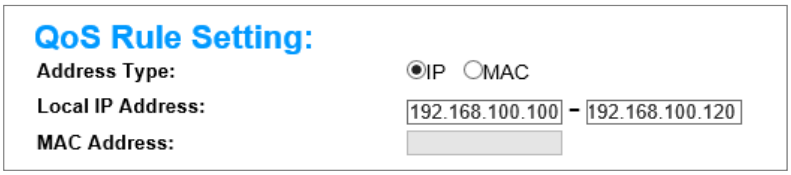
In “QoS” option of this product’s web management interface, select the checkbox of "Enable QoS".

Step 2.

Select the checkbox of “Automatic Uplink (Downlink) Speed” to set an automatic uplink/downlink speed, or disable the checkbox to manually set the uplink/downlink speed in the “Manual Uplink/Downlink Speed (Kbps)” input field.

Step 3.

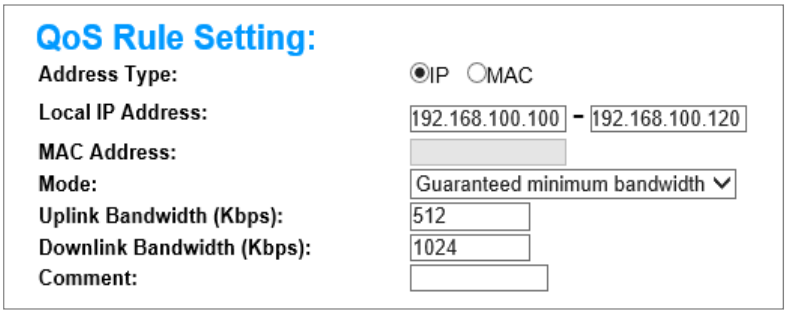
Select one address type from IP and MAC, and input the IP address range or MAC address you want to make a rule for.
IP address example:



MAC address example:

Step 4.

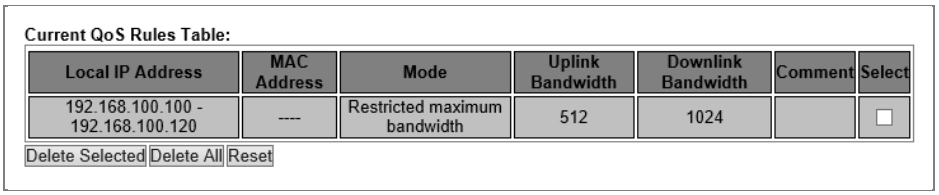
Select one speed limiting type from guaranteed minimum bandwidth and restricted maximum bandwidth in the drop-down list of “Mode”, and input an appropriate uplink/downlink bandwidth in the “Uplink (Downlink) Bandwidth (Kbps)” input field.



After set the uplink/downlink bandwidth, click “Apply Changes” button to save it.

Step 5.

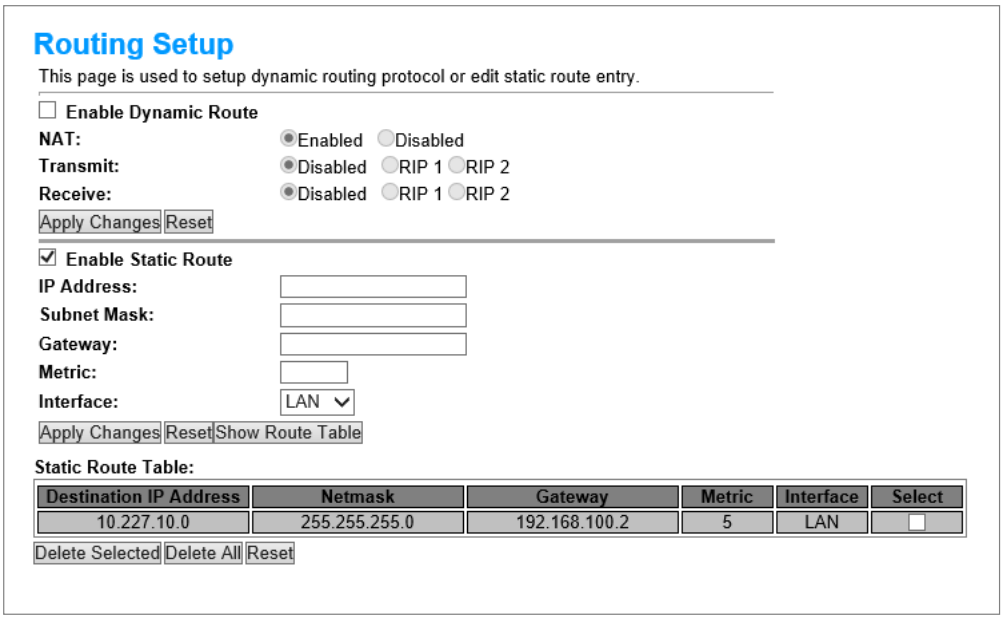
If you need to add more rules, click “Reboot Later” button and repeat Step 3, 4.
The form “Current QoS Rules Table” shows the QoS rules you have added.



When you want to remove a rule, you can delete it from the form and click “Apply Changes” button.
When all the rules are added, click “Reboot Now” to restart the product.

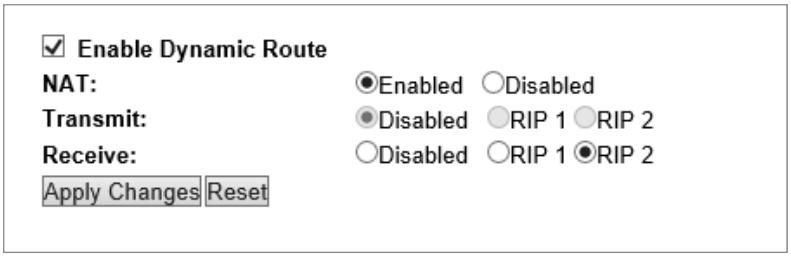
Route Setup

Route Setup function is used to set dynamic routing protocol or static route entries. In “Route Setup” option of this product’s web management interface, you can set dynamic or static route.
Route Setup function is only supported in Router mode.



Dynamic Route

To use Static Route function, select the checkbox of "Enable Dynamic Route".



- **NAT**

Network Address Translation (NAT) function is used to translate the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

- **Transmit / Receive**

These two options are used to select whether the router allows to transmit and receive RIP or RIP2 packet or not.
When the NAT function is enabled, “Transmit” option is not available.
The Routing Information Protocol (RIP) is a distance-vector protocol that uses hop count as a routing metric.

Static Route

A static route is a pre-determined path that network information must travel to

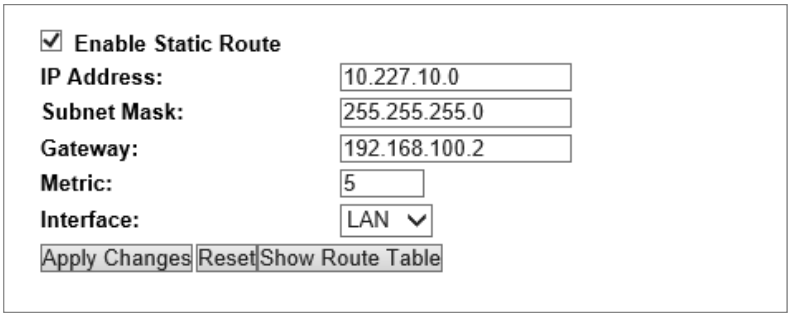
reach a specific host or network.
To use Static Route function:

Step 1.

Select the checkbox of "Enable Static Route".

Step 2.

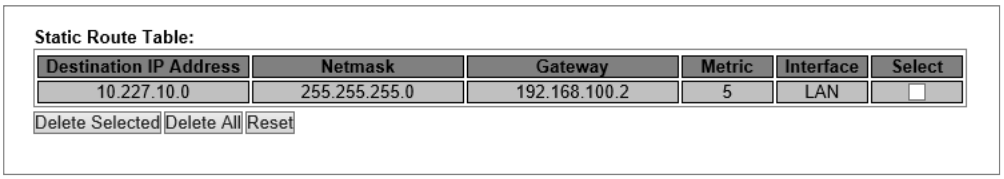
Input the IP address and subnet mask of the network or host that you want to assign to a static route in “IP Address” and “Subnet Mask” input field.
Input the IP address of the gateway device that allows for contact between the router and the network or host in “Gateway” input field.



Input the routing metric which is used to measure the distance between the source and the destination network in “Metric” input field.
Select the interface type of the destination to LAN or WAN.
After set the static route, click “Apply Changes” button to save it.

Step 3.

If you need to add more static routes, click “Reboot Later” button and repeat Step 3.
The form “Static Route Table” shows the static routes you have added.

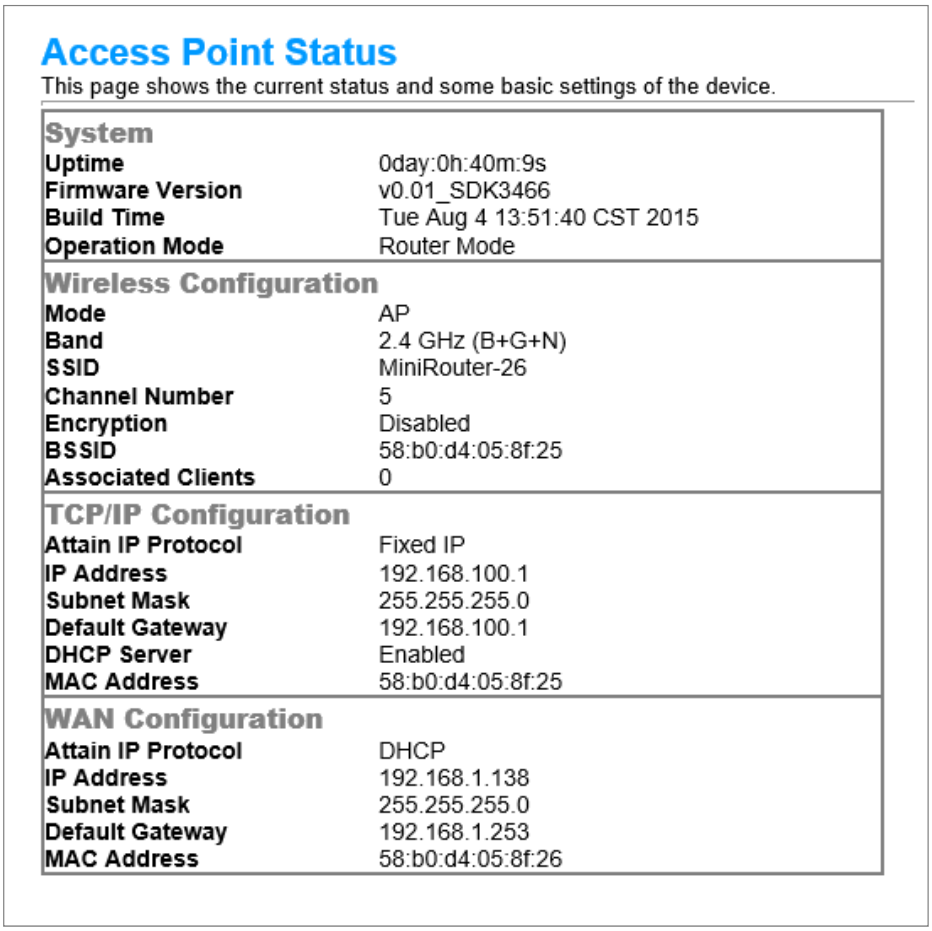


When you want to remove a static route, you can delete it from the form and click “Apply Changes” button.
When all the static routes are added, click “Reboot Now” to restart the product.

Router Management

Current Status

In “Router Management” > “Current Status” option of this product’s web management interface, you can see the current status and basic settings of the router.



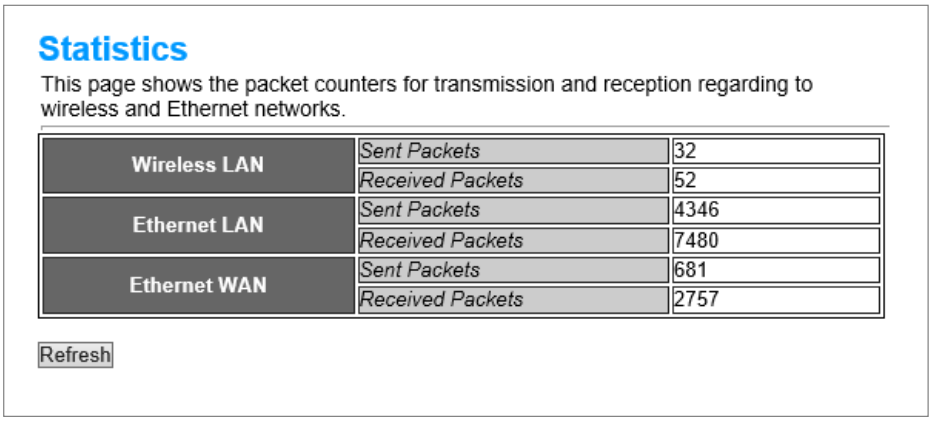
Access Point Status

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

System	
Uptime	0day:0h:40m:9s
Firmware Version	v0.01_SDK3466
Build Time	Tue Aug 4 13:51:40 CST 2015
Operation Mode	Router Mode
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	MiniRouter-26
Channel Number	5
Encryption	Disabled
BSSID	58:b0:d4:05:8f:25
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.100.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.100.1
DHCP Server	Enabled
MAC Address	58:b0:d4:05:8f:25
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.1.138
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.253
MAC Address	58:b0:d4:05:8f:26

Statistics

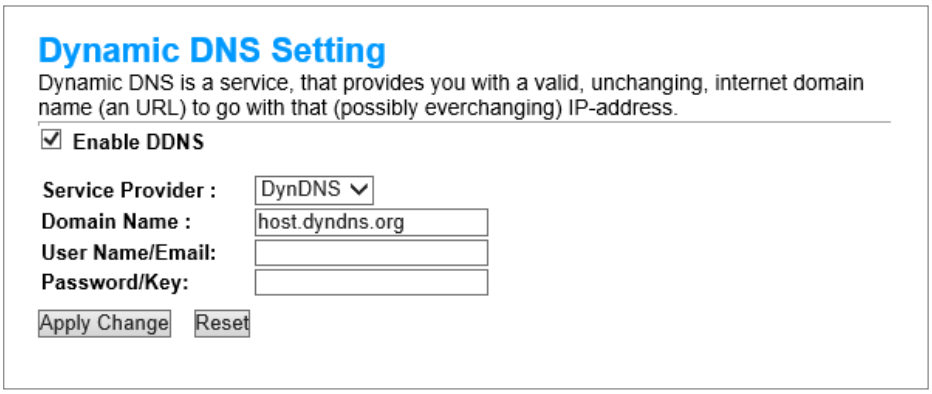
In “Router Management” > “Statistics” option of this product’s web management interface, you can see the packets traffic of sending and receiving.



Click “Refresh” button to update the data.

DDNS

Dynamic Domain Name Server (DDNS) is a service that provides a fixed domain name to map a frequently changed IP address.



To use DDNS function:

Step 1.

In “Router Management” > “DDNS” option of this product’s web management interface, select the checkbox of "Enable DDNS".

Step 2.

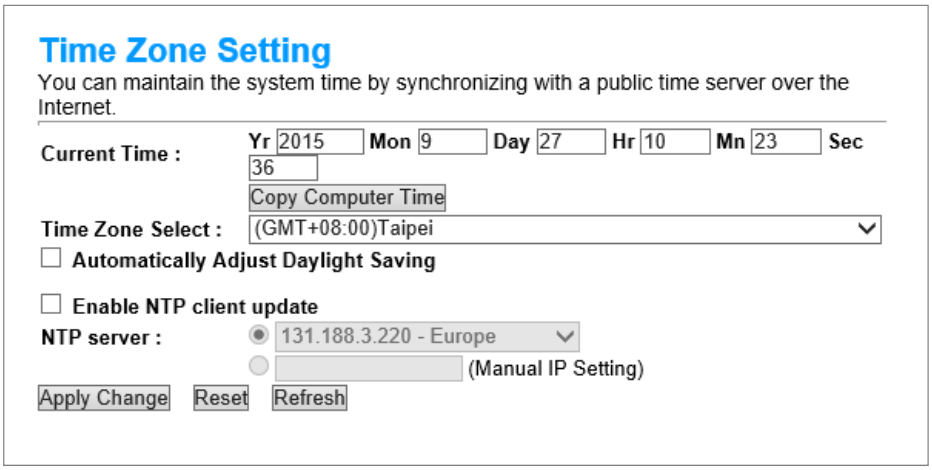
Select the service providers to “DynDNS” or “TZO”, and input the domain name you registered, your user name or email and password on the service provider’s website.

Step 3.

Click “Apply Change” button and reboot the router.

Time Zone Setting

In “Router Management” > “Time Zone Setting” option of this product’s web management interface, you can set the system time and time zone.
After setting the parameters, please click “Apply Change” button and reboot the product.



- **Set Time**

Change the value of “Current Time” to set the system time, or click “Copy Computer Time” button to directly copy the computer time to the product.

- **Set Time Zone**

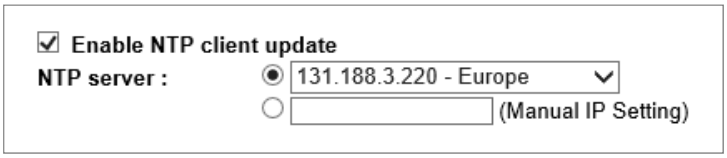
Select the time zone in the drop-down list of “Time Zone Select”.

- **Daylight Saving Time**

Daylight saving time is the practice of setting the clock forward by one hour during the warmer part of the year, so that evenings have more daylight and mornings have less.
To set daylight saving time, enable “Automatically Adjust Daylight Saving” option after NTP updating enabled.

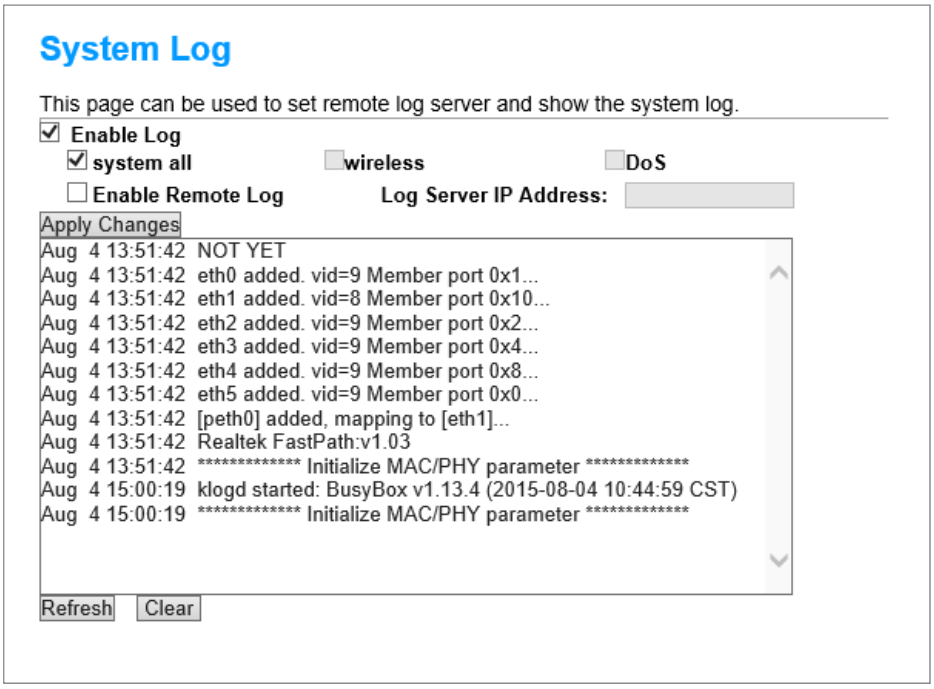
- **NTP Updating Time**

Network Time Protocol (NTP) is used to synchronize the system time with a network server.
To use NTP updating time, enable “Enable NTP client update” option, and select a NTP server or manually input an NTP server IP.



System Log

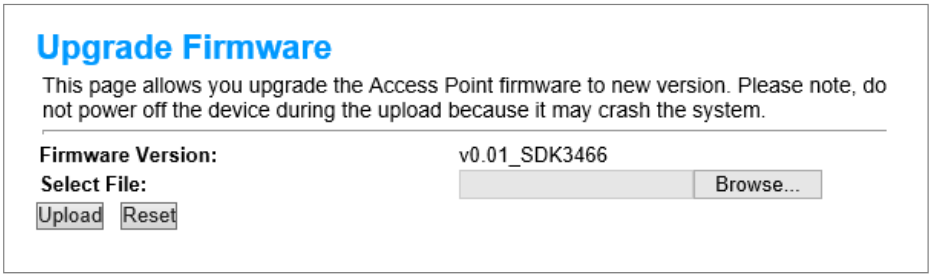
In “Router Management” > “System Log” option of this product’s web management interface, you can enable the logging function to record the activities on the product.



To use system log function, select the checkbox of “Enable Log” option, and select log type from “wireless”, “QoS” or “system all”, and then click “Apply Changes” button and reboot the product.
When the product rebooted, the log will be displayed in the text area. You can click “Refresh” button to refresh the log, or click “Clear” button to clean the text area.

Upgrade Firmware

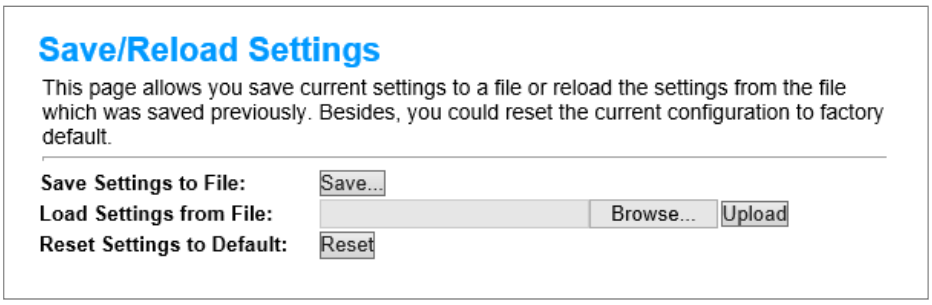
In “Router Management” > “Upgrade Firmware” option of this product’s web management interface, you can upgrade the firmware if this product has a new version.



To upgrade the firmware, click “Browse” button to select the firmware file on the local disk, and then click “Upload” button to execute it.
After the router rebooted, you can check firmware version to confirm whether the firmware upgrade is successful or not.

Save/Reload Settings

In “Router Management” > “Save/Reload Settings” option of this product’s web management interface, you can save or reload the settings of the product.



- **Save Settings to File**

Save current settings of the router to a configuration file.

- **Load Settings from File**

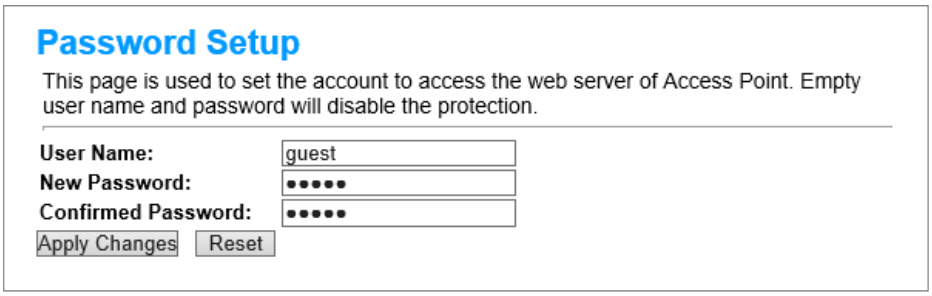
Reload the settings from a configuration file.
To use this function, click “Browse” button and select the configuration file saved before, and then click “Upload” button to reload the settings from the file.

- **Reset Settings to Default**

Restore current settings to the factory default settings.

Admin Password

In “Router Management” > “Admin Password” option of this product’s web management interface, you can change the user name and password that used to login the management interface.
Default user name and password are both “admin”. You can set a new user name and password. For example:



After change the user name and password, click “Apply Changes” button to save it. The product will reboot automatically and logout, you need to re-login by the new user name and password.

Logout

In “Management” > “Logout” option of this product’s web management interface, click “Apply Change” button then you will save previous settings and log out from the management interface.

Troubleshooting

Q1. Cannot access to the web management interface.

- Check that you are connecting to the right SSID on the computer, and input the right URL “http://MiniH733.setup” to access to the web management interface.
- Make a wired connection to the router with a LAN cable for accessing the web management interface. If the router is working in Bridge mode, you need to set TCP/IP properties manually on your computer as the steps in **Appendix A: TCP/IP Settings**.

Q2. Cannot connect to the SSID of the router

- Check "Broadcast SSID" option is enabled in the web management interface, and you are connecting to the right SSID on the computer.
- Check that you sent the right encryption key for connecting when the router is encrypted.

Q3. Cannot access to Internet when connected to the SSID

- Check whether the router is successful to connect to the other router or modem. If connection is failed, please reconnect to the AP.
- Check whether the other router or modem can access to the Internet. If there is any problem with the modem, please contact the ISP.

Q4. Forgot the user name or password to login the web management interface

- You can reset the router by the rest button. Press and hold the reset button on the router for more than 5 seconds and then release it, the system will be restored to the factory settings, and you can login to the web management interface with the default user name and password both for “admin”.

Glossary

802.11b

802.11b is used in a point-to-multipoint configuration, wherein an access point communicates via an omnidirectional antenna with one or more nomadic or mobile clients that are located in a coverage area around the access point. 802.11b has a maximum raw data rate of 11 Mbit/s and uses the same CSMA/CA media access method defined in the original standard.

802.11g

802.11g is the third modulation standard for wireless LANs. It works in the 2.4 GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbit/s, or about 19 Mbit/s net throughputs.

802.11n

802.11n has a significant increase in the maximum net data rate from 54 Mbit/s to 600 Mbit/s with the use of four spatial streams at a channel width of 40 MHz. 802.11n standardized support for multiple-input multiple-output and frame aggregation, and security improvements, among other features.

Daylight Saving Time

Daylight Saving Time (DST) which also called summer time in several countries in British English, and European official terminology, is the practice of advancing clocks so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

DHCP

The Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices so that they can communicate on an IP network.

DNS

Domain Name Server (DNS) is a network system used to translate names into IP addresses.

DSL

Digital Subscriber Line (DSL) is a family of technologies that provide internet access by transmitting digital data over the wires of a local telephone network.

ISP

Internet Service Provider (ISP) is a business or organization that offers users' access to the Internet and related services.

Infrastructure & Ad-Hoc Mode

Infrastructure mode requires a central access point that all devices connect to. Devices on the network all communicate through a single access point, which is generally the wireless router.
Ad-hoc mode is also known as "peer-to-peer" mode. Ad-hoc networks don't require

a centralized access point. Instead, devices on the wireless network connect directly to each other.

NTP

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

SSID

Service Set Identifier (SSID) is a sequence of characters that uniquely names a wireless local area network (WLAN). The maximum length of the SSID is currently 32 characters long.

WEP

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. WEP, recognizable by the key of 10 or 26 hexadecimal digits, is widely in use and is often the first security choice presented to users by router configuration tools.

WLAN

Wireless Local Area Network (WLAN) is a technology which combines computer network and wireless communication system.

WMM

Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks.

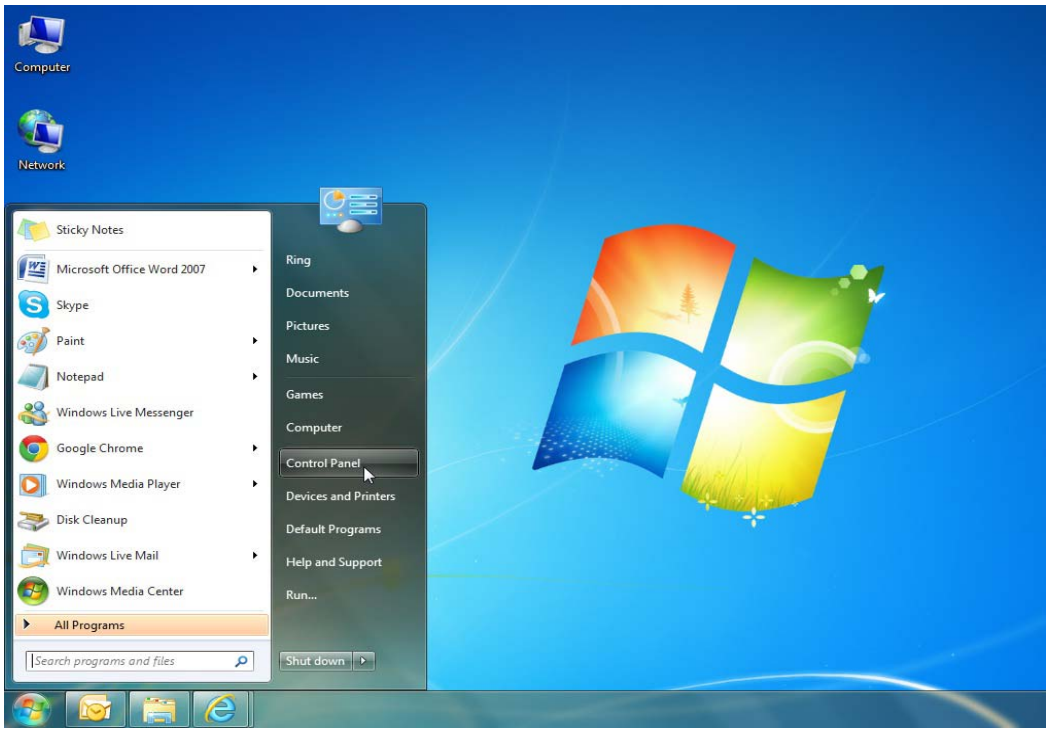
WPA/WPA2

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy).

Appendix A: TCP/IP Settings

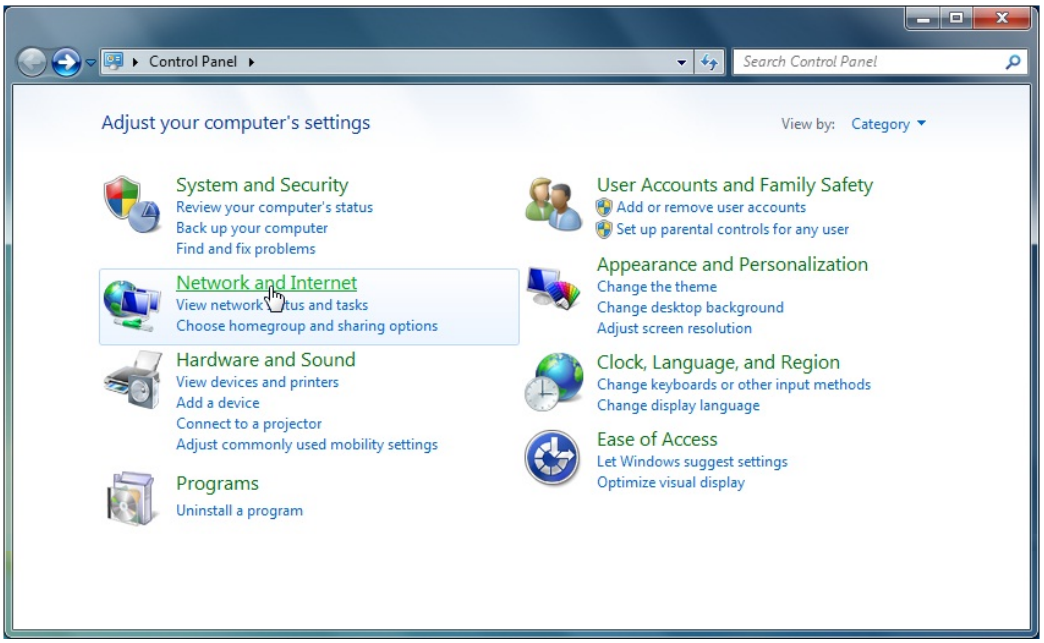
Step 1:

On the desktop of your computer, click “Start” –> “Control Panel”.



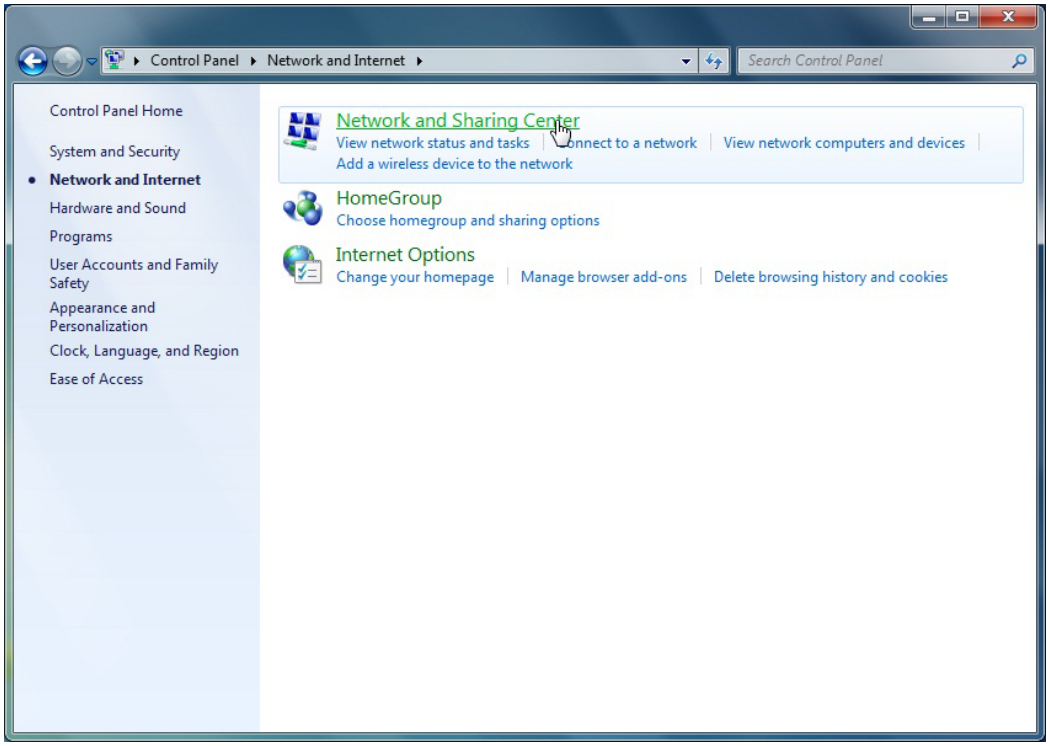
Step 2:

Click “Network and Internet”.



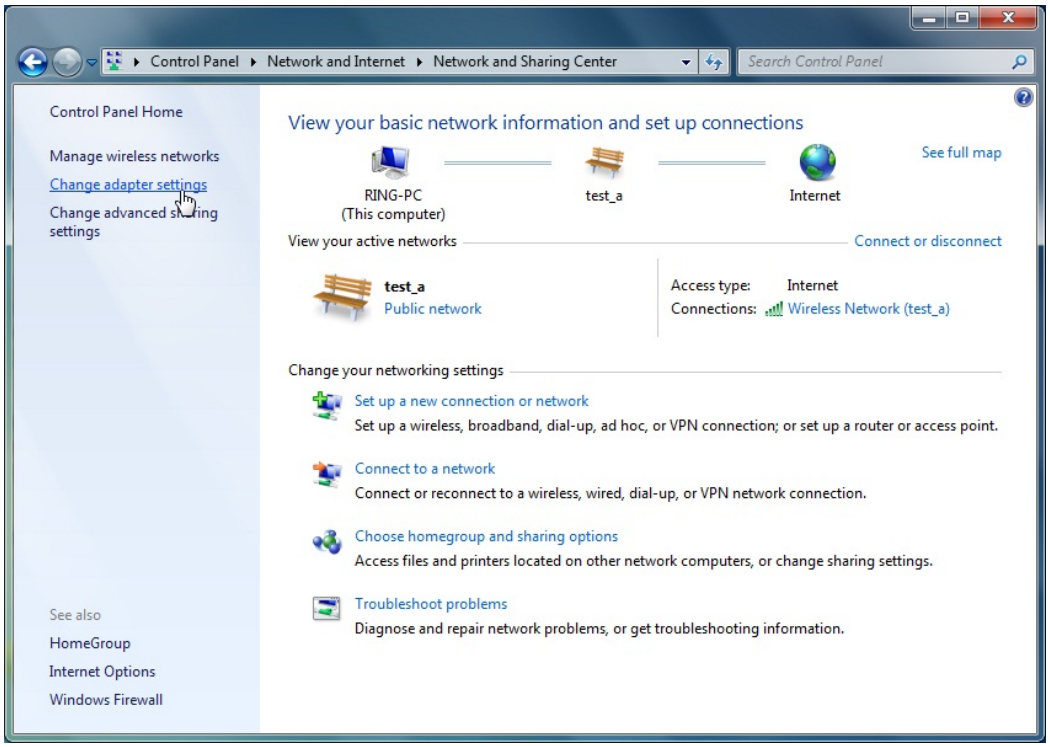
Step 3:

Click “Network and Sharing Center”.



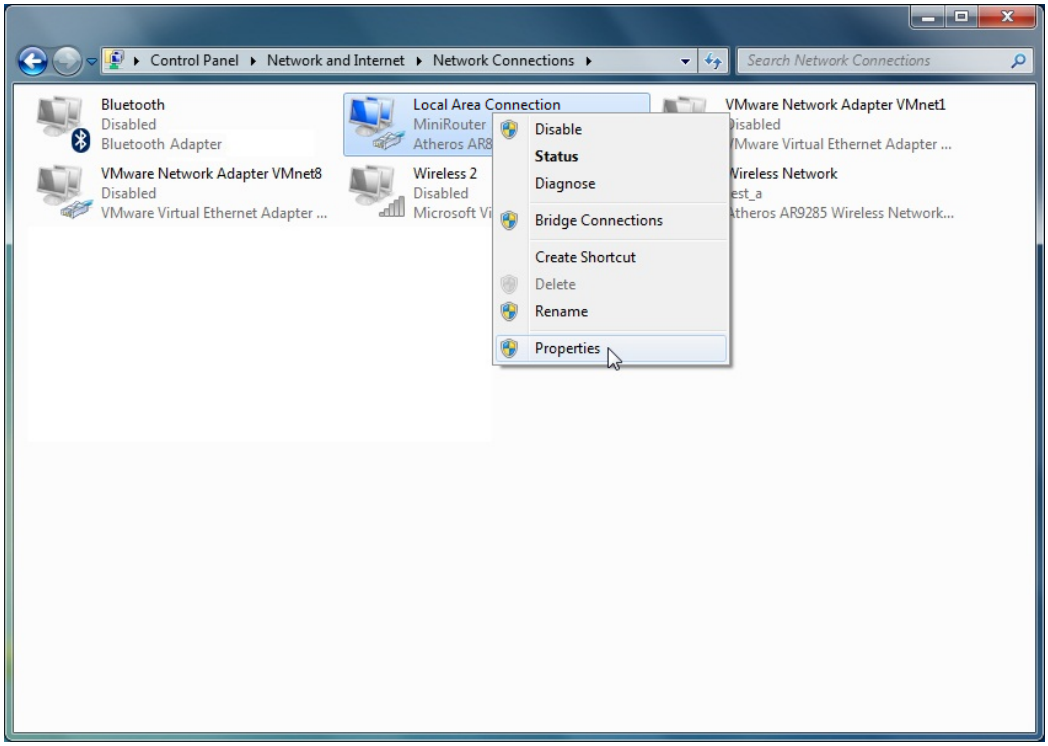
Step 4:

Click “Change adapter settings” on the left side.



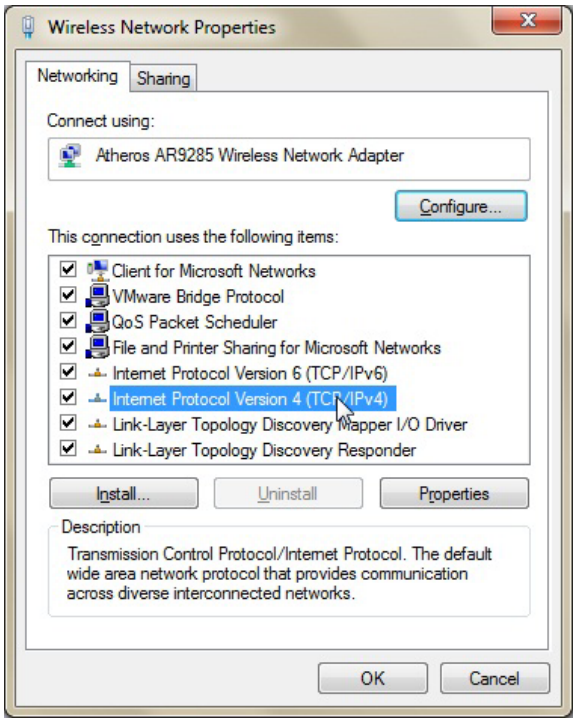
Step 5:

Right click on your local area connection, select “Properties”.



Step 6:

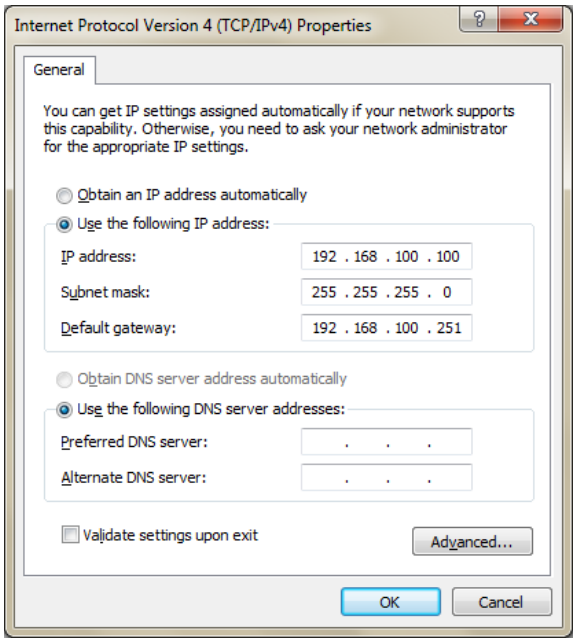
Double click on “Internet Protocol Version 4 (TCP/IPv4)” to enter its properties.



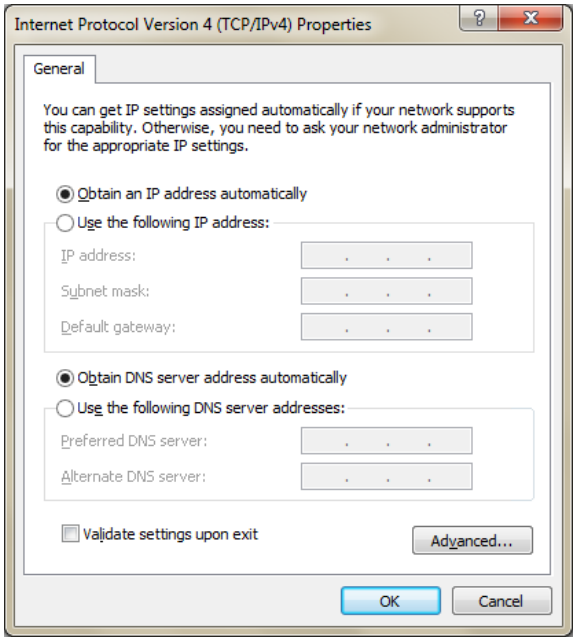
Step 7:

In AP mode, your computer cannot get dynamically assigned IP address through a wired LAN connection to the router. So you need to manually set IP address, subnet mask, and default gateway (LAN interface IP of the router), and then click “OK” to apply.

Default LAN interface in AP mode: 192.168.100.251



In Router mode, your computer can get dynamically assigned IP address through a wired LAN connection to the router. So select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, and then click “OK” to apply.



Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

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

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.