WELL WRC8500AN
Dual Gigabit Router

User's Manual

Table of Contents

1 Introduction

Congratulations on becoming the owner of the 802.11n WLAN Gigabit Router. You will now be able to access the Internet using your high-speed xDSL/Cable modem connection.

This User Guide will show you how to connect your 802.11n WLAN Gigabit Router, and how to customize its configuration to get the most out of your new product.

Features

The list below contains the main features of the device and may be useful to users with knowledge of networking protocols. If you are not an experienced user, the chapters throughout this guide will provide you with enough information to get the most out of your device.

Features include:

- 10/100/1000 Mbps Ethernet router to provide Internet connectivity to all computers on your LAN
- Network address translation (NAT) functions to provide security for your LAN
- Network configuration through DHCP Server and DHCP Client
- Services including IP route and DNS configuration, RIP, and IP
- Supports remote software upgrades
- Plug & Play, Auto Configuration / Auto Provisioning
- User-friendly configuration program accessed via a web browser

The 802.11n WLAN Gigabit Router has the internal Ethernet switch allows for a direct connection to a 10/100/1000 Mbps Ethernet network via an RJ-45 interface, with LAN connectivity for both the 802.11n WLAN Gigabit Router and a co-located PC or other Ethernet-based device.

Device Requirements

In order to use the 802.11n WLAN Gigabit Router, you must have the following:

- One RJ-45 Broadband Internet connection via cable modem or xDSL modem
- Instructions from your ISP on what type of Internet access you will be using, and the addresses needed to set up access
- One or more computers each containing an Ethernet card (10/100/1000 Mbps network interface card (NIC))
- TCP/IP protocol for each PC
- For system configuration using the supplied
  a. web-based program: a web browser such as Internet Explorer v7 or later. Note that version 7 of each browser is the minimum version requirement – for optimum display

quality, use Internet Explorer v8

Note

You do not need to use a hub or switch in order to connect more than one Ethernet PC to your device. Instead, you can connect up to four Ethernet PCs directly to your device using the ports labeled Ethernet on the rear panel.

Using this Document

Notational conventions

- Acronyms are defined the first time they appear in the text and also in the glossary.
- For brevity, the 802.11n WLAN Gigabit Router is referred to as "the device".
- The term *LAN* refers to a group of Ethernet-connected computers at one site.

Typographical conventions

- *Italic* text is used for items you select from menus and drop-down lists and the names of displayed web pages.
- **Bold** text is used for text strings that you type when prompted by the program, and to emphasize important points.

Special messages

This document uses the following icons to draw your attention to specific instructions or explanations.

Note

Provides clarifying or non-essential information on the current topic.

Definition

Explains terms or acronyms that may be unfamiliar to many readers. These terms are also included in the Glossary.

WARNING

Provides messages of high importance, including messages relating to personal safety or system integrity.

Getting Support

Supplied by:
Helpdesk Number:
Website:

2 Getting to know the device

Computer / System requirements

- 1. Pentium 200MHZ processor or above

- 2. Windows 98SE, Windows Me, Windows 2000, Windows XP, Windows Vista and Windows 7
- 3. 64MB of RAM or above
- 4. 25MB free disk space

Package Contents

1. 802.11n WLAN Gigabit Router
2. CD-ROM (Software & Manual)
3. Quick Installation Guide
4. Ethernet Cable (RJ-45)
5. Power Adapter
6. Detachable Antenna (Optional)

LED meanings & activations

Front Panel

The front panel contains lights called Light Emitting Diodes (LEDs) that indicate the status of the unit.

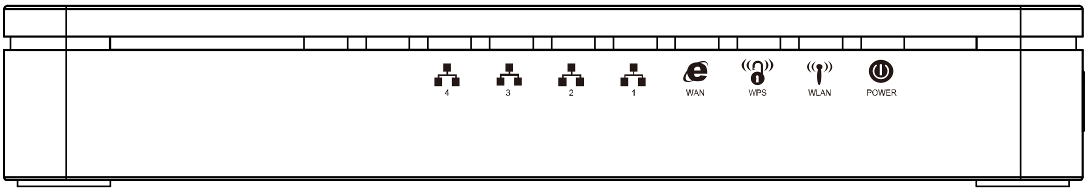


Figure 1: Front Panel and LEDs

Label	Color	Function
POWER	green	On: device is powered on Off: device is powered off
WLAN	green	On: WLAN link established and active Blink: Valid Wireless packet being transferred
WPS	green	Off: WPS link isn't established and active Blink: Valid WPS packet being transferred
WAN & LAN 1/2/3/4	green	On: 10/100MB Ethernet connection established and active Off: No Ethernet connection Blink: Valid Ethernet packet being transferred
	Amber	On: 1000MB Ethernet connection established and active Off: No Ethernet connection Blink: Valid Ethernet packet being transferred

Rear and Right Panel and bottom Side

The rear and right panel and bottom side contains a *Restore Defaults* button, the ports for the unit's data and power connections.

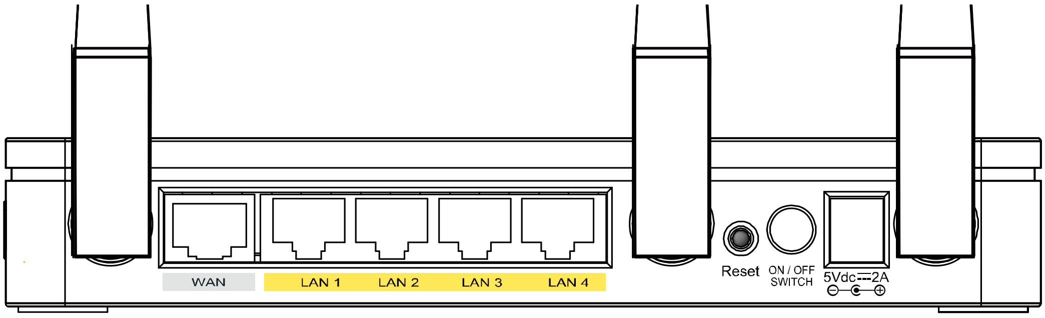


Figure 2: Rear Panel Connections

**** Actual ANTENNA may vary depending on model.***

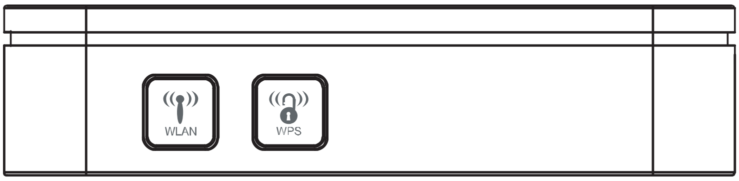


Figure 3: Right Panel Connections

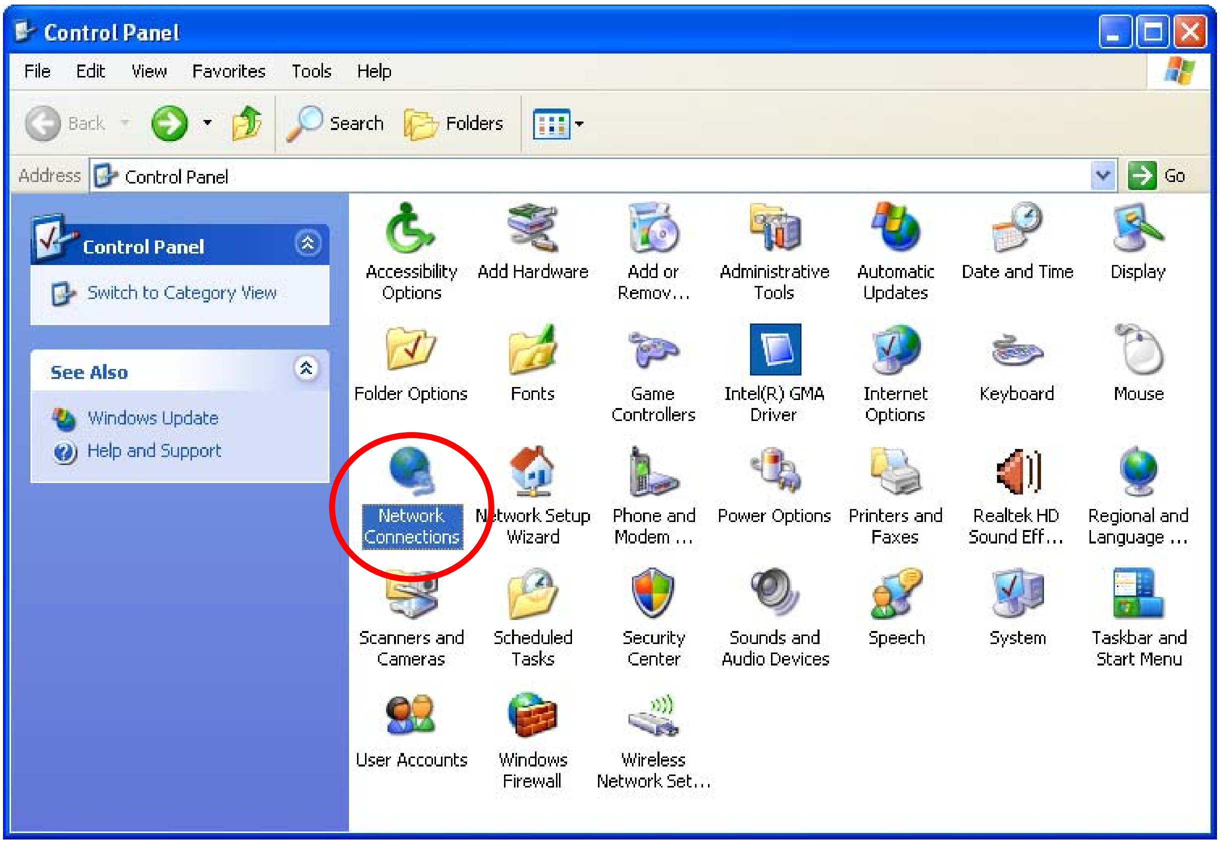
Label	Function
ANTENNA (Optional)	Option 1: 3 fixed ANTENNA Option 2: 3 detachable ANTENNA
ON/OFF SWITCH	Power on/off the device
POWER	Connects to the supplied power adaptor
LAN 4/3/2/1	Connects the device via LAN Ethernet to up to 4 PCs
WAN	Connects the device via WAN Ethernet to xDSL / Cable Modem
WLAN	Press this button for at least 2 full second to turn off/on wireless signals
WPS	Press this button for at least 0.5 full seconds and the WPS LED will flash to start WPS. Now go to the wireless adapter or device and press its WPS button. Make sure to press the button within 120 seconds (2 minutes) after pressing the router's WPS button.
RESET	Reset button. RESET the 802.11n WLAN router to its default settings. Press this button for at least 2 full seconds to RESET device to its default settings.

3 Computer configurations under different OS, to obtain IP address automatically

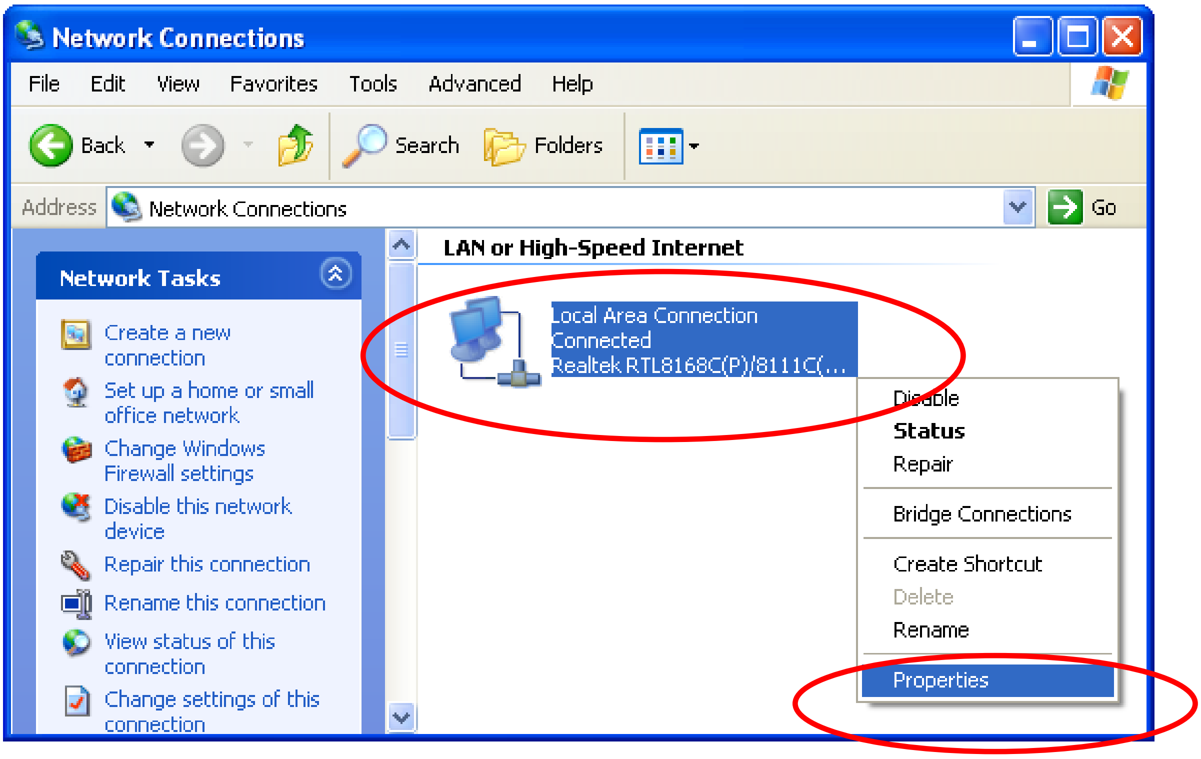
Before starting the 802.11n WLAN Gigabit Router configuration, please kindly configure the PC computer as below, to have automatic IP address / DNS Server.

For Windows 98SE / ME / 2000 / XP

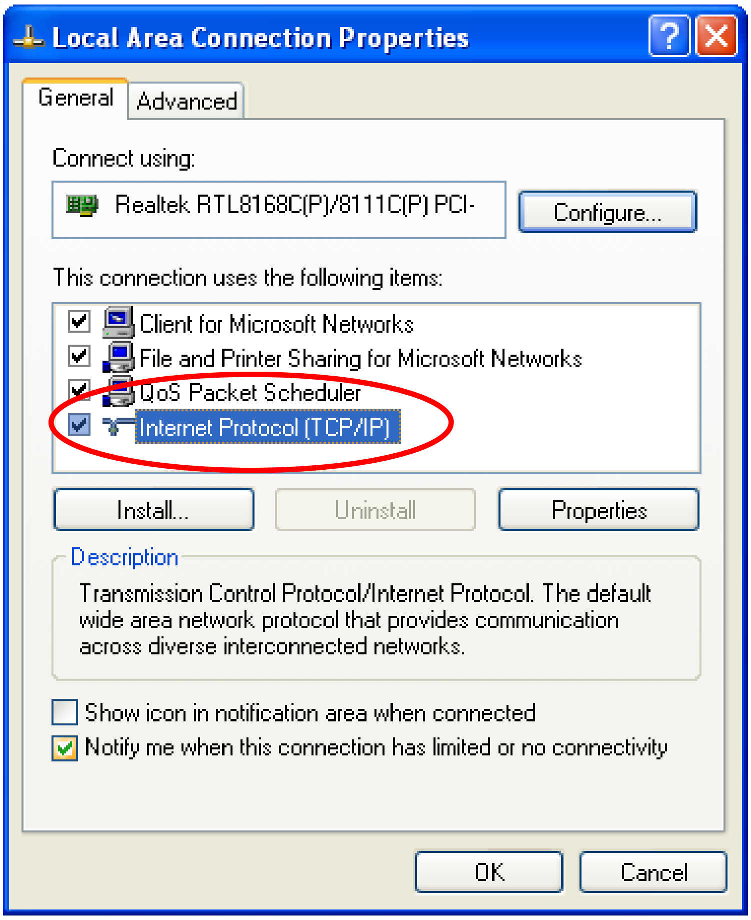
1. Click on "**Start**" -> "**Control Panel**" **(in Classic View)**. In the Control Panel, double click on "**Network Connections**" to continue.



2. Single RIGHT click on "**Local Area connection**", then click "**Properties**".


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections Go
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
LAN or High-Speed Internet
Local Area Connection
Connected
Realtek RTL8168C(P)/8111C(...
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties

3. Double click on "**Internet Protocol (TCP/IP)**".


Local Area Connection Properties
General Advanced
Install... Uninstall Properties
OK Cancel
Configure...

Connect using:

Realtek RTL8168C(P)/8111C(P) PCI-

This connection uses the following items:

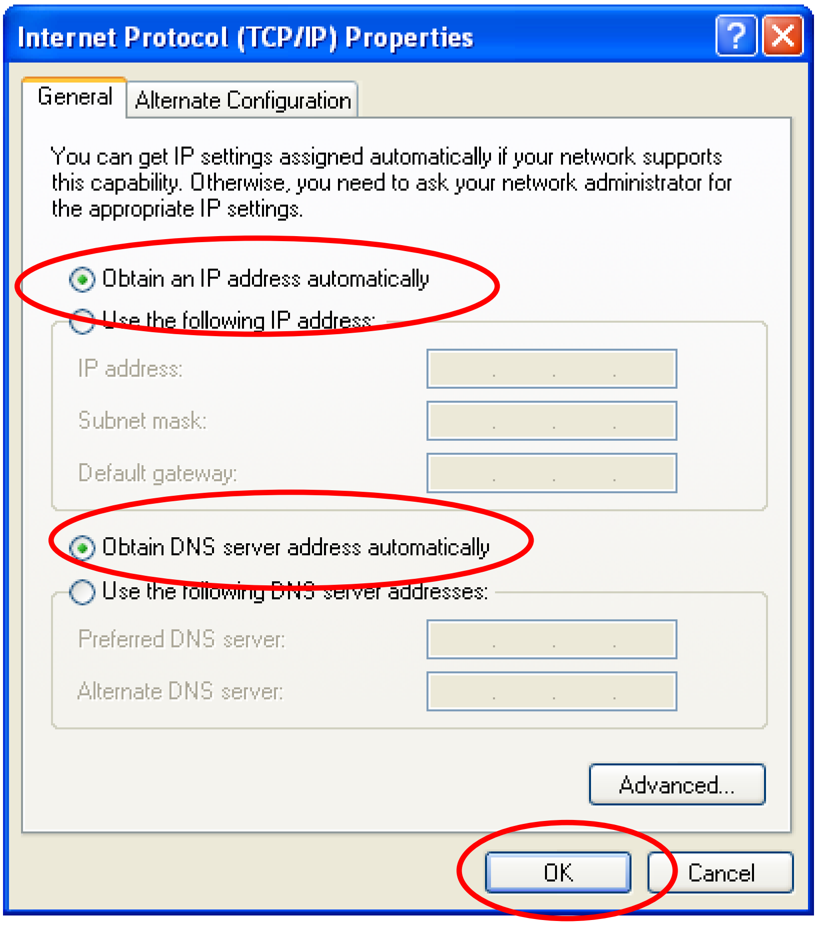
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

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

4. Check "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" then click on "**OK**" to continue.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

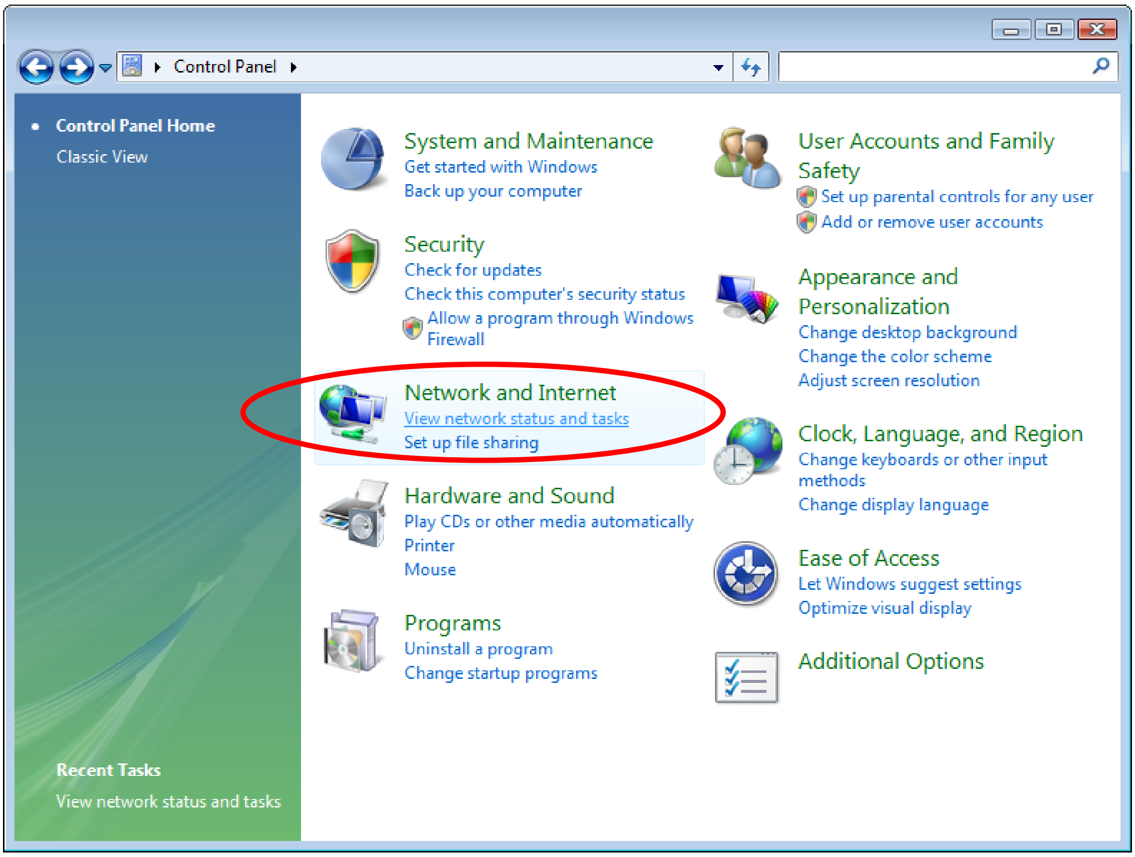
Preferred DNS server: . . .

Alternate DNS server: . . .

5. Click "**Show icon in notification area when connected**" (see screen image in 3. above) then Click on "**OK**" to complete the setup procedures.

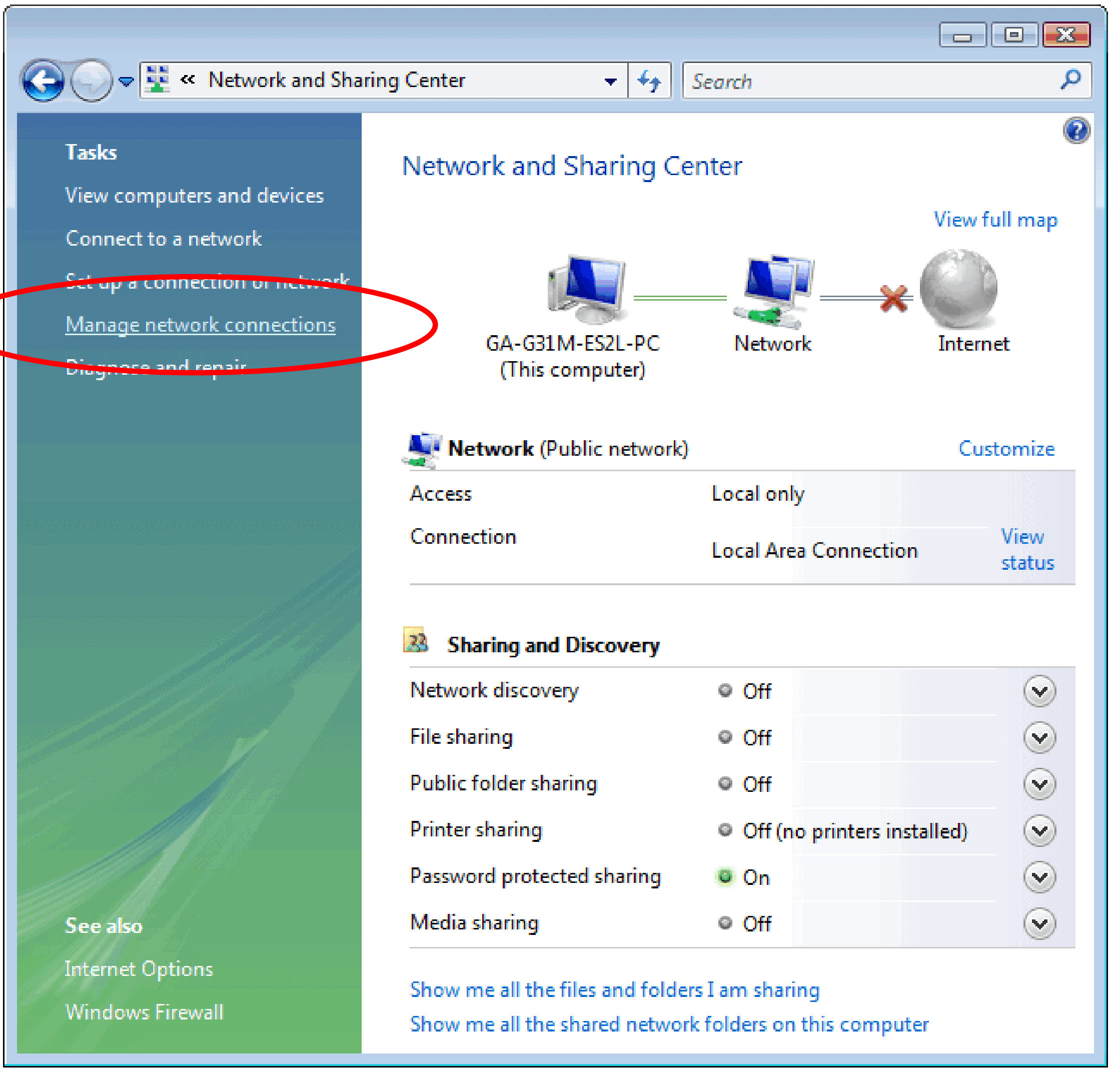
For Windows Vista-32/64

1. Click on "Start" -> "Control Panel" -> "View network status and tasks".



Control Panel
Control Panel Home
Classic View
System and Maintenance
Get started with Windows
Back up your computer
Security
Check for updates
Check this computer's security status
Allow a program through Windows Firewall
Network and Internet
View network status and tasks
Set up file sharing
Hardware and Sound
Play CDs or other media automatically
Printer
Mouse
Programs
Uninstall a program
Change startup programs
User Accounts and Family Safety
Set up parental controls for any user
Add or remove user accounts
Appearance and Personalization
Change desktop background
Change the color scheme
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display
Additional Options
Recent Tasks
View network status and tasks

2. In the Manage network connections, click on "**Manage network connections**" to continue.



Network and Sharing Center

Network (Public network)

Access	Local only
Connection	Local Area Connection

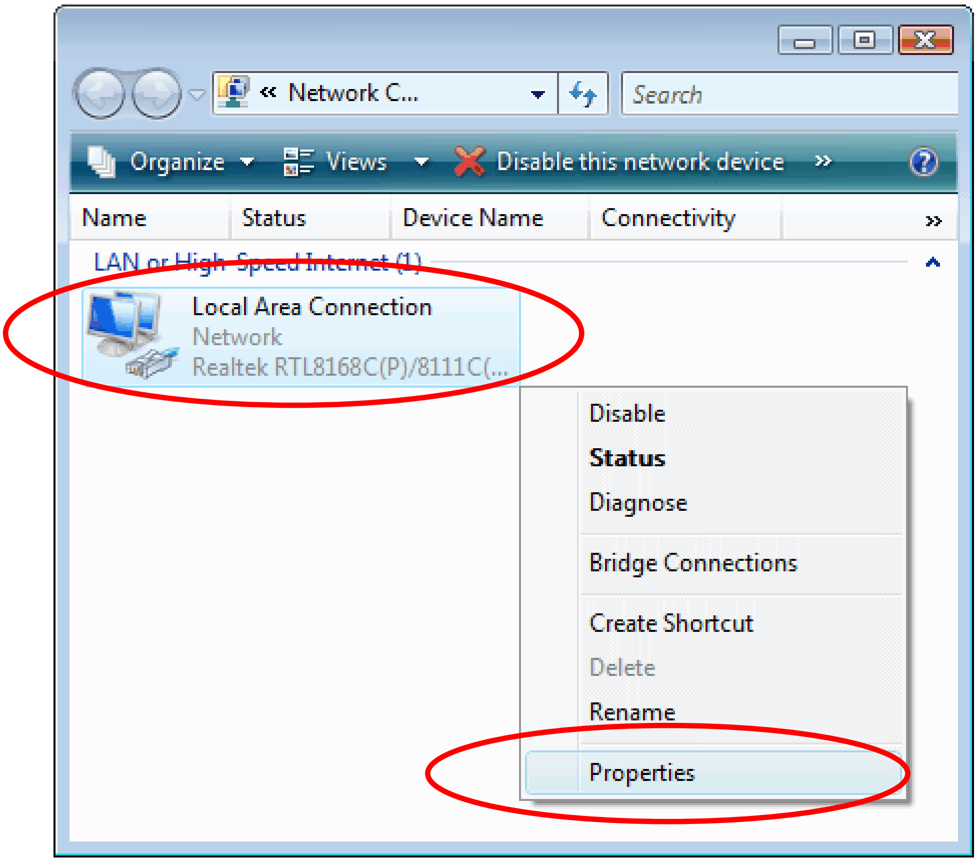
Sharing and Discovery

Network discovery	○ Off
File sharing	○ Off
Public folder sharing	○ Off
Printer sharing	○ Off (no printers installed)
Password protected sharing	● On
Media sharing	○ Off

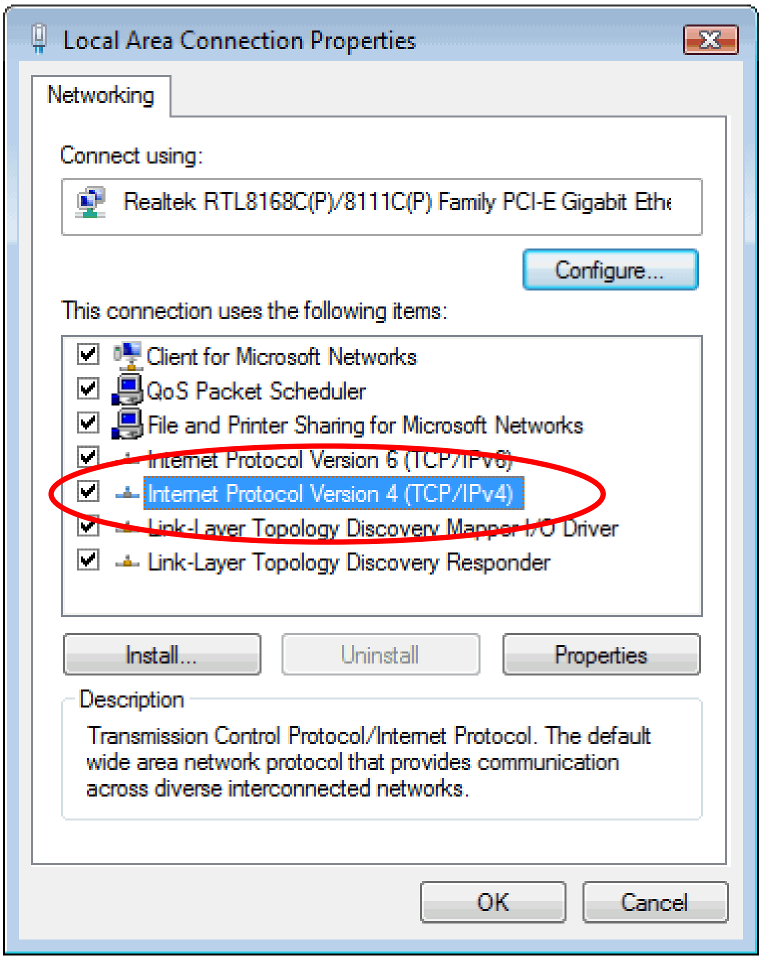
Show me all the files and folders I am sharing

Show me all the shared network folders on this computer

3. Single RIGHT click on "**Local Area connection**", then click "**Properties**".



4. The screen will display the information "**User Account Control**" and click "**Continue**" to continue.
5. Double click on "**Internet Protocol Version 4 (TCP/IPv4)**".



Local Area Connection Properties

Networking

Connect using:

Realtek RTL8168C(P)/8111C(P) Family PCI-E Gigabit Ethe

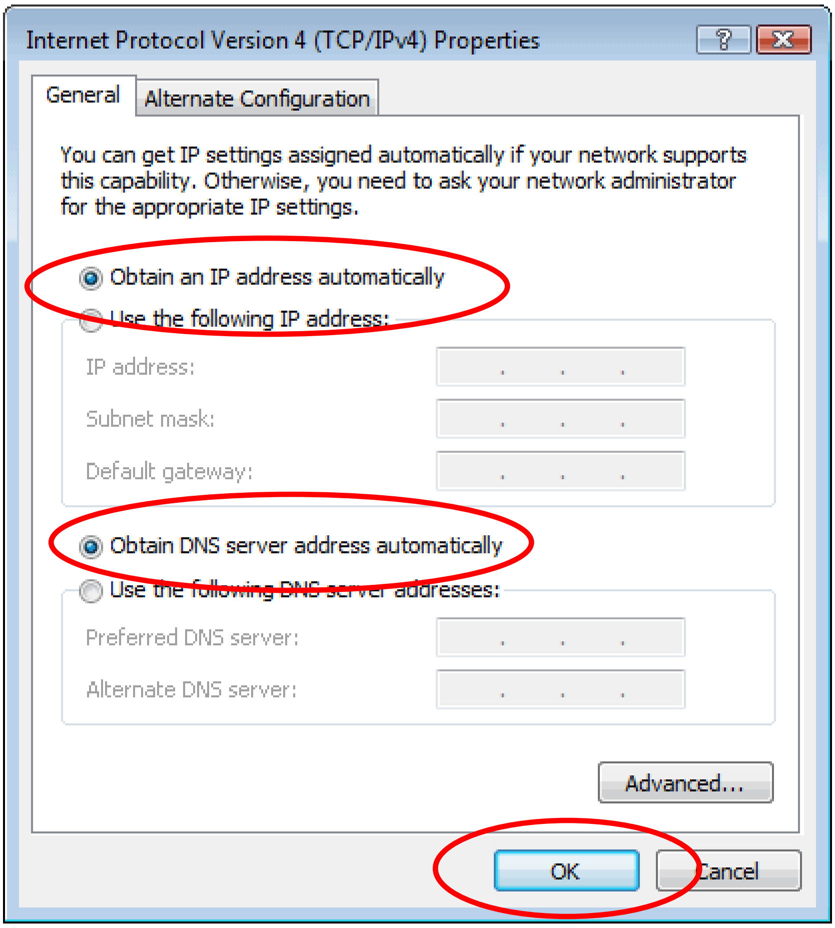
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

6. Check "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" then click on "**OK**" to continue.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

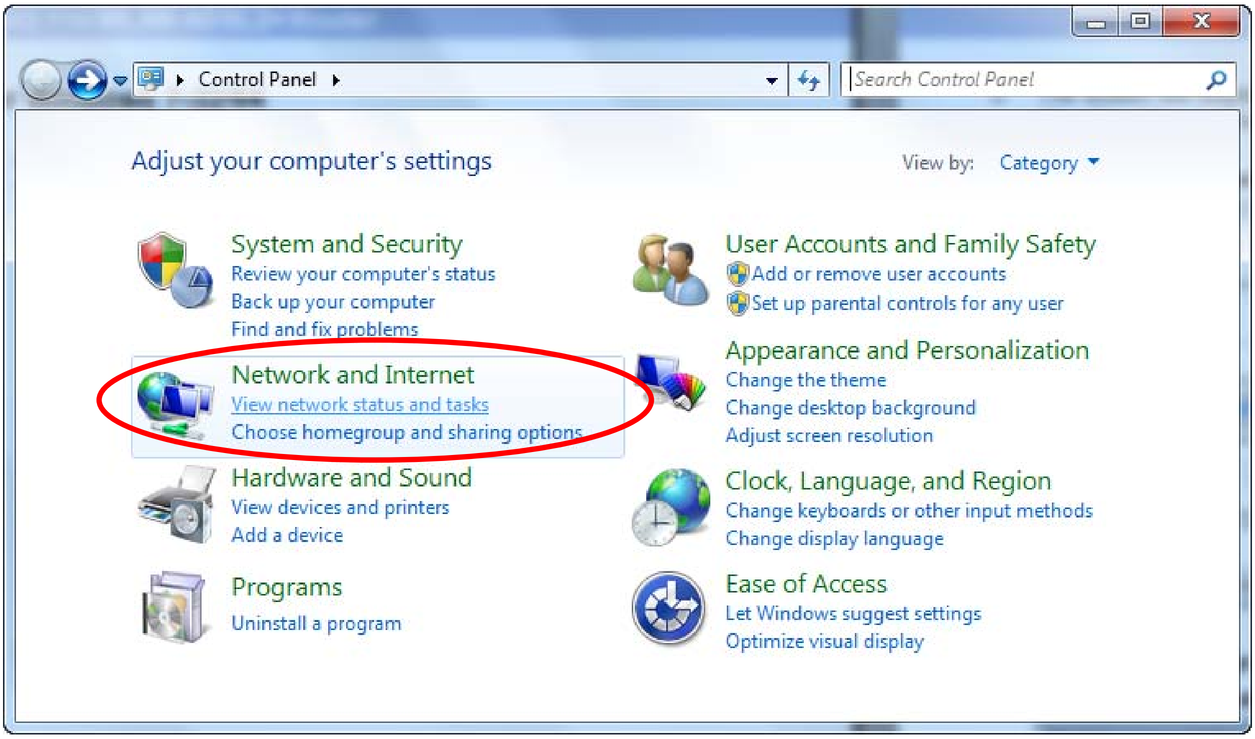
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

For Windows 7-32/64

1. Click on "Start" -> "Control Panel" (in Category View) -> "View network status and tasks".



Control Panel

Search Control Panel

Adjust your computer's settings

View by: Category

System and Security
Review your computer's status
Back up your computer
Find and fix problems

Network and Internet
View network status and tasks
Choose homegroup and sharing options

Hardware and Sound
View devices and printers
Add a device

Programs
Uninstall a program

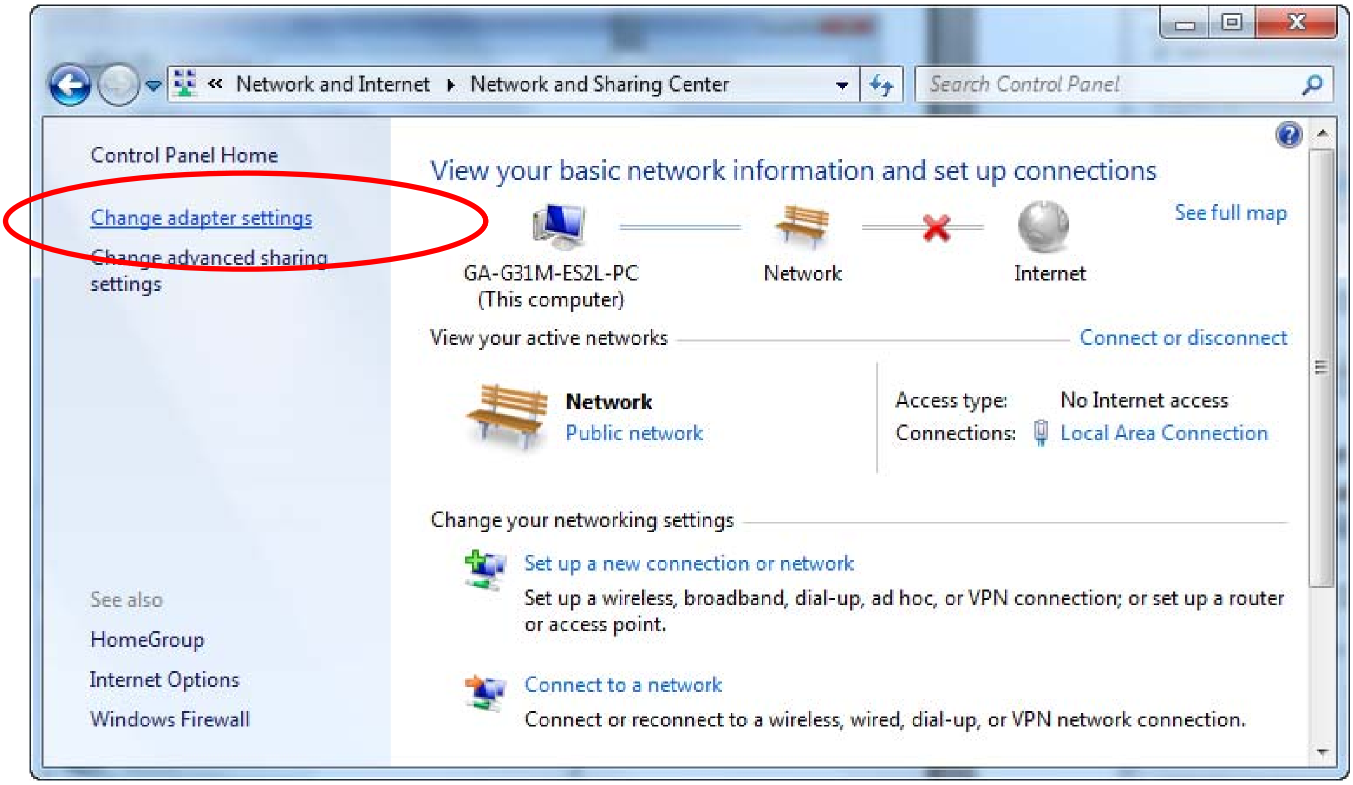
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user

Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution

Clock, Language, and Region
Change keyboards or other input methods
Change display language

Ease of Access
Let Windows suggest settings
Optimize visual display

2. In the Control Panel Home, click on "**Change adapter settings**" to continue.



« Network and Internet ▸ Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

See also

HomeGroup

Internet Options

Windows Firewall

View your basic network information and set up connections

See full map

GA-G31M-ES2L-PC (This computer) — Network — Internet

View your active networks

Connect or disconnect

Network
Public network

Access type: No Internet access

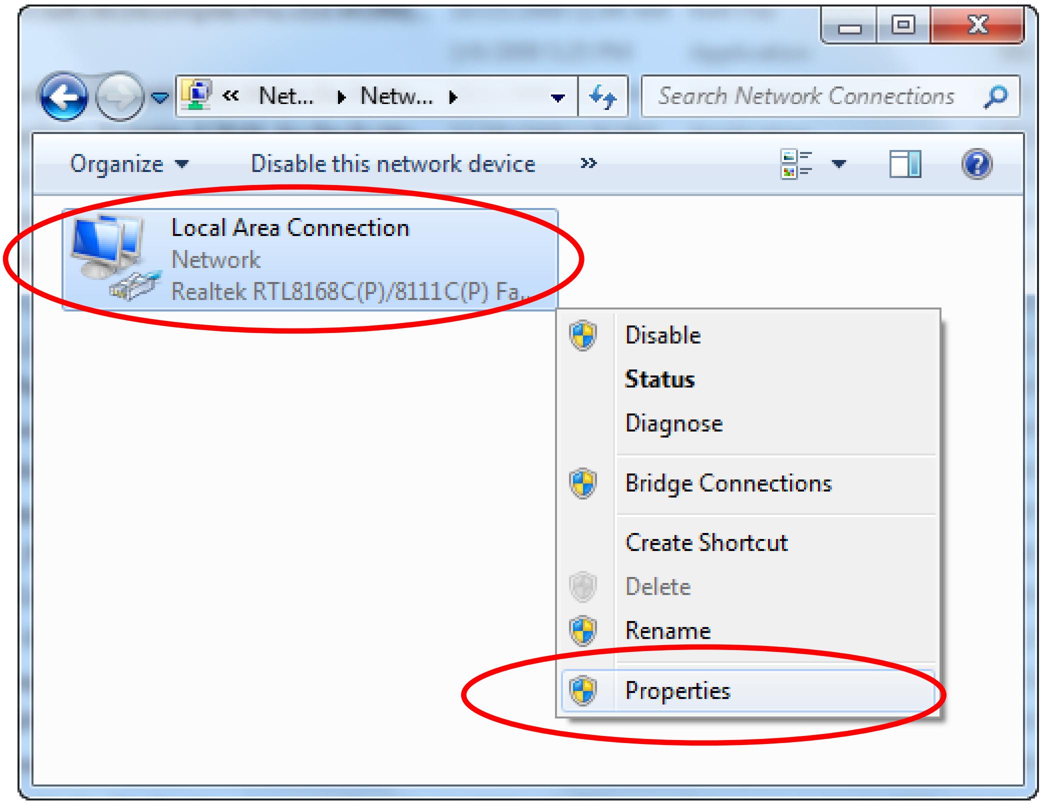
Connections: Local Area Connection

Change your networking settings

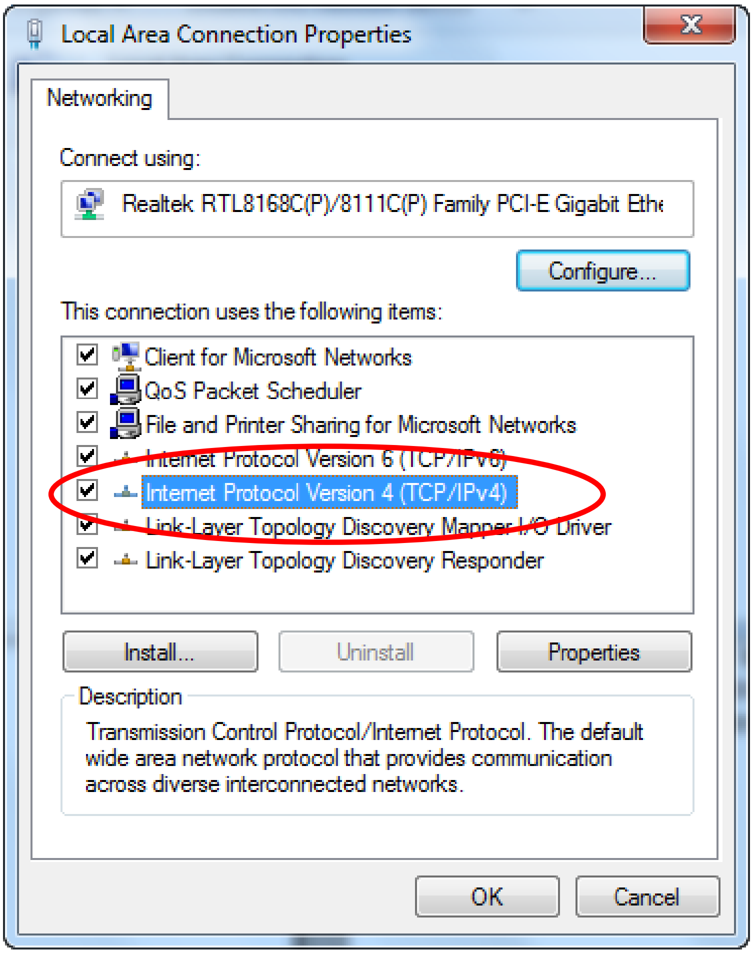
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

3. Single RIGHT click on "**Local Area Connection**", then click "**Properties**".



4. Double click on "**Internet Protocol Version 4 (TCP/IPv4)**".



Connect using:

Realtek RTL8168C(P)/8111C(P) Family PCI-E Gigabit Ethe

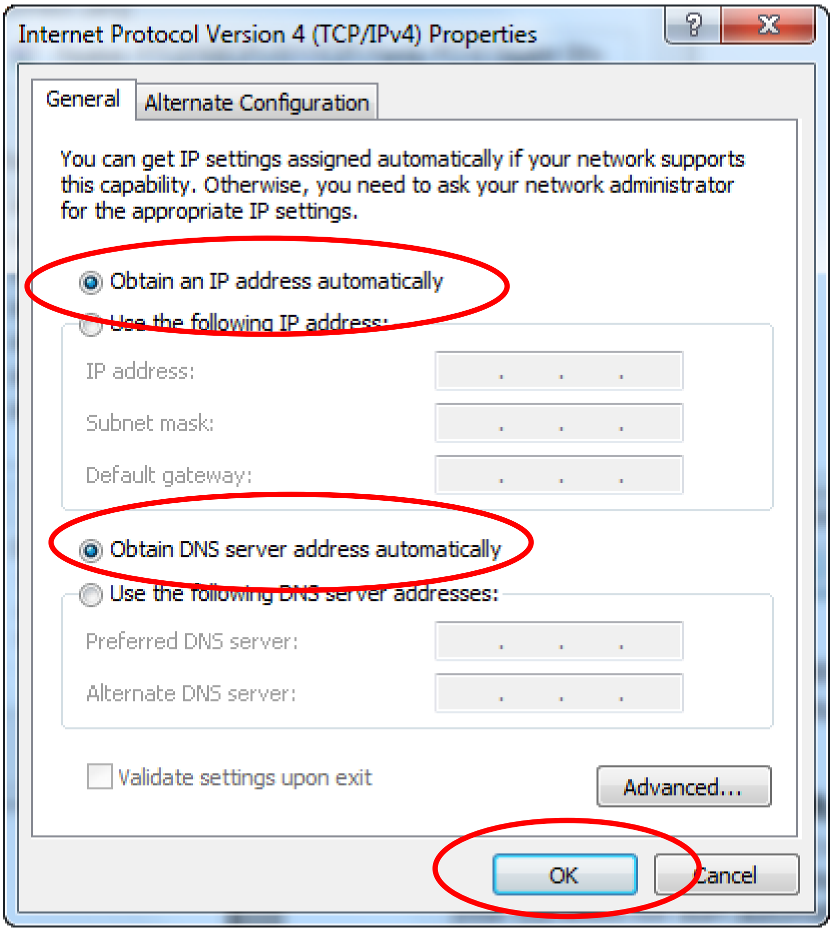
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. Check "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" then click on "**OK**" to continue.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

4 Connecting your device

This chapter provides basic instructions for connecting the 802.11n WLAN Gigabit Router to a computer or LAN and to the Internet.

In addition to configuring the device, you need to configure the Internet properties of your computer(s). For more details, see the following sections:

- *Configuring Ethernet PCs*

This chapter assumes that you have already established a DSL/Cable service with your Internet service provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters for additional configuration instructions.

Connecting the Hardware

This section describes how to connect the device to the wall phone port, the power outlet and your computer(s) or network.

⚠ **WARNING**

Before you begin, turn the power off for all devices. *These include your computer(s), your LAN hub/switch (if applicable), and the device.*

The diagram below illustrates the hardware connections. The layout of the ports on your device may vary from the layout shown. Refer to the steps that follow for specific instructions.

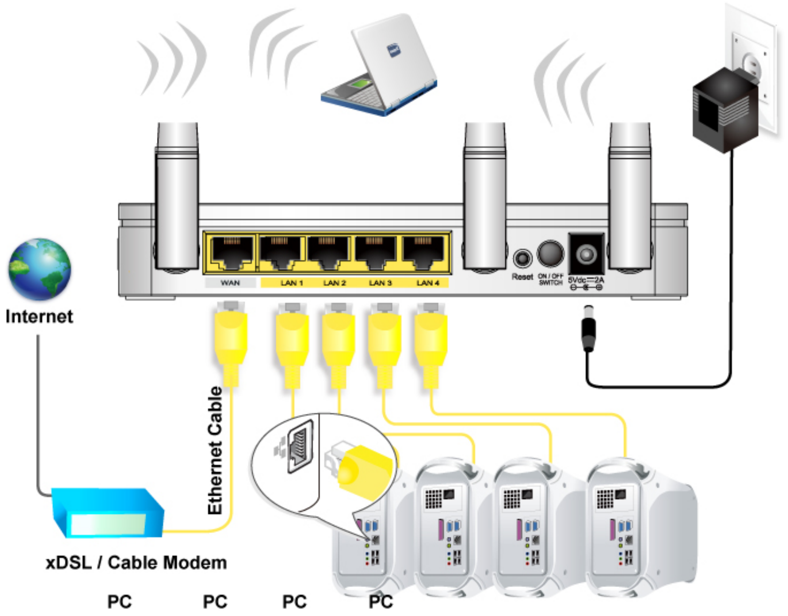


Figure 4: Overview of Hardware Connections

Step 1. Connect the Ethernet cable to WAN Port

Connect the RJ45 Ethernet cable from your xDSL/Cable Modem's Ethernet port to 802.11n WLAN Gigabit Router's WAN Port.

Step 2. Connect the Ethernet cable to LAN Port

Connect the supplied RJ45 Ethernet cable from your PC's Ethernet port to any of the 4 802.11n WLAN Gigabit Router's LAN Ports.

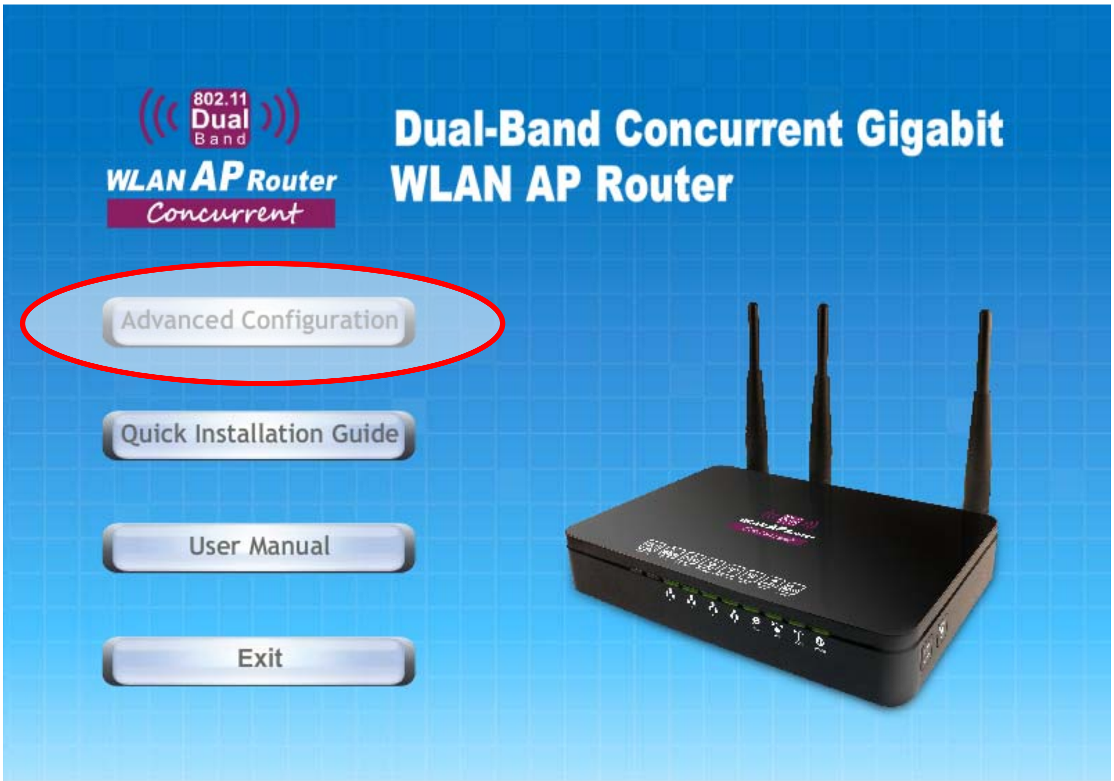
Step 3. Attach the power connector

Connect the power adapter to the power inlet "**POWER**" of the 802.11n WLAN Gigabit Router and turn the power switch "**ON/OFF SWITCH**" of your 802.11n WLAN Gigabit Router on.

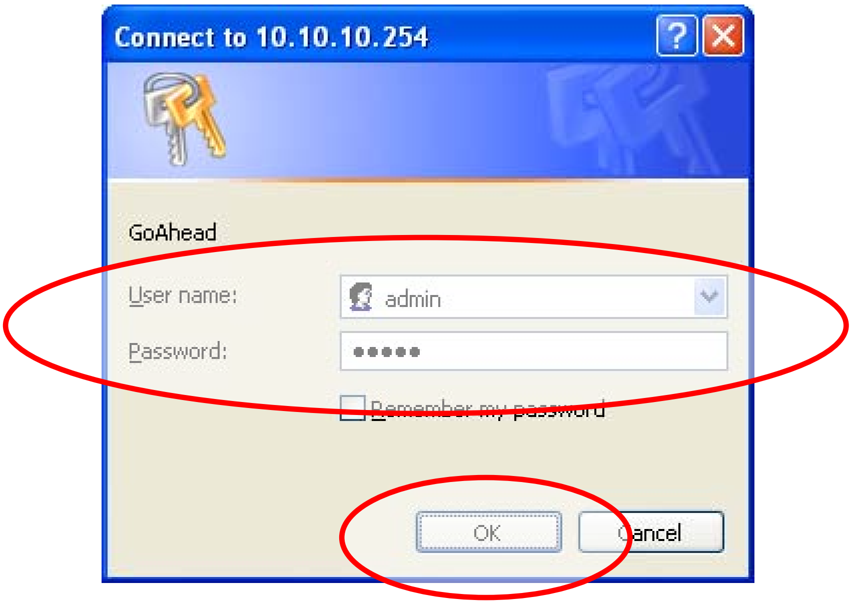
**** Actual ANTENNA may vary depending on model***

802.11n WLAN Gigabit Router Configuration

1. Please insert the supplied CD into your CD-ROM drive.
2. The CD should auto-start, displaying the window shown in 3. below. If your CD does not start automatically, go to Windows Explorer, Select your CD drive and double click **autorun.exe**.
3. To configure the device, please click on **Advanced Configuration** button.



4. Please enter the User Name: **admin** and Password: **admin** and then click on **OK** button.



Connect to 10.10.10.254

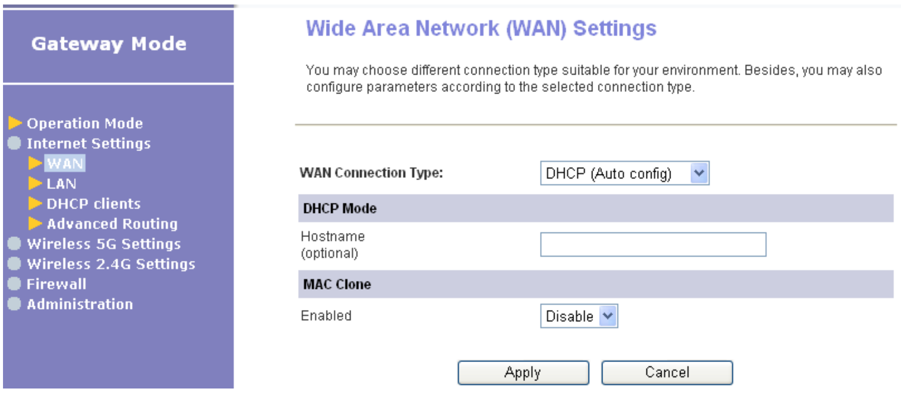
GoAhead

User name: admin

Password: •••••

□ Remember my password

5. From the **Internet Settings** menu, click on **WAN**.



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: DHCP (Auto config)

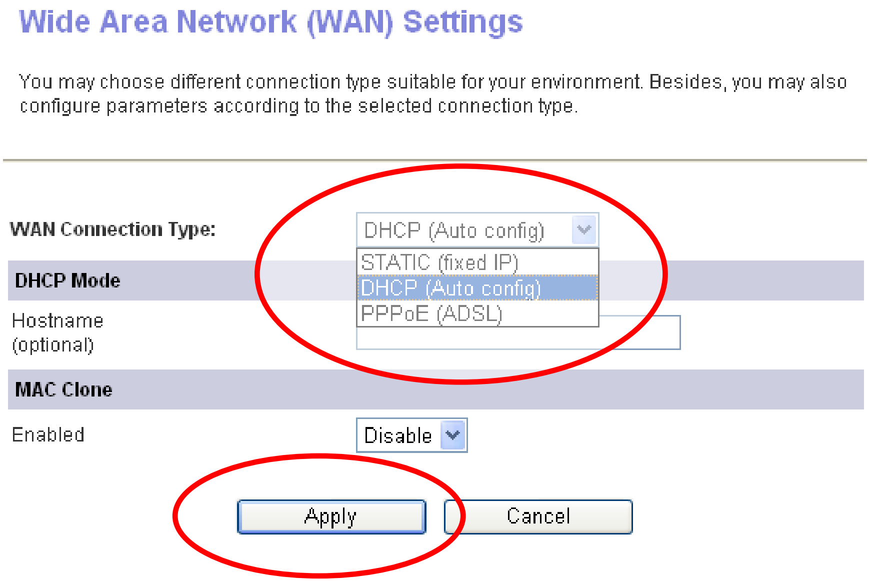
DHCP Mode

Hostname (optional)

MAC Clone

Enabled: Disable

6. Select the WAN Connection Type **STATIC (fixed IP)** , **DHCP (Auto config)** or **PPPoE (ADSL)** and enter related parameters that your ISP (Internet Services Provider) or Network Administrator provided and then click on **Apply** button.



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: DHCP (Auto config)

DHCP Mode

Hostname (optional)

MAC Clone

Enabled: Disable

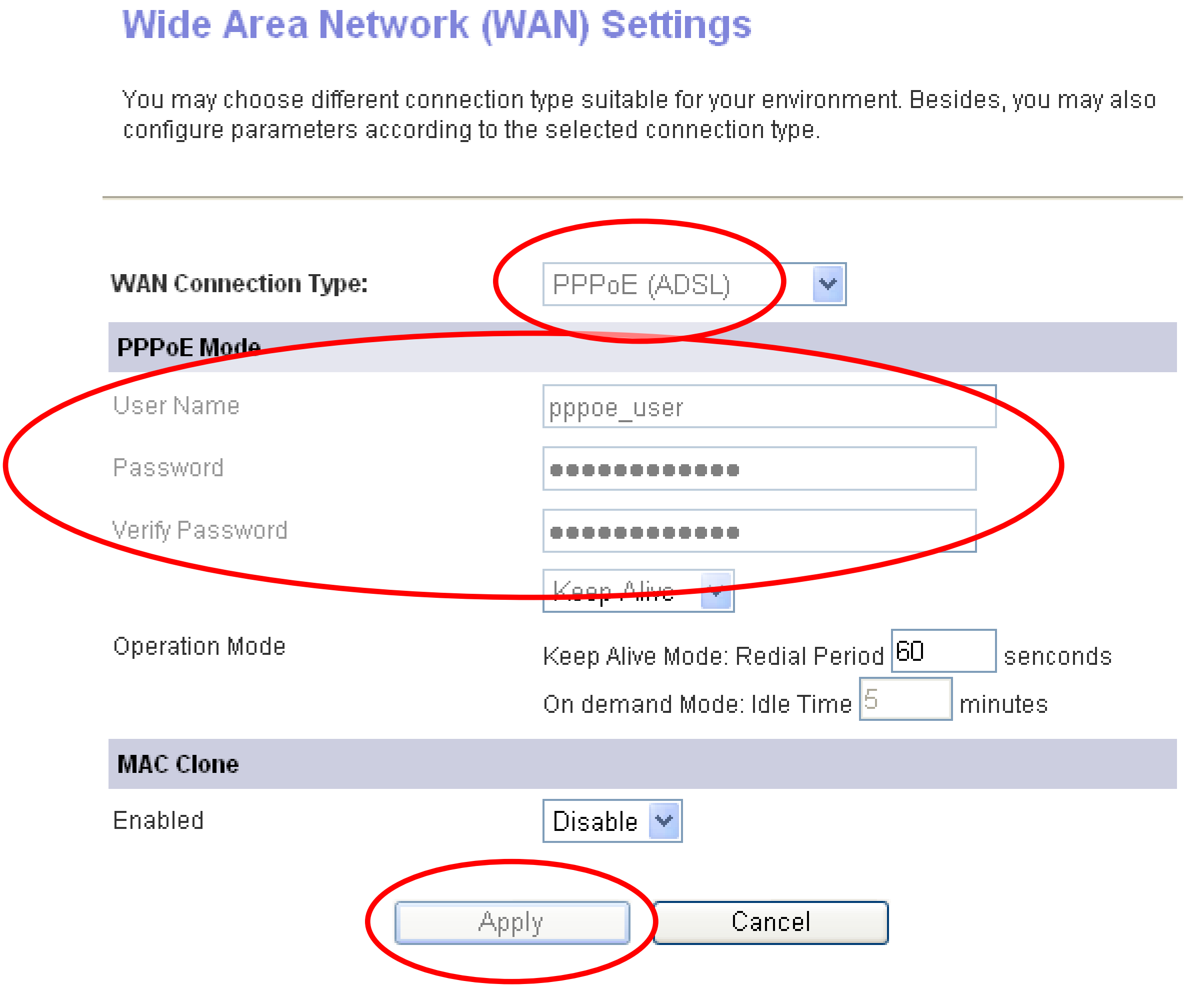
Examples

6-1. PPPoE (ADSL)

Select **PPPoE (ADSL)** from WAN Connection Type drop-down list

Enter **User Name**, **Password** and **Verify Password** offered by the ISP

Click on **Apply** button



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: PPPoE (ADSL)

PPPoE Mode

User Name: pppoe_user

Password: ●●●●●●●●●●●●

Verify Password: ●●●●●●●●●●●●

Operation Mode: Keep Alive

Keep Alive Mode: Redial Period 60 senconds

On demand Mode: Idle Time 5 minutes

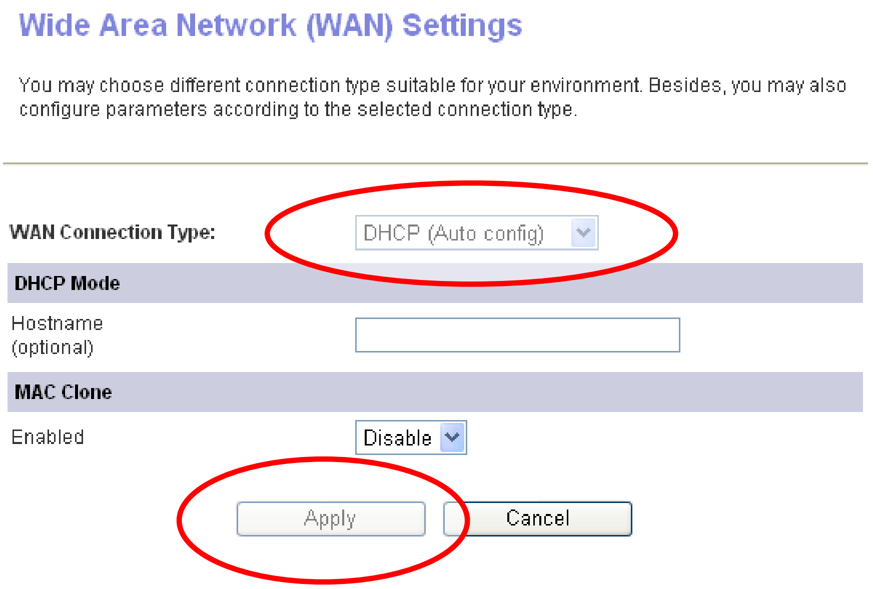
MAC Clone

Enabled: Disable

6-2. DHCP (Auto config)

Select **DHCP (Auto config)** from WAN Connection Type drop-down list

Click on **Apply** button



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

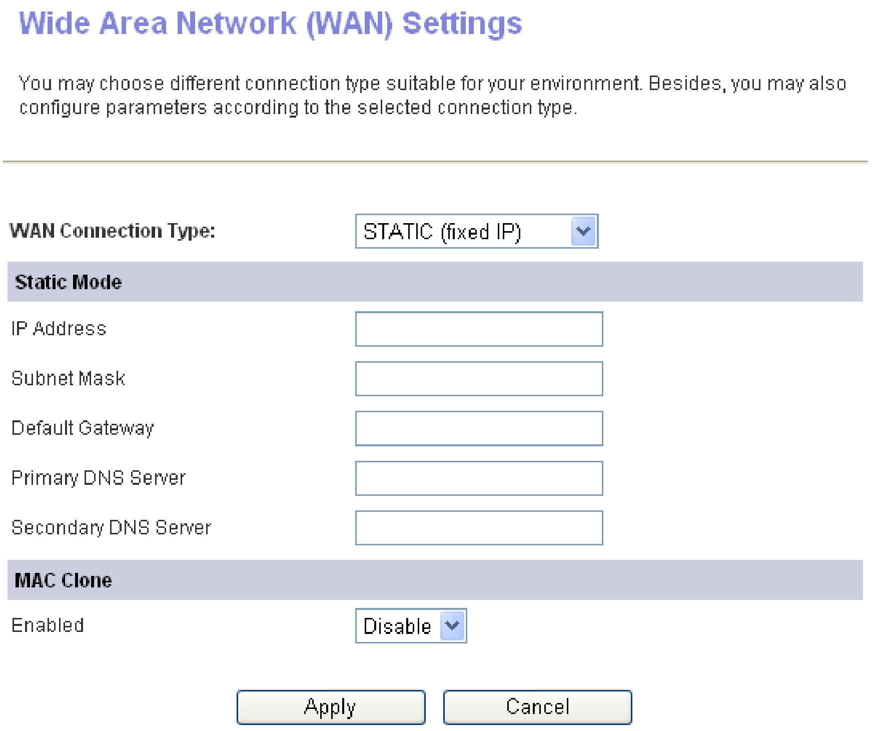
WAN Connection Type:	DHCP (Auto config)
DHCP Mode	
Hostname (optional)	
MAC Clone	
Enabled	Disable

6-3. STATIC (fixed IP)

Select **STATIC (fixed IP)** from WAN Connection Type drop-down list

Config **IP Address, Subnet Mask, Default Gateway, Primary DNS Server** and **Secondary DNS Server** offered by ISP (Internet Services Provider) or Network Administrator

Click on **Apply** button

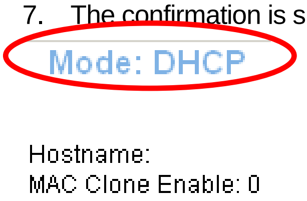


Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type:	STATIC (fixed IP)
Static Mode	
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
MAC Clone	
Enabled	Disable

7. The confirmation is shown as screen below:



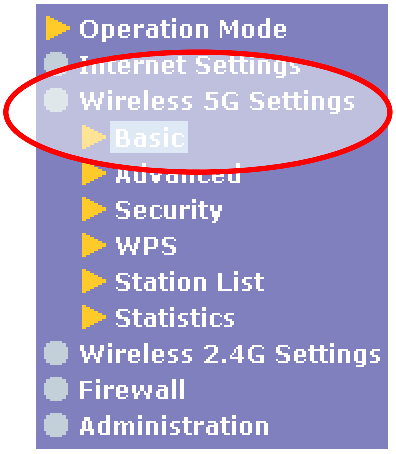
Mode: DHCP

Hostname:
MAC Clone Enable: 0

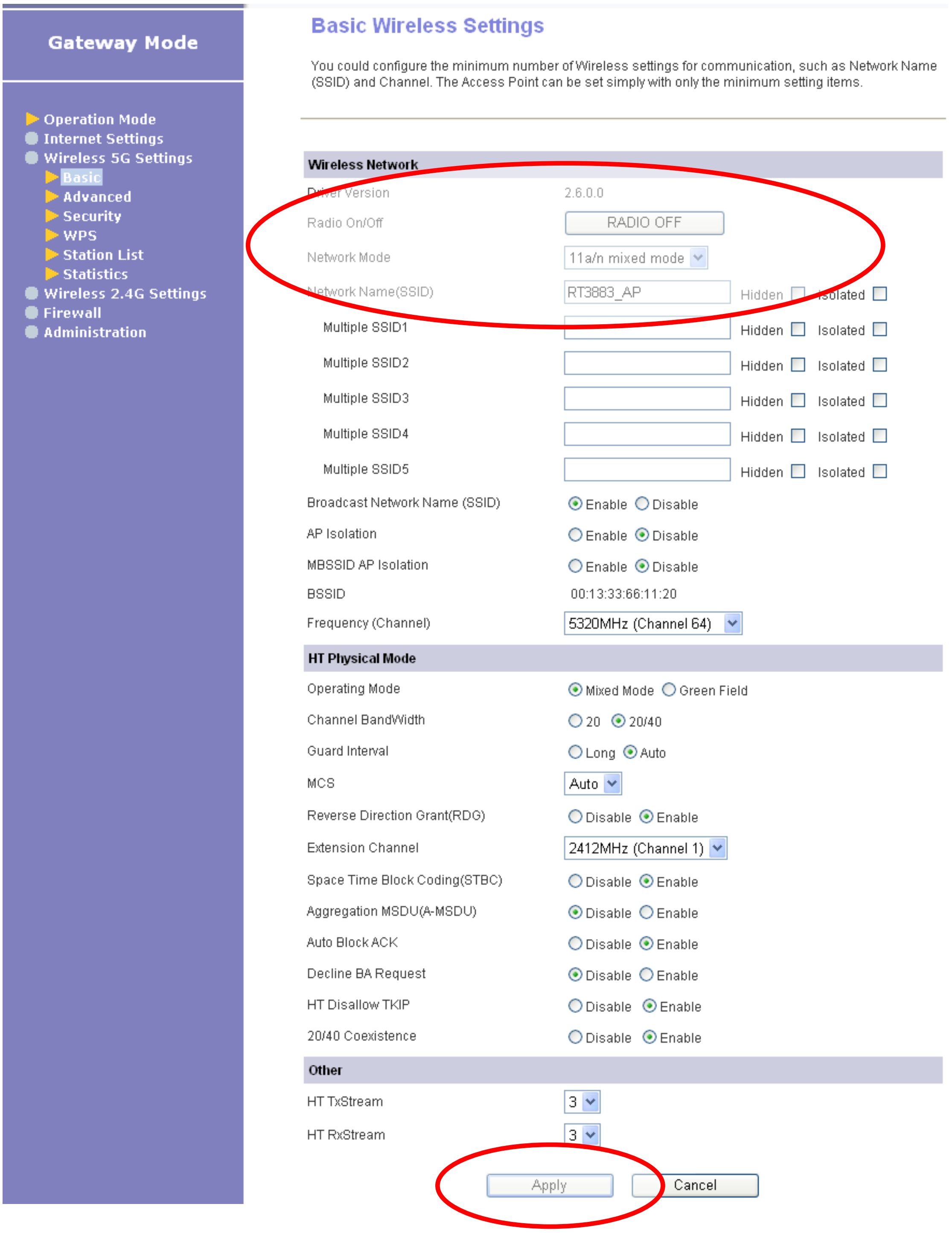
**** Actual ANTENNA may vary depending on setting***

Wireless 5G Settings

8. From the **Wireless 5G Settings** menu, click on **Basic**.



9. Choose the Network Mode if necessary, as 11a only, 11a/n mixed mode and 11n only(5G) (**the default settings Network Mode = 11a/n mixed mode**). For example, you choose 11a/n mixed mode.
10. Please enter the Network Name(SSID) and if you want to change (**the default settings Radio On/Off = On, Network Name(SSID) = RT3883_AP**).
11. Please click **Apply** button to continue.



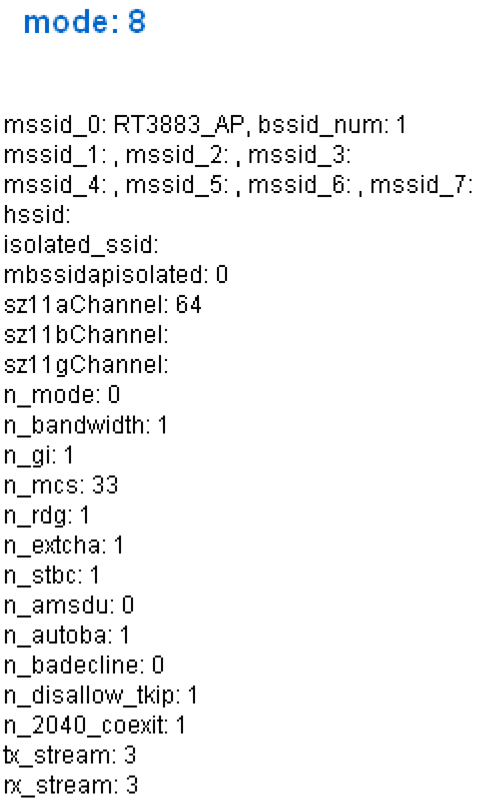
Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
Driver Version	2.6.0.0
Radio On/Off	RADIO OFF
Network Mode	11a/n mixed mode
Network Name(SSID)	RT3883_AP Hidden □ Isolated □
Multiple SSID1	Hidden □ Isolated □
Multiple SSID2	Hidden □ Isolated □
Multiple SSID3	Hidden □ Isolated □
Multiple SSID4	Hidden □ Isolated □
Multiple SSID5	Hidden □ Isolated □
Broadcast Network Name (SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	00:13:33:66:11:20
Frequency (Channel)	5320MHz (Channel 64)
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Auto
MCS	Auto
Reverse Direction Grant(RDG)	○ Disable ● Enable
Extension Channel	2412MHz (Channel 1)
Space Time Block Coding(STBC)	○ Disable ● Enable
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
HT Disallow TKIP	○ Disable ● Enable
20/40 Coexistence	○ Disable ● Enable
Other	
HT TxStream	3
HT RxStream	3

Apply Cancel

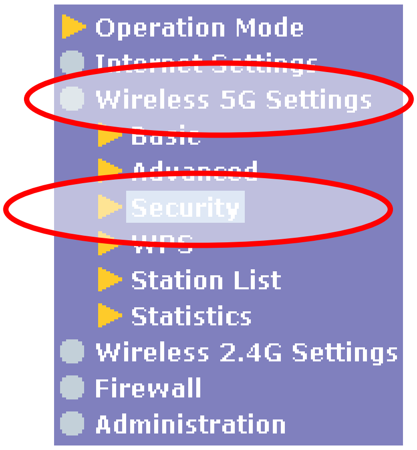
12. The confirmation is shown as screen below:



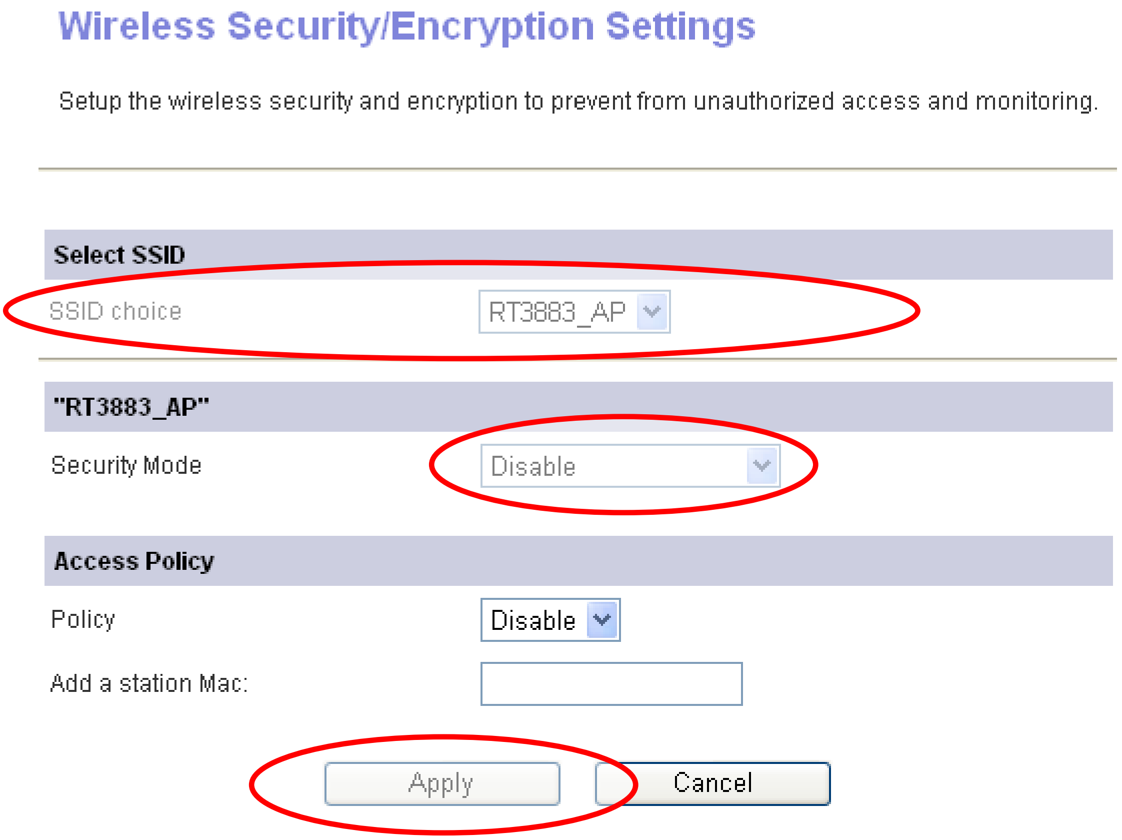
```
mode: 8


mssid_0: RT3883_AP, bssid_num: 1
mssid_1: , mssid_2: , mssid_3:
mssid_4: , mssid_5: , mssid_6: , mssid_7:
hssid:
isolated_ssid:
mbssidapisolated: 0
sz11aChannel: 64
sz11bChannel:
sz11gChannel:
n_mode: 0
n_bandwidth: 1
n_gi: 1
n_mcs: 33
n_rdg: 1
n_extcha: 1
n_stbc: 1
n_amsdu: 0
n_autoba: 1
n_badecline: 0
n_disallow_tkip: 1
n_2040_coexit: 1
tx_stream: 3
rx_stream: 3
```

**** Actual ANTENNA may vary depending on setting***

13. From the **Wireless 5G Settings** menu, click on **Security**.



14. Choose the Security Mode if necessary, as Disable / OPENWEP / SHAREDWEP / WEPAUTO / WPA-PSK / WPA2-PSK and WPAPSKWPA2PSK **(the default settings Security Mode = Disable)**. For example, you choose the Disable Mode.
15. Please click **Apply** button to continue.



Wireless Security/Encryption Settings

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

Select SSID

SSID choice: RT3883_AP

"RT3883_AP"

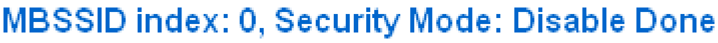
Security Mode: Disable

Access Policy

Policy: Disable

Add a station Mac:

16. The confirmation is shown as screen below:



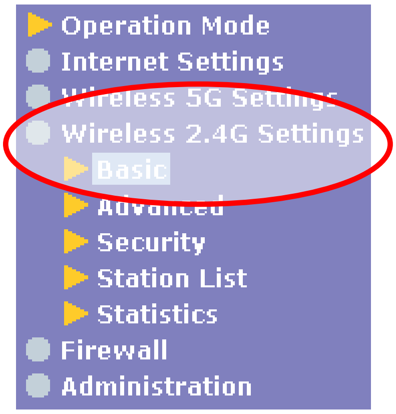
MBSSID index: 0, Security Mode: Disable Done

**** Actual ANTENNA may vary depending on setting***

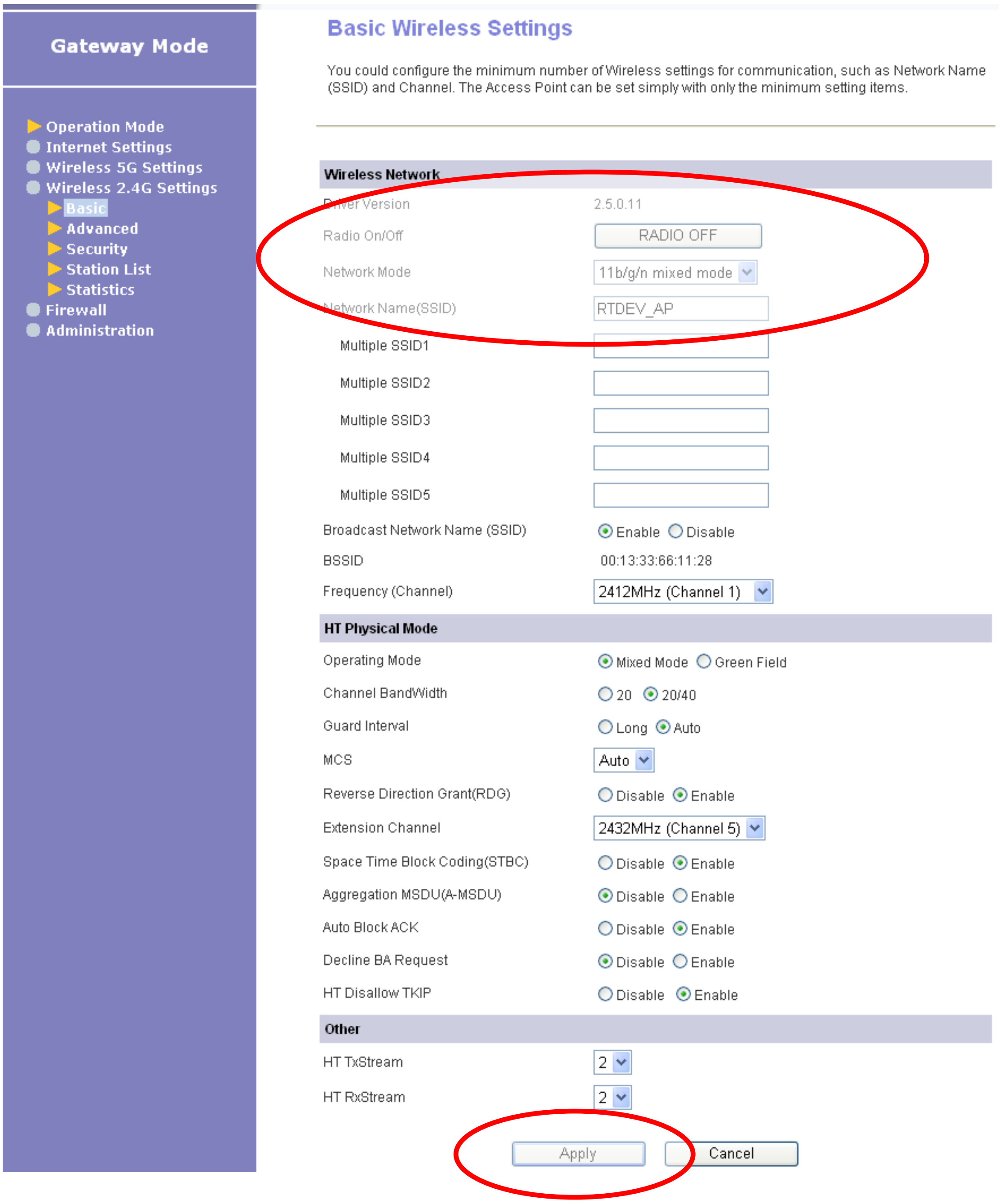
17. WLAN Router has been configured completely, and suitable for Wireless and Internet Connections.

Wireless 2.4G Settings

18. From the **Wireless 2.4G Settings** menu, click on **Basic**.



19. Choose the Network Mode if necessary, as 11b/g mixed mode, 11b only, 11g only, 11b/g/n mixed mode and 11n only(2.4G) (**the default settings Network Mode = 11b/g/n mixed mode**). For example, you choose 11b/g/n mixed mode.
20. Please enter the Network Name(SSID) and if you want to change (**the default settings Radio On/Off = On, Network Name(SSID) = RTDEV_AP**).
21. Please click **Apply** button to continue.

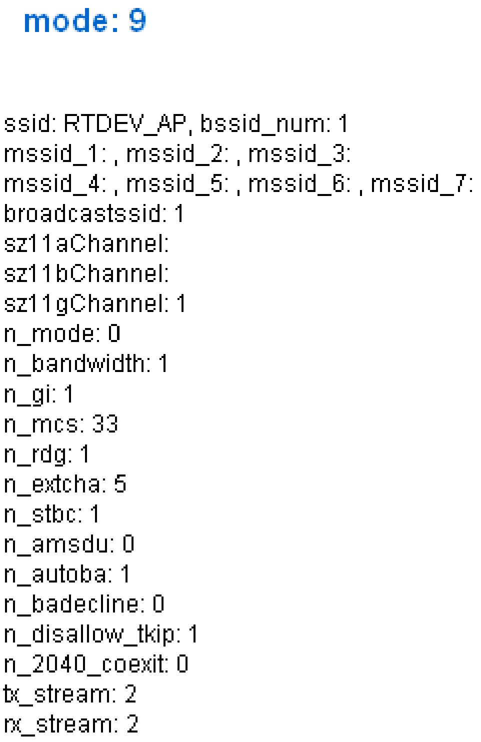


Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
Driver Version	2.5.0.11
Radio On/Off	RADIO OFF
Network Mode	11b/g/n mixed mode
Network Name(SSID)	RTDEV_AP
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Broadcast Network Name (SSID)	● Enable ○ Disable
BSSID	00:13:33:66:11:28
Frequency (Channel)	2412MHz (Channel 1)
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Auto
MCS	Auto
Reverse Direction Grant(RDG)	○ Disable ● Enable
Extension Channel	2432MHz (Channel 5)
Space Time Block Coding(STBC)	○ Disable ● Enable
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
HT Disallow TKIP	○ Disable ● Enable
Other	
HT TxStream	2
HT RxStream	2

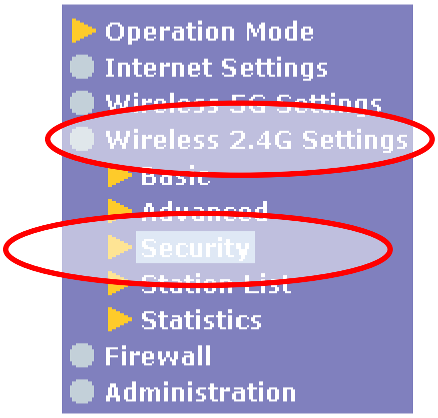
22. The confirmation is shown as screen below:



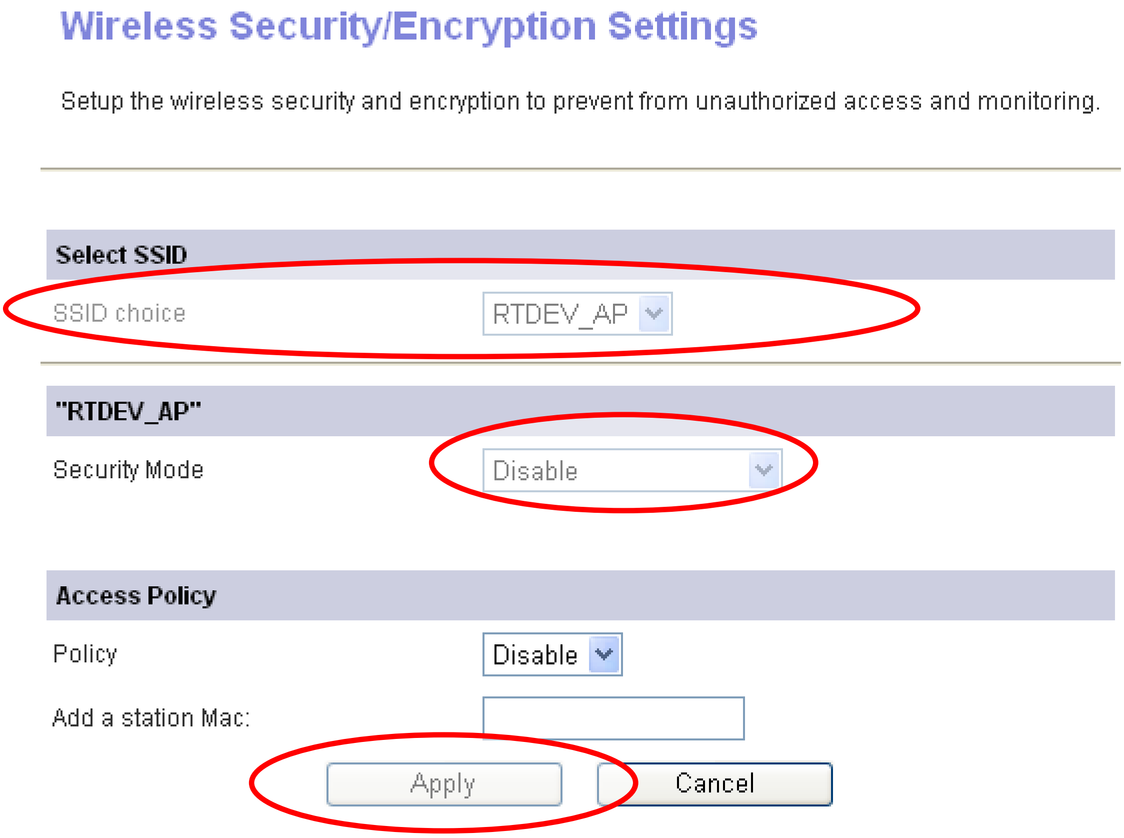
```
mode: 9


ssid: RTDEV_AP, bssid_num: 1
mssid_1: , mssid_2: , mssid_3:
mssid_4: , mssid_5: , mssid_6: , mssid_7:
broadcastssid: 1
sz11aChannel:
sz11bChannel:
sz11gChannel: 1
n_mode: 0
n_bandwidth: 1
n_gi: 1
n_mcs: 33
n_rdg: 1
n_extcha: 5
n_stbc: 1
n_amsdu: 0
n_autoba: 1
n_badecline: 0
n_disallow_tkip: 1
n_2040_coexit: 0
tx_stream: 2
rx_stream: 2
```

**** Actual ANTENNA may vary depending on setting***

23. From the **Wireless 2.4G Settings** menu, click on **Security**.



24. Choose the Security Mode if necessary, as Disable / OPENWEP / SHAREDWEP / WEPAUTO / WPA-PSK / WPA2-PSK and WPAPSKWPA2PSK **(the default settings Security Mode = Disable)**. For example, you choose the Disable Mode.
25. Please click **Apply** button to continue.



Wireless Security/Encryption Settings

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

Select SSID

SSID choice: RTDEV_AP

"RTDEV_AP"

Security Mode: Disable

Access Policy

Policy: Disable

Add a station Mac:

26. The confirmation is shown as screen below:

MBSSID index: 0, Security Mode: Disable Done

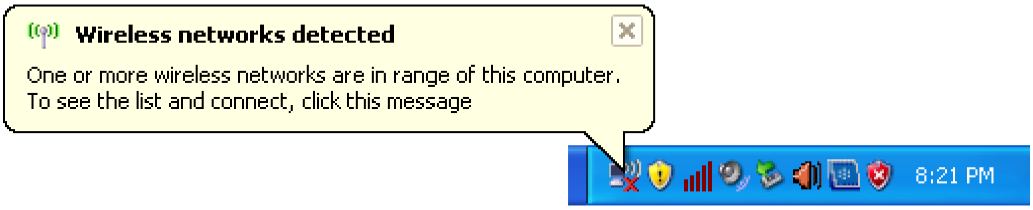
**** Actual ANTENNA may vary depending on setting***

27. WLAN Router has been configured completely, and suitable for Wireless and Internet Connections.

Wireless Connection

For easy installation it is saved to keep the settings. You can later change the wireless settings via the wireless configuration menu. (see user manual on the CD – Chapter 14 for 5G or 16 for 2.4G).

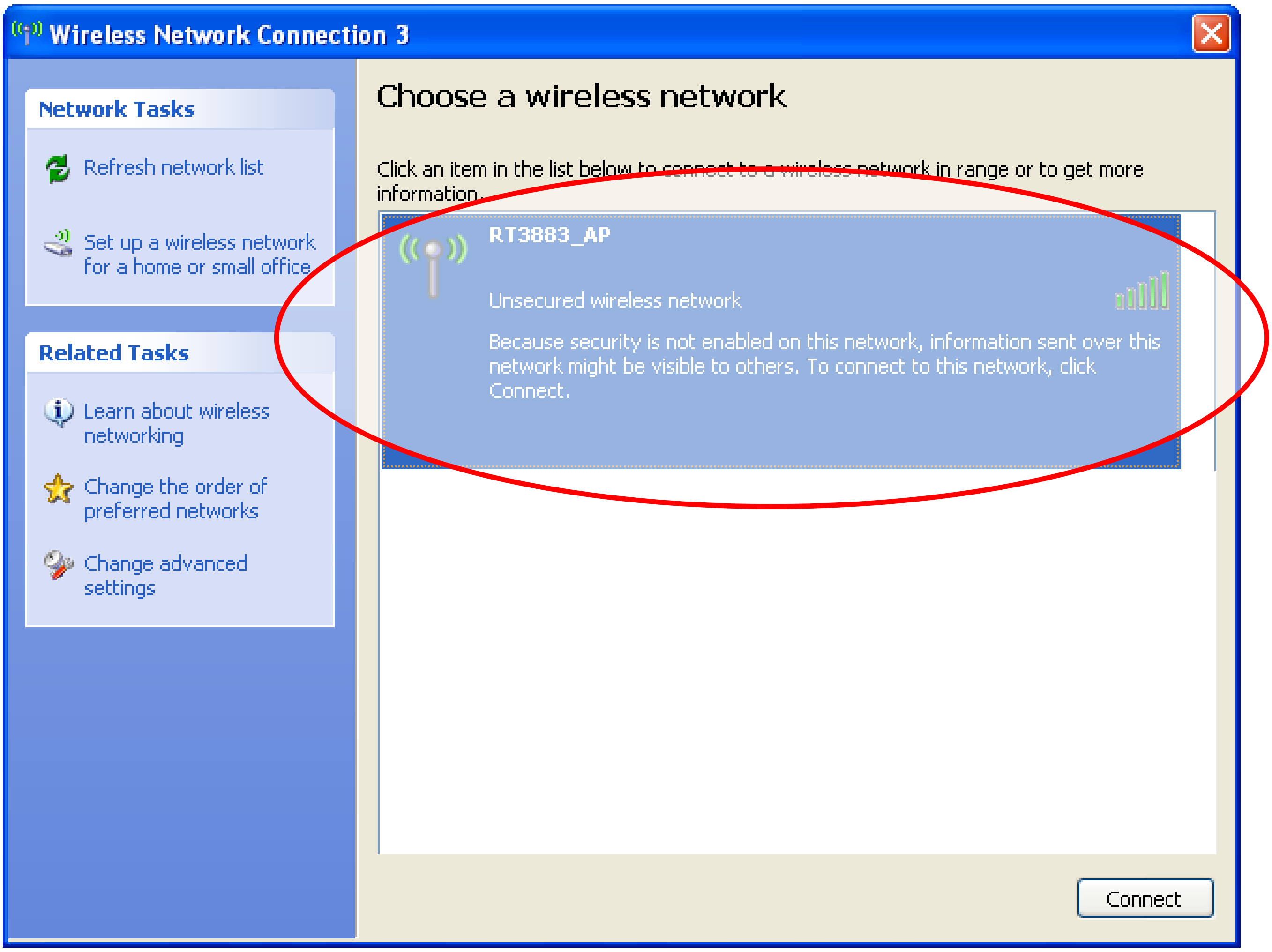
28. Double click on the wireless icon on your computer and search for the wireless network that you enter **Network Name(SSID)** name.



Wireless networks detected

One or more wireless networks are in range of this computer.
To see the list and connect, click this message

29. Click on the wireless network that you enter **SSID** name to connect. **(the default settings Radio On/Off = On, Network Name(SSID) = RT3883_AP for 5G or RTDEV_AP for 2.4G)**



Wireless Network Connection 3

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

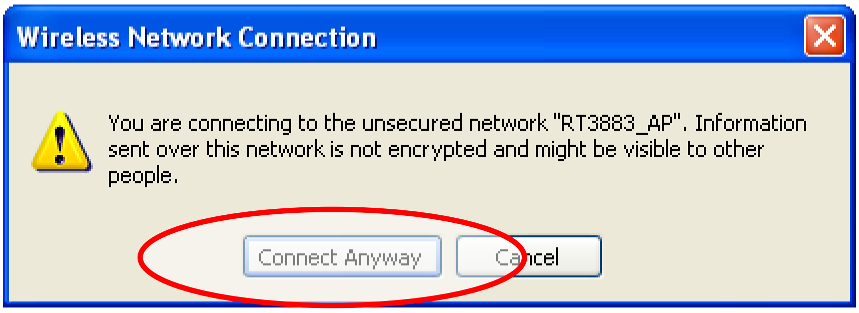
RT3883_AP

Unsecured wireless network

Because security is not enabled on this network, information sent over this network might be visible to others. To connect to this network, click Connect.

Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

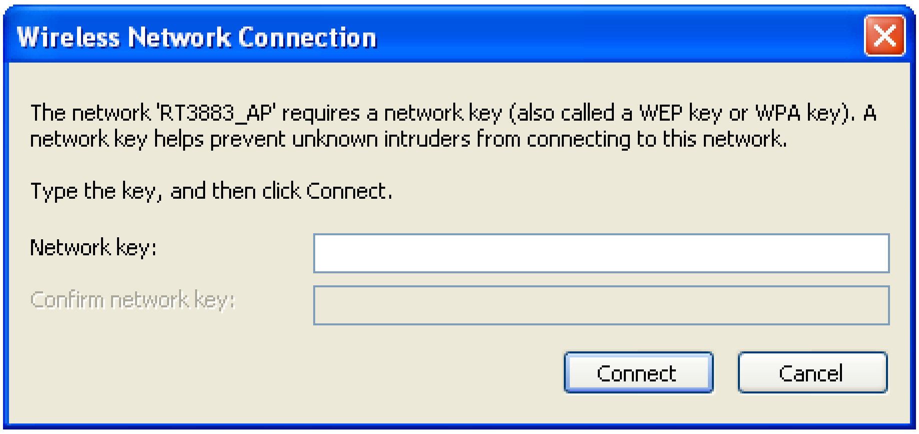
30. If the wireless network isn't encrypted, click on "**Connect Anyway**" to connect.



Wireless Network Connection

You are connecting to the unsecured network "RT3883_AP". Information sent over this network is not encrypted and might be visible to other people.

31. If the wireless network is encrypted, enter the network key that belongs to your authentication type and key **(the default settings Security Mode = Disable)**. You can later change this network key via the wireless configuration menu. (see user manual on the CD – Chapter 14 for 5G or 16 for 2.4G).



Wireless Network Connection

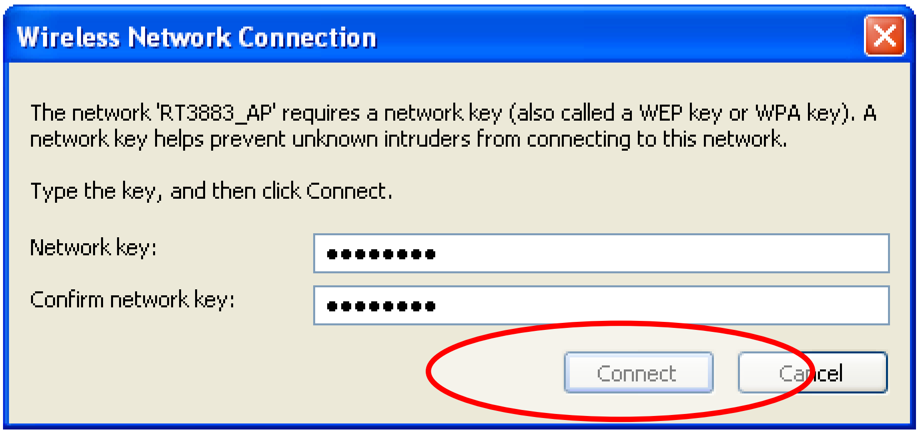
The network 'RT3883_AP' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key:

Confirm network key:

32. Click on "Connect" or "Apply".



Wireless Network Connection

The network 'RT3883_AP' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key: ●●●●●●●●●

Confirm network key: ●●●●●●●●●

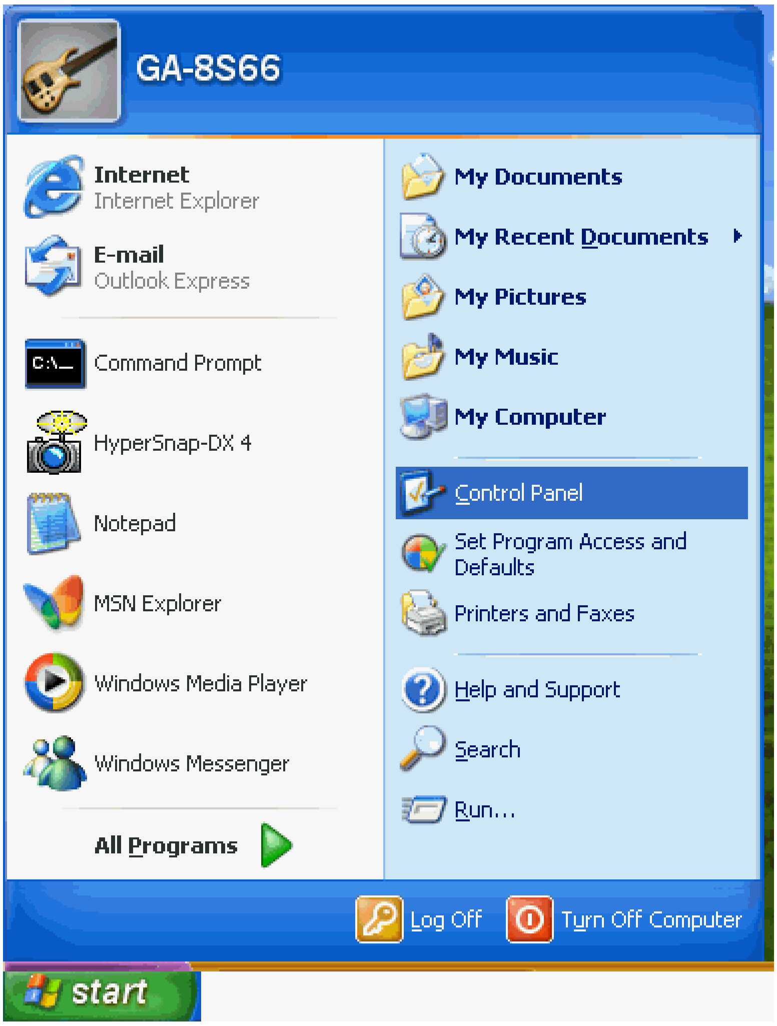
33. Now you are ready to use the Wireless Network to Internet or intranet.

5 What the Internet/WAN access of your own Network now is

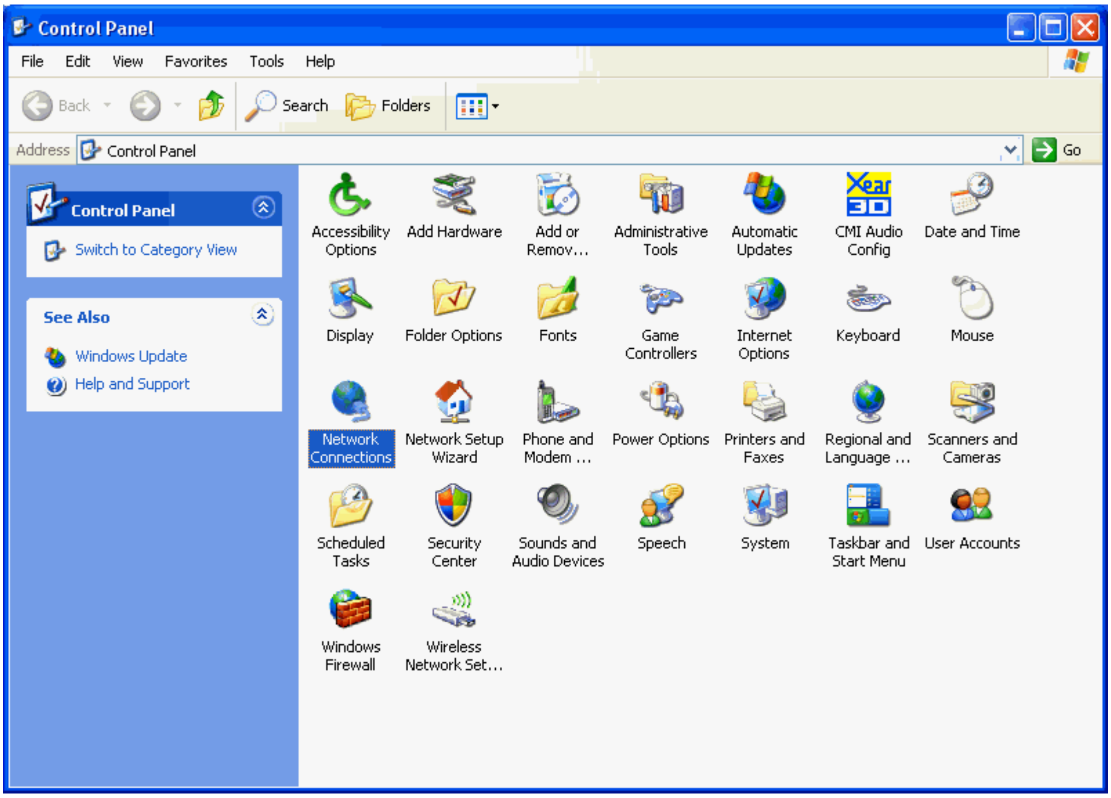
Now you could check what the Internet/WAN access of your network is to know how to configure the WAN port of 802.11n WLAN Gigabit Router.

Please follow steps below to check what the Internet/WAN access if your own Network is DHCP Client, Static IP or PPPoE Client.

1. Click Start -> Control Panel



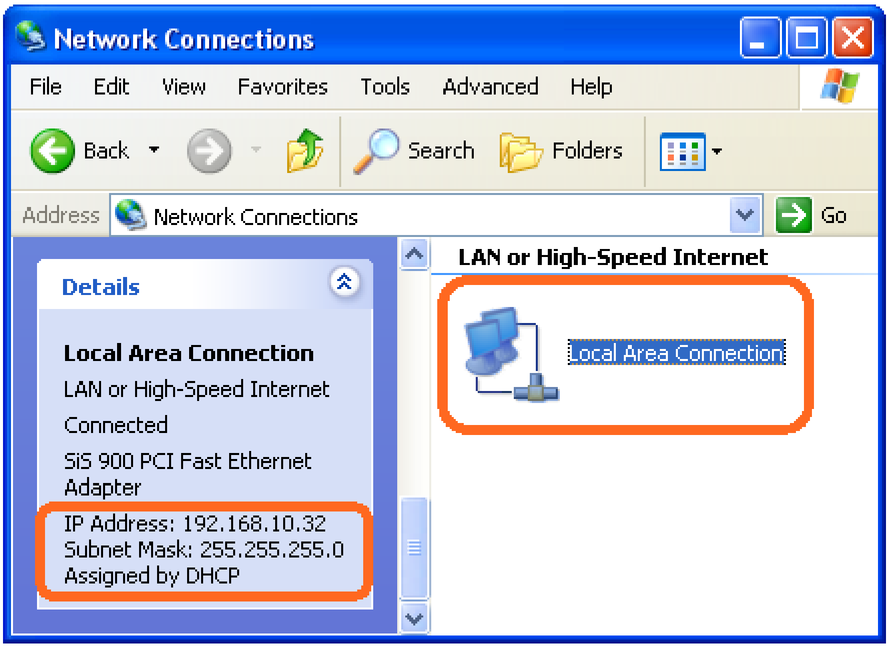
2. Double click ***Network Connections***



Internet/WAN access is the DHCP client

If you cannot see any **Broadband Adapter** in the **Network Connections**, your Internet/WAN access is **DHCP Client** or **Static IP**.

1. Click Local Area Connection in LAN or High-Speed Internet and you could see string Assigned by DHCP in Details.

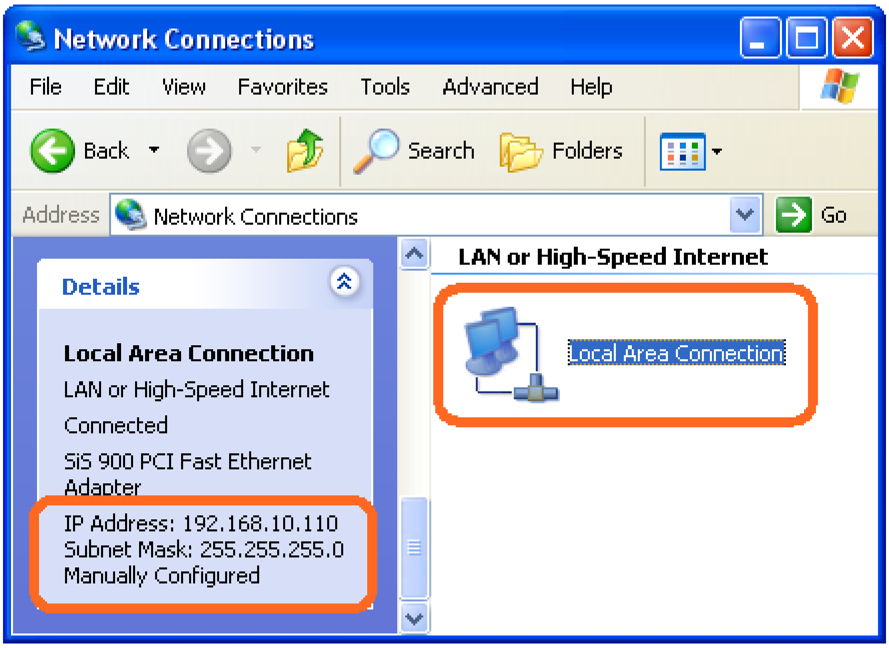


Local Area Connection
LAN or High-Speed Internet
Connected
SiS 900 PCI Fast Ethernet Adapter
IP Address: 192.168.10.32
Subnet Mask: 255.255.255.0
Assigned by DHCP

Internet/WAN access is the Static IP

If you cannot see any **Broadband Adapter** in the **Network Connections**, your Internet/WAN access is **DHCP Client** or **Static IP**.

1. Click Local Area Connection in LAN or High-Speed Internet and you could see string Manually Configured in Details.



Local Area Connection
LAN or High-Speed Internet
Connected
SiS 900 PCI Fast Ethernet Adapter
IP Address: 192.168.10.110
Subnet Mask: 255.255.255.0
Manually Configured

2. Right click **Local Area Connection** and click **Properties** and then you could get the IP settings in detail and write down the IP settings as follow:

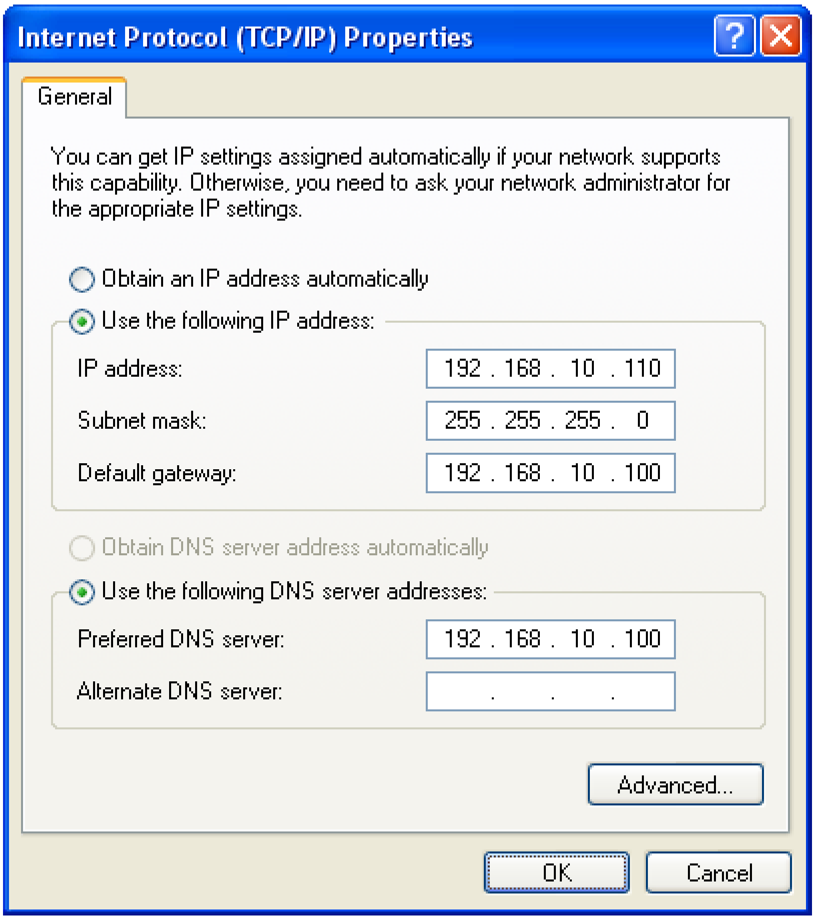
IP Address: 10.10.100.110

Subnet mask: 255.255.255.0

Default gateway: 10.10.100.100

Preferred DNS server: 10.10.100.100

Alternate DNS Server: If you have it, please also write it down.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 10 . 110

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 10 . 100

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 10 . 100

Alternate DNS server: . . .

Internet/WAN access is the PPPoE client

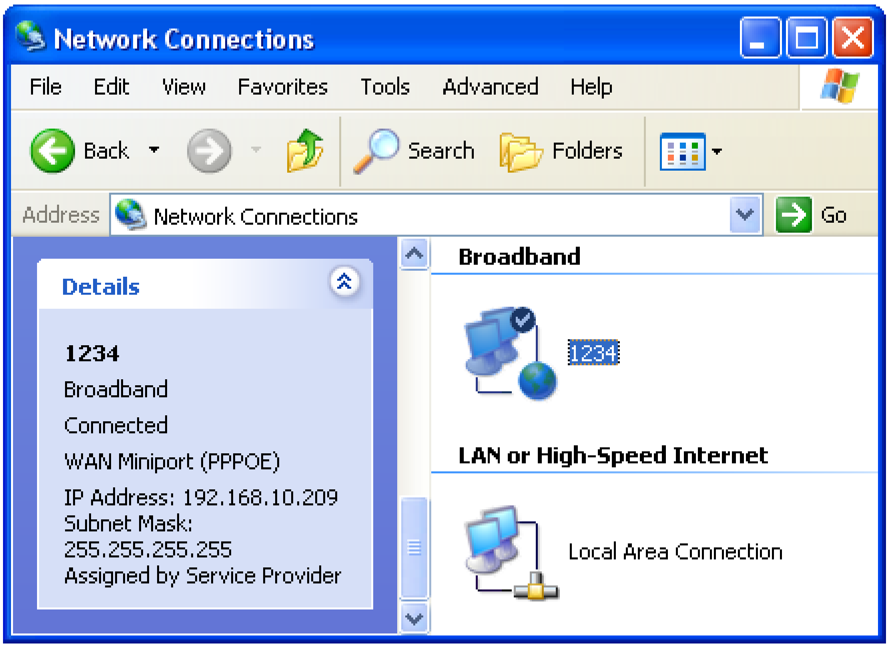
If you can see any **Broadband Adapter** in the **Network Connections**, your Internet/WAN access is **PPPoE Client**.

1. Click Broadband Adapter in Broadband and you could see string Assigned by Service Provider in Details.

For PPPoE configuration on 802.11n WLAN Gigabit Router, you'll need following information that you could get from your Telecom, or by your Internet Service Provider.

Username of PPPoE: 1234 for example

Password of PPPoE: 1234 for example



Details

1234
Broadband
Connected
WAN Miniport (PPPOE)
IP Address: 192.168.10.209
Subnet Mask:
255.255.255.255
Assigned by Service Provider

6 Getting Started with the Web pages

The 802.11n WLAN Gigabit Router includes a series of Web pages that provide an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You can access it through your web browser from any PC connected to the device via the LAN ports.

Accessing the Web pages

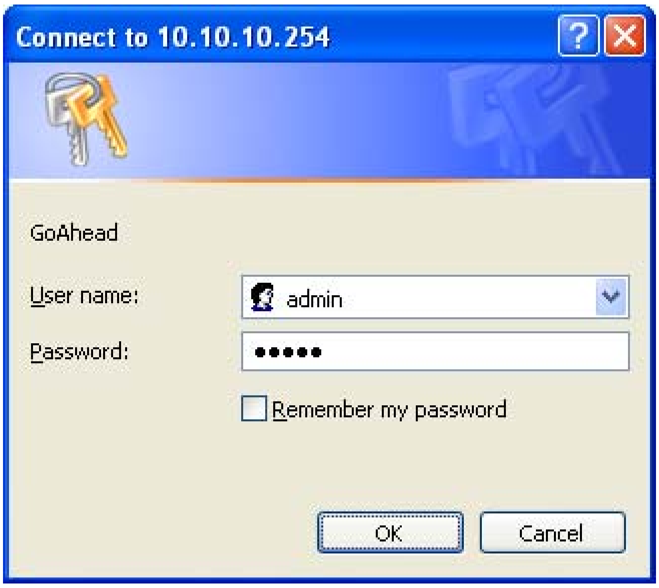
To access the Web pages, you need the following:

- A PC or laptop connected to the LAN port on the device.
- A web browser installed on the PC. The minimum browser version requirement is Internet Explorer v4 or Netscape v4. For the best display quality, use latest version of Internet Explorer, Netscape or Mozilla Firefox.From any of the LAN computers, launch your web browser, type the following URL in the web address (or location) box, and press [Enter] on your keyboard:

  http://10.10.10.254

  The first time that you click on an entry from the left-hand menu, a login box is displayed. You must enter your username and password to access the pages.

  A login screen is displayed:



GoAhead

User name: admin

Password: ●●●●●

□ Remember my password

Figure 5: Login screen

2. Enter your user name and password. The first time you log into the program, use these defaults:

User Name:	**admin**
Password:	**admin**

Note

You can change the password at any time or you can configure your device so that you do not need to enter a password. See Password.

3. Click on OK.

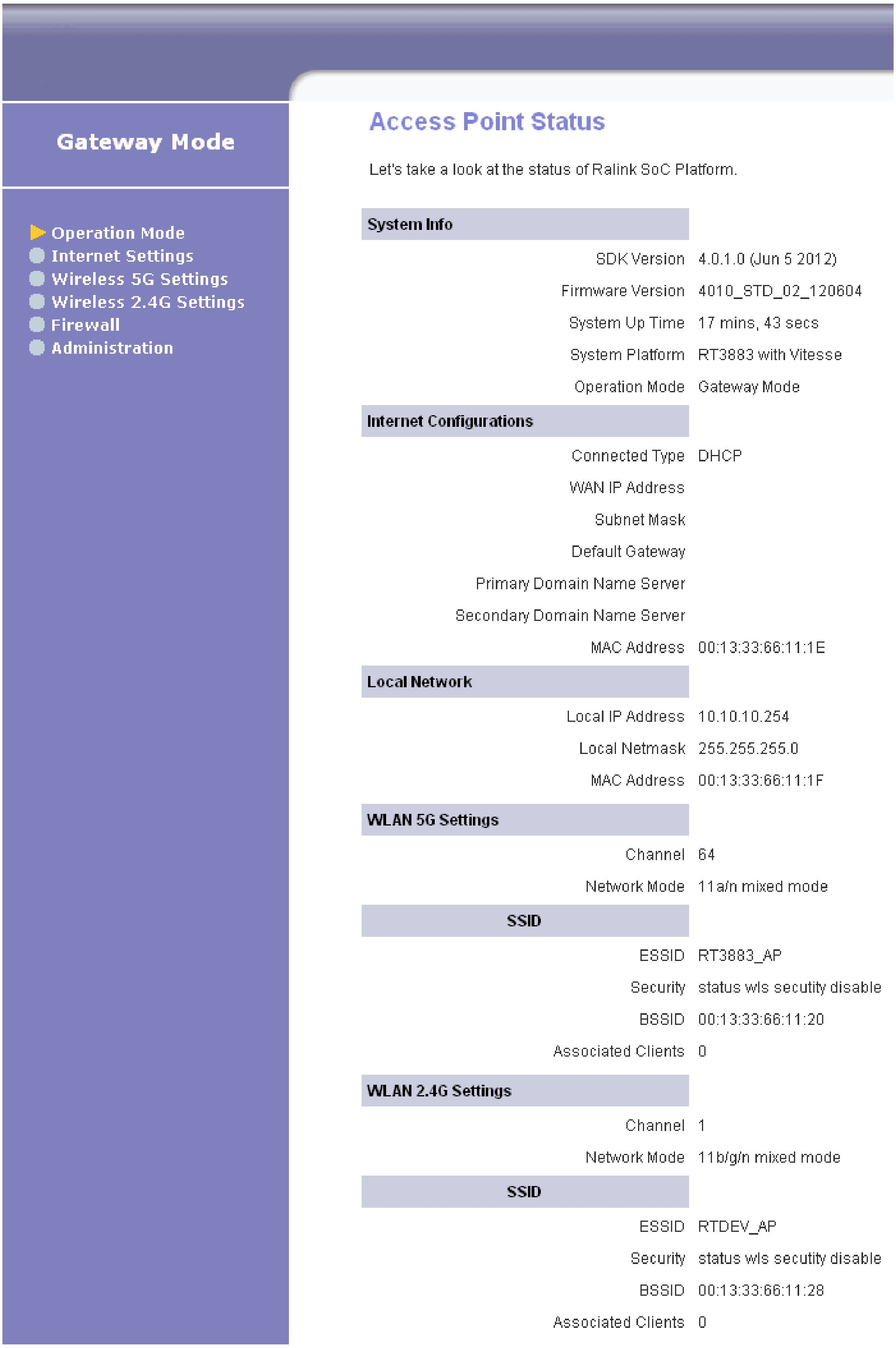
This is the first page displayed each time you log in to the Web pages.

Note

If you receive an error message or the Welcome page is not displayed, see Troubleshooting Suggestions.

4. You are now ready to configure your device.

The homepage for the web pages is displayed:



Access Point Status

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

System Info	
SDK Version	4.0.1.0 (Jun 5 2012)
Firmware Version	4010_STD_02_120604
System Up Time	17 mins, 43 secs
System Platform	RT3883 with Vitesse
Operation Mode	Gateway Mode
Internet Configurations	
Connected Type	DHCP
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	
Secondary Domain Name Server	
MAC Address	00:13:33:66:11:1E
Local Network	
Local IP Address	10.10.10.254
Local Netmask	255.255.255.0
MAC Address	00:13:33:66:11:1F
WLAN 5G Settings	
Channel	64
Network Mode	11a/n mixed mode
SSID	
ESSID	RT3883_AP
Security	status wls secutity disable
BSSID	00:13:33:66:11:20
Associated Clients	0
WLAN 2.4G Settings	
Channel	1
Network Mode	11b/g/n mixed mode
SSID	
ESSID	RTDEV_AP
Security	status wls secutity disable
BSSID	00:13:33:66:11:28
Associated Clients	0

Figure 6: Homepage

Testing your Setup

Once you have connected your hardware and configured your PCs, any computer on your LAN should be able to use the DSL /Cable connection to access the Internet.

To test the connection, turn on the device, wait for 30 seconds and then verify that the LEDs are illuminated as follows:

Table 1. LED Indicators

Label	Color	Function
POWER	green	On: device is powered on Off: device is powered off
WLAN	green	On: WLAN link established and active Blink: Valid Wireless packet being transferred
WPS	green	Off: WPS link isn't established and active Blink: Valid WPS packet being transferred
WAN	green	On: WAN link established and active Off: No LAN link Blink: Valid Ethernet packet being transferred
LAN 1/2/3/4	green	On: LAN link established and active Off: No LAN link Blink: Valid Ethernet packet being transferred

If the LEDs illuminate as expected, test your Internet connection from a LAN computer. To do this, open your web browser, and type the URL of any external website (such as http://www.yahoo.com). The LED labeled *WAN* should blink rapidly and then appear solid as the device connects to the site.

If the LEDs do not illuminate as expected, you may need to configure your Internet access settings using the information provided by your ISP. For details, see *Internet Access*. If the LEDs still do not illuminate as expected or the web page is not displayed, see *Troubleshooting Suggestions* or contact your ISP for assistance.

Default device settings

In addition to handling the xDSL / Cable modem connection to your ISP, the 802.11n WLAN Gigabit Router can provide a variety of services to your network. The device is preconfigured with default settings for use with a typical home or small office network.

The table below lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration, review these settings to verify that they meet the needs of your network. Follow the instructions to change them if necessary. If you are unfamiliar with these settings, try using the device without modification, or contact your ISP for assistance.

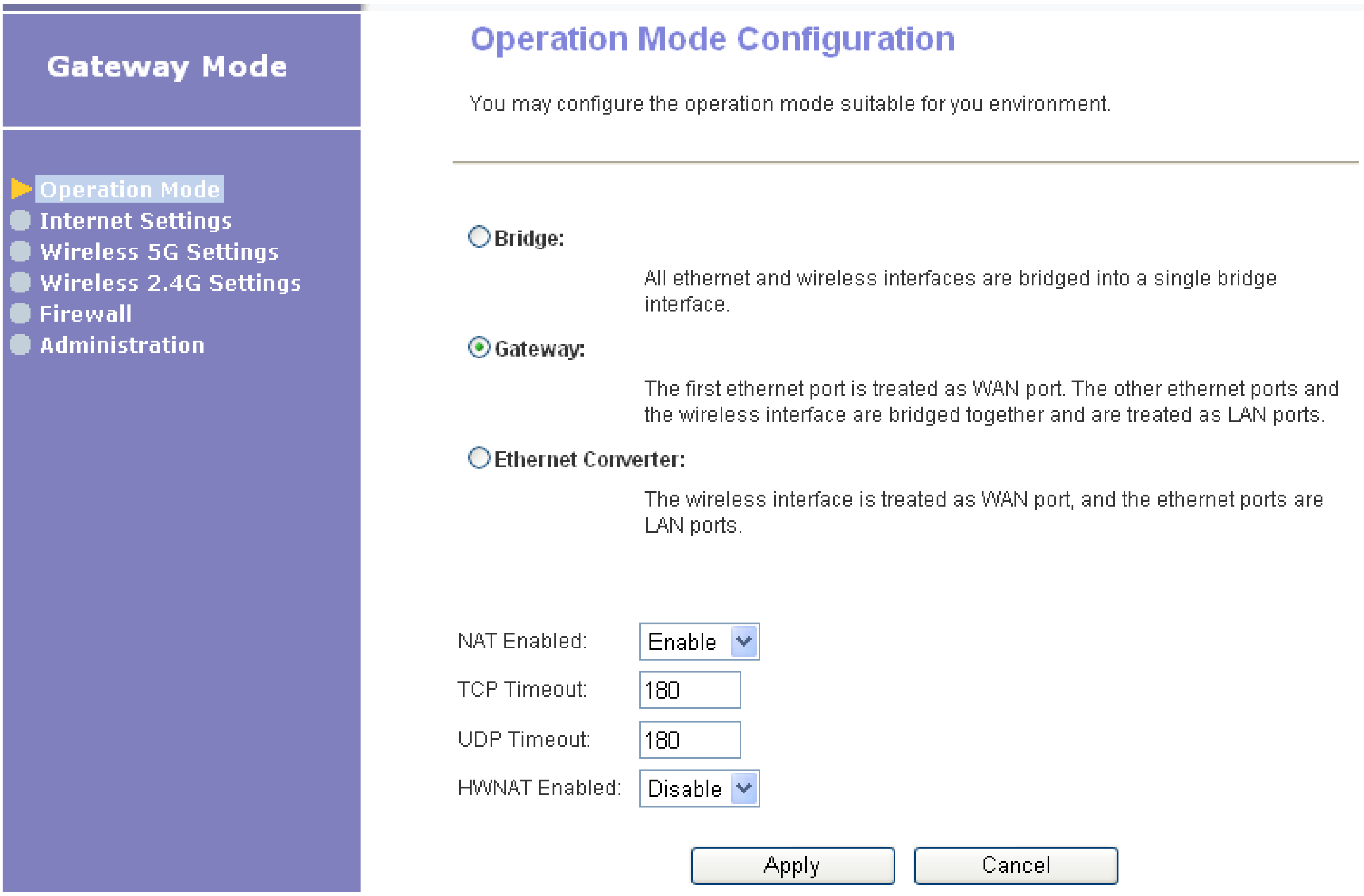
WARNING

We strongly recommend that you contact your ISP prior to changing the default configuration.

Option	Default Setting	Explanation/Instructions
WAN Port IP Address	DHCP Client	This is the temporary public IP address of the WAN port on the device. It is an unnumbered interface that is replaced as soon as your ISP assigns a 'real' IP address. See *Network Settings -> WAN Interface*.
LAN Port IP Address	Assigned static IP address: 10.10.10.254 Subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See *Network Settings -> LAN Interface*.
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 10.10.10.100 through 10.10.10.200	The 802.11n WLAN Gigabit Router maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in *Configuring Ethernet PCs*.

7 Operation Mode

There are 4 operation modes can choose, Bridge, Gateway, Ethernet Converter and AP Client.



Operation Mode Configuration

You may configure the operation mode suitable for you environment.

○ Bridge:

All ethernet and wireless interfaces are bridged into a single bridge interface.

● Gateway:

The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

○ Ethernet Converter:

The wireless interface is treated as WAN port, and the ethernet ports are LAN ports.

NAT Enabled: Enable

TCP Timeout: 180

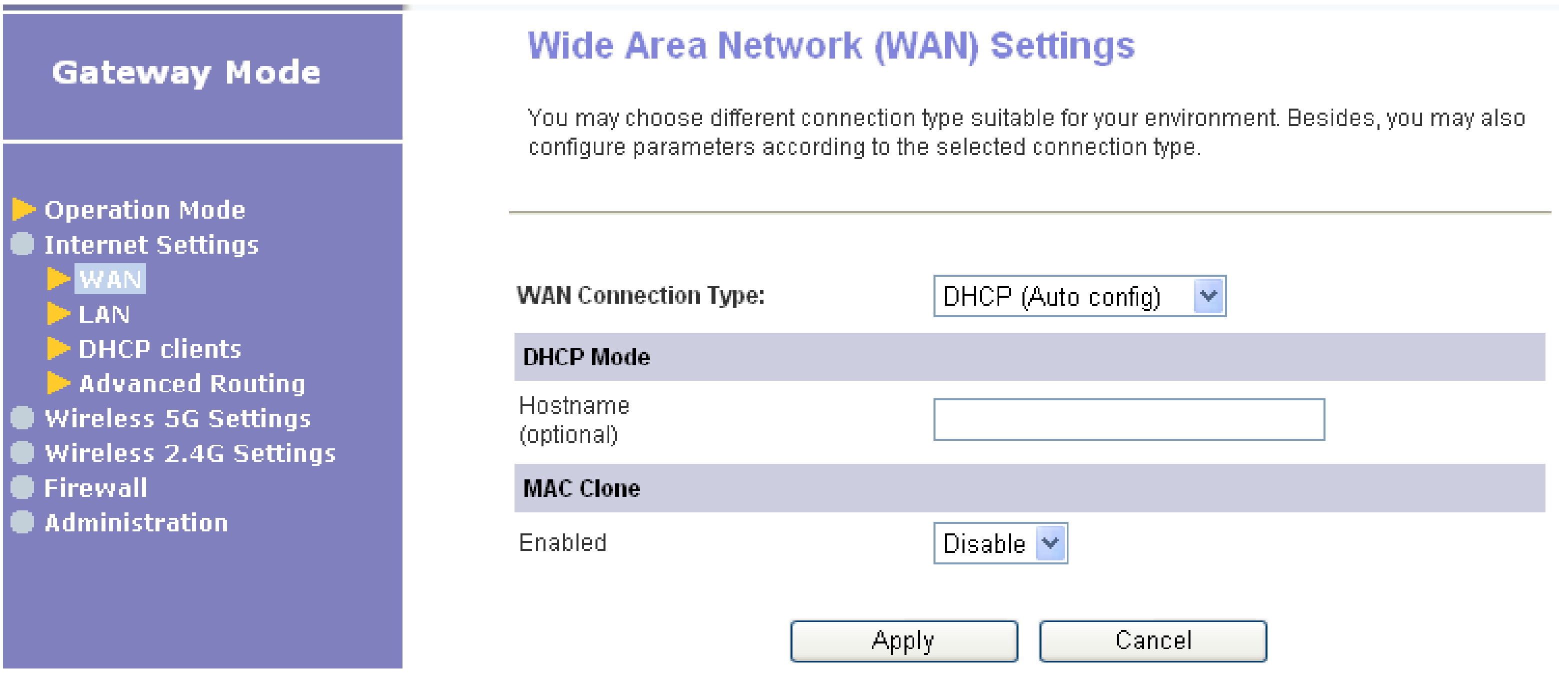
UDP Timeout: 180

HWNAT Enabled: Disable

Field	Description
Bridge	**All Ethernet ports and wireless interfaces are bridged into a single bridge interface. The router will work as bridge only.**
Gateway	**The device work as wireless router. The NAT will can set as enable or disable, WAN port need to link to the Internet.**
Ethernet Converter	**The wireless interface is treated as WAN port, and the Ethernet ports are LAN ports.**

8 Wide Area Network (WAN) Settings

There are 3 selections for WAN connection type which are STATIC (fixed IP), DHCP (Auto config) and PPPoE (ADSL).



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: DHCP (Auto config)

DHCP Mode

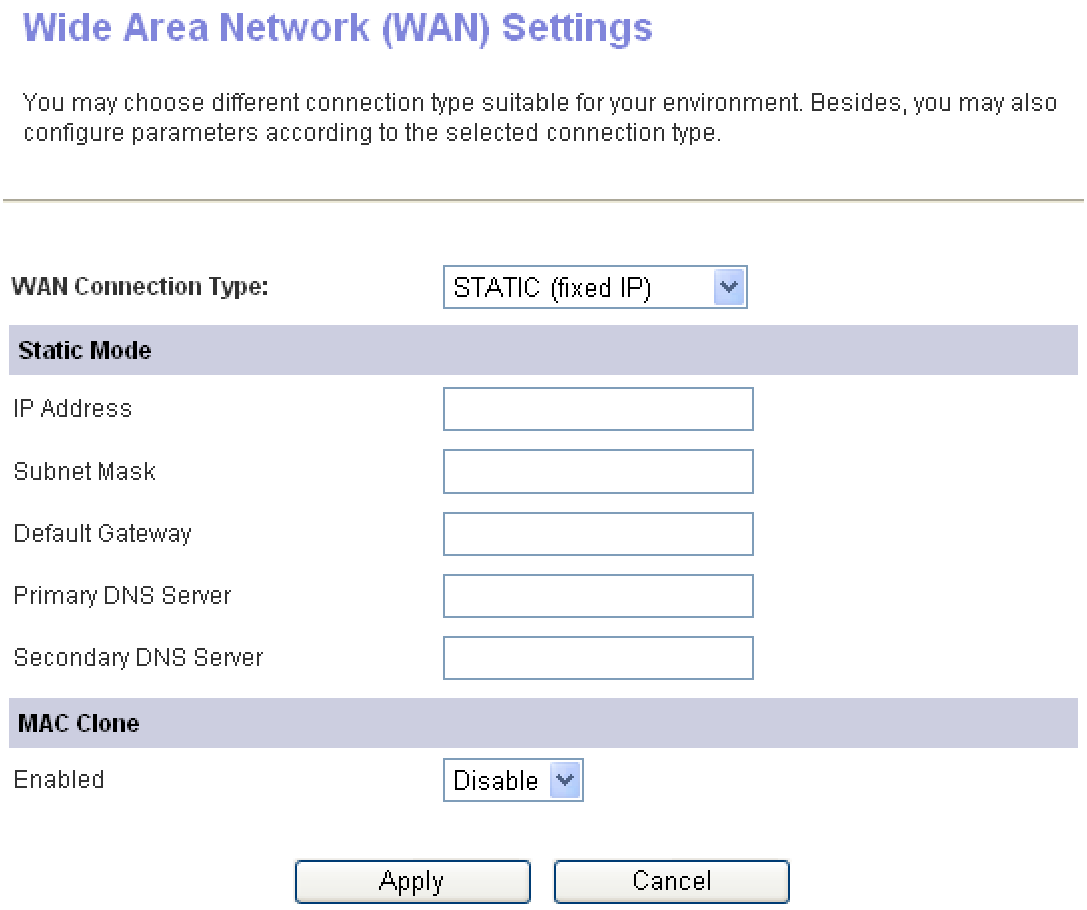
Hostname (optional):

MAC Clone

Enabled: Disable

STATIC(Fixed IP)

If you need to assign static IP addresses to the devices in your network, please remember that the IP address for each computer or device must be in the same IP address range as all the devices in the network. Each device must also have the same subnet mask. For example: Assign the first computer an IP address of 192.168.0.2 and a subnet mask of 255.255.255.0, the second device an IP address of 192.168.0.3 and a subnet mask of 255.255.255.0, and so on.



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: STATIC (fixed IP)

Static Mode

IP Address

Subnet Mask

Default Gateway

Primary DNS Server

Secondary DNS Server

MAC Clone

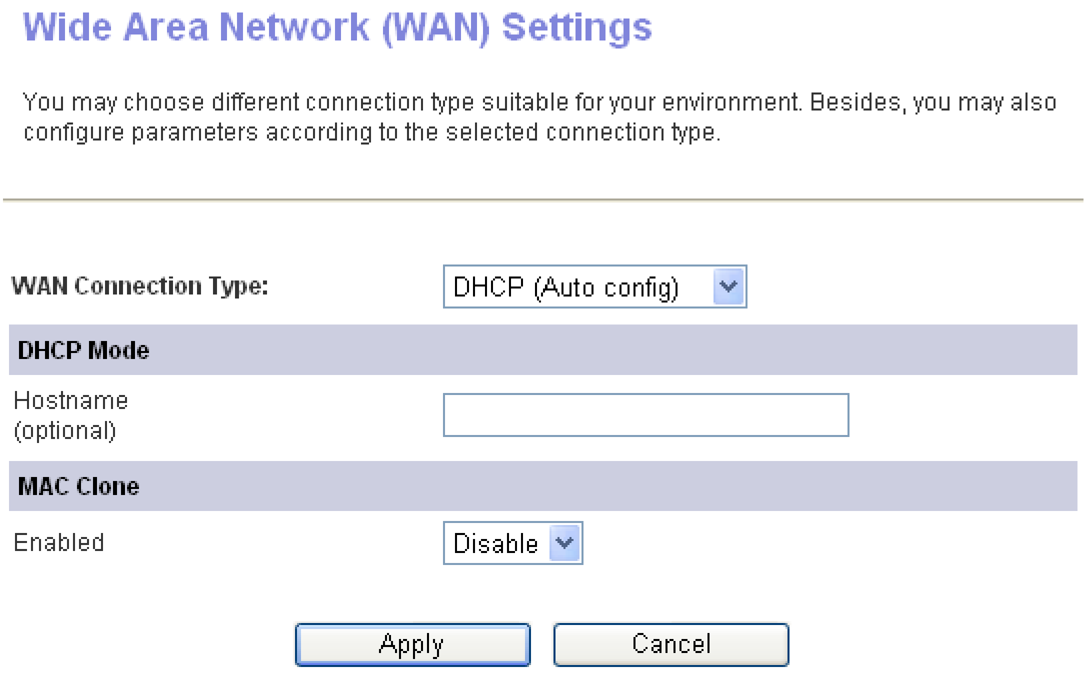
Enabled: Disable

Field	Description
IP Address	**Enter the IP address assigned by your service provider.**
Subnet Mask	**Enter the subnet mask assigned by your service provider.**
Default Gateway	**Enter the IP address assigned by your service provider.**
Primary DNS Server and Secondary DNS Server	**Enter Primary DNS Server and/or Secondary DNS Server assigned by your service provider.**
MAC Clone Enabled	**Enable MAC Clone**
MAC Clone MAC Address	**Enter the MAC address of your computer if your service provider only permits a computer with a certain MAC address to access the Internet. If you're using the computer to connect to the Internet via cable**

	modem, you can simply click "Fill my MAC" to fill the "MAC Address" field with the MAC address of your computer.

DHCP(Auto config)

It's will auto get the IP address from the DHCP Server. Assign the length of time for the IP lease, default setting is 86400 seconds. The Hostname is the name of the device.



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: DHCP (Auto config)

DHCP Mode

Hostname (optional):

MAC Clone

Enabled: Disable

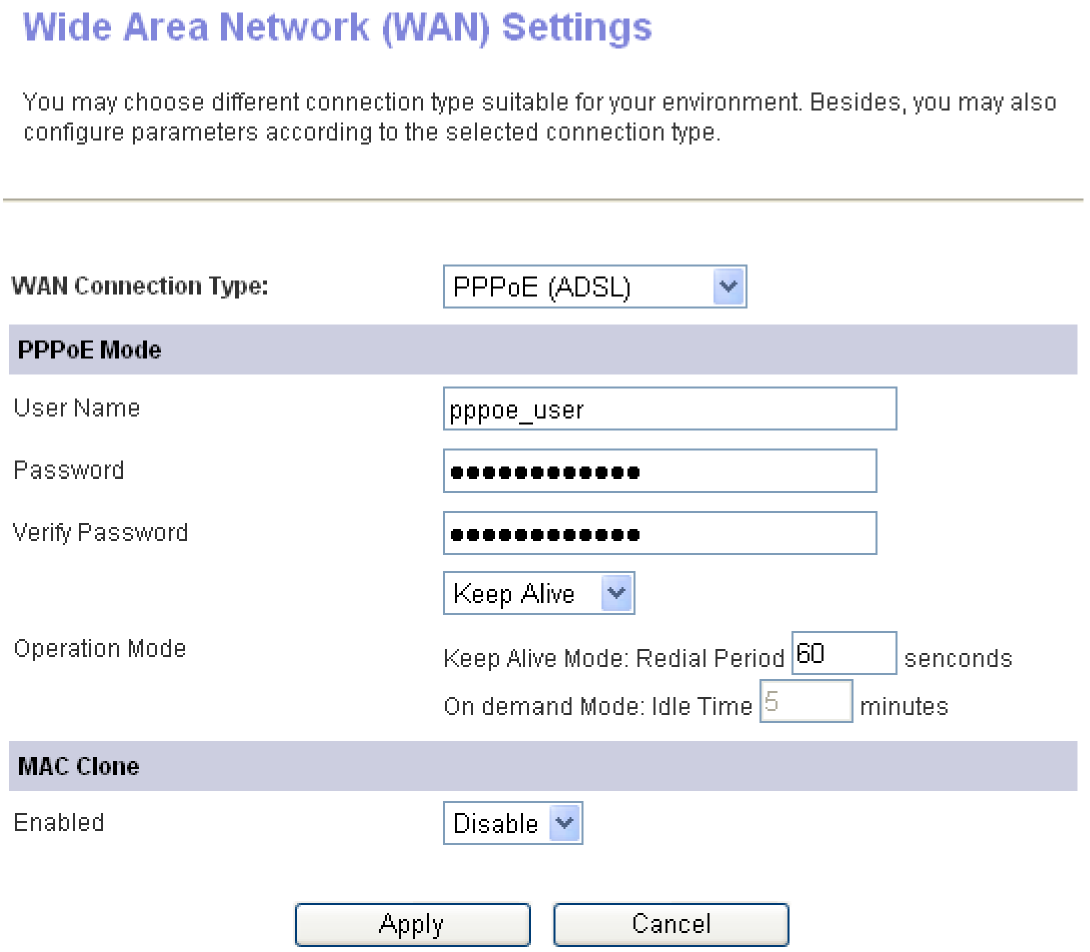
Field	Description
Host Name	**Enter the host name of your computer. (This is optional and is only required if your service provider asks you to do so.)**
MAC Clone Enabled	**Enable MAC Clone**
MAC Clone MAC Address	**Enter the MAC address of your computer if your service provider only permits a computer with a certain MAC address to access the Internet. If you're using the computer to connect to the Internet via cable modem, you can simply click "Fill my MAC" to fill the "MAC Address" field with the MAC address of your computer.**

PPPoE(ADSL)

Username and Password: Fill in the User Name and Password that provided by your ISP.

Verify Password: Retype the password to confirm.

Operation Mode: Set the router as Keep Alive or On demand.



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: PPPoE (ADSL)

PPPoE Mode

User Name: pppoe_user

Password: ●●●●●●●●●●●●●

Verify Password: ●●●●●●●●●●●●●

Operation Mode: Keep Alive

Keep Alive Mode: Redial Period 60 senconds

On demand Mode: Idle Time 5 minutes

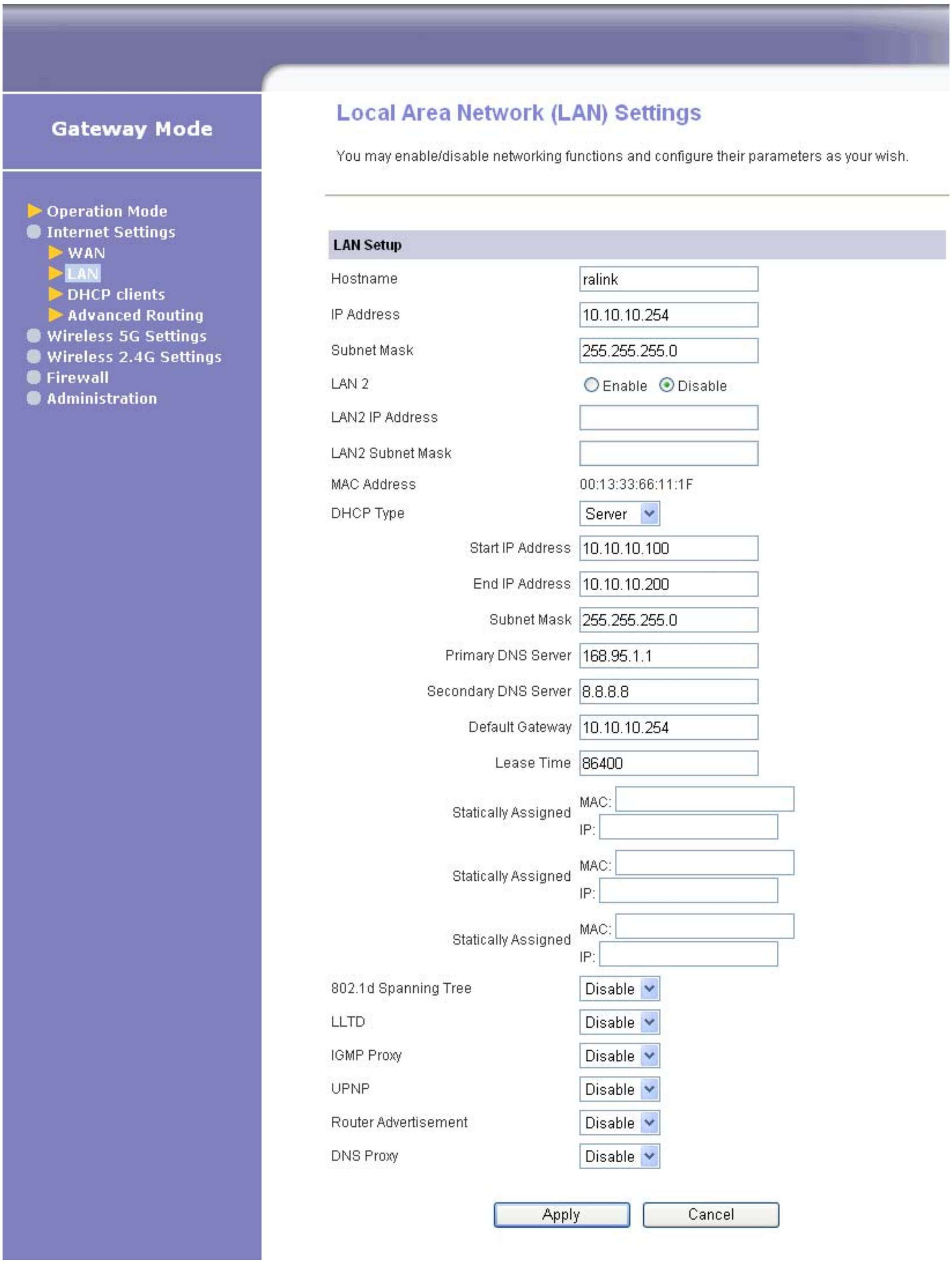
MAC Clone

Enabled: Disable

Field	Description
User Name	**Enter the user name assigned by your Internet service provider**
Password	**Enter the password assigned by your Internet service provider**
Verify Password	**Retype the password to confirm**
Operation Mode	**Set the router as Keep Alive or On demand or Manual**
MAC Clone Enabled	**Enable MAC Clone**
MAC Clone MAC Address	**Enter the MAC address of your computer if your service provider only permits a computer with a certain MAC address to access the Internet. If you're using the computer to connect to the Internet via cable modem, you can simply click "Fill my MAC" to fill the "MAC Address" field with the MAC address of your computer.**

9 Local Area Network (LAN) Settings

To set up the configuration of LAN interface, private IP of your router LAN port and subnet mask for your LAN segment.



Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

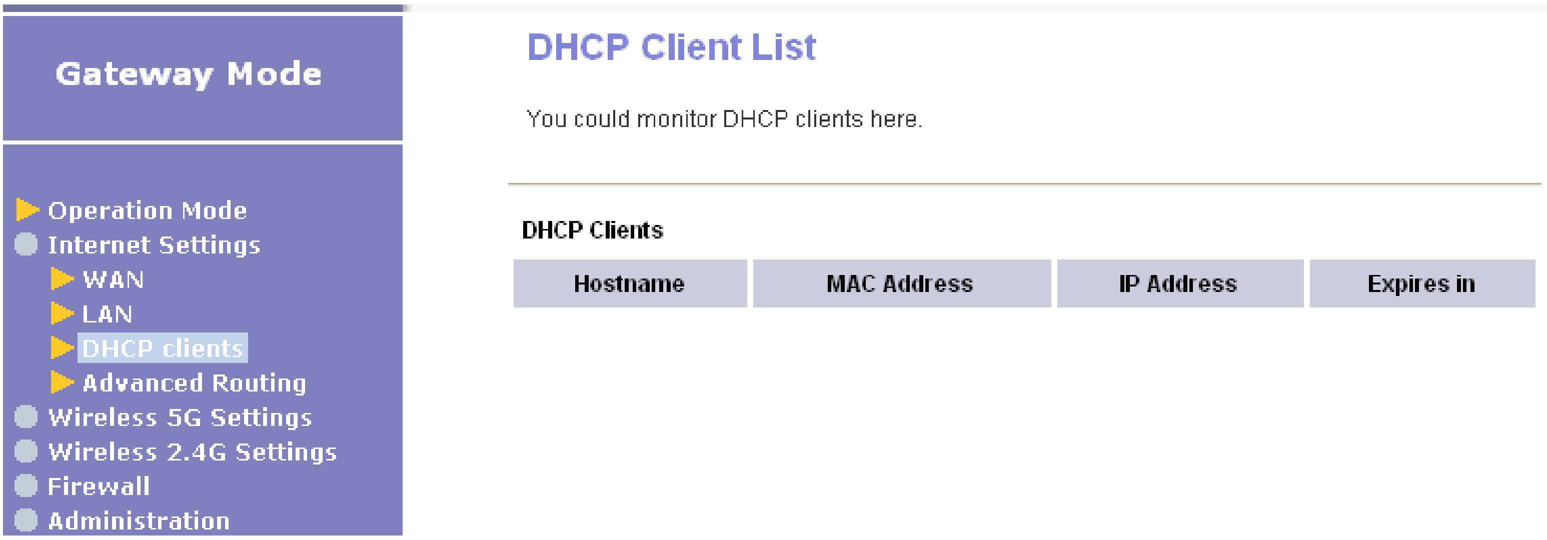
LAN Setup	
Hostname	ralink
IP Address	10.10.10.254
Subnet Mask	255.255.255.0
LAN 2	○ Enable ● Disable
LAN2 IP Address	
LAN2 Subnet Mask	
MAC Address	00:13:33:66:11:1F
DHCP Type	Server
Start IP Address	10.10.10.100
End IP Address	10.10.10.200
Subnet Mask	255.255.255.0
Primary DNS Server	168.95.1.1
Secondary DNS Server	8.8.8.8
Default Gateway	10.10.10.254
Lease Time	86400
Statically Assigned	MAC: IP:
Statically Assigned	MAC: IP:
Statically Assigned	MAC: IP:
802.1d Spanning Tree	Disable
LLTD	Disable
IGMP Proxy	Disable
UPNP	Disable
Router Advertisement	Disable
DNS Proxy	Disable

Field	Description
Host Name	**Enter the host name of your computer. (This is optional and is only required if your service provider asks you to do so.)**
IP Address	**The IP of your Router LAN port.**
Subnet Mask	**Subnet Mask of you LAN. All devices on the network must have the same subnet mask to communicate on the network.**
LAN2	**Enable / Disable LAN 2.**
LAN2 IP	**The IP address of LAN2.**
LAN2 Subnet Mask	**Subnet Mask of LAN2.**
DHCP Type	**To give your LAN Client an IP, you have to enable DHCP server. If not, manual setting up your client IP is necessary when you want to use the router as your client's default gateway.**
Start IP Address	**Specify the DHCP Client start IP address.**
End IP Address	**Specify the DHCP Client End IP address.** **The number of the "End IP" must be greater than "Start IP", and cannot be the same as the router's IP address.**
Subnet Mask	**Subnet Mask of you LAN (default 255.255.255.0). All devices on the network must have the same subnet mask to communicate on the network.**
Primary DNS Server	**Specify the Primary DNS Server IP Address.**
Secondary DNS Server	**Specify the Secondary DNS Server IP Address.**
Default Gateway	**Specify the Default Gateway IP Address.**
Lease Time	**Choose the length of the time for the device to recycle and give out the IP addresses to the devices in your network (default 86400).**
Statically Assigned	**Can statically assigned the client MAC and IP address. There are three IP can assign.**
802.1d Spanning Tree	**Enable/Disable 802.1d Spanning Tree.**
LLTD	**Enable/Disable LLTD.**
IGMP Proxy	**Enable/Disable. IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts.**
UPNP	**Enable/Disable. (Universal Plug-and-Play). Network architecture based on TCP/IP and intended to allow terminals to be networked without the need for configuration. In the Barricade router, for example, the correct ports are automatically opened for applications like Net meeting, online games, etc. You can choose to enable or disable the UPnP Service.**

Router Advertisement	**Enable/Disable Router Advertisement.**
DNS Proxy	**Enable/Disable DNS Proxy.**

10 DHCP Client

The information of IP, MAC, address and expire time of the DHCP clients that have connected with this device.



DHCP Client List

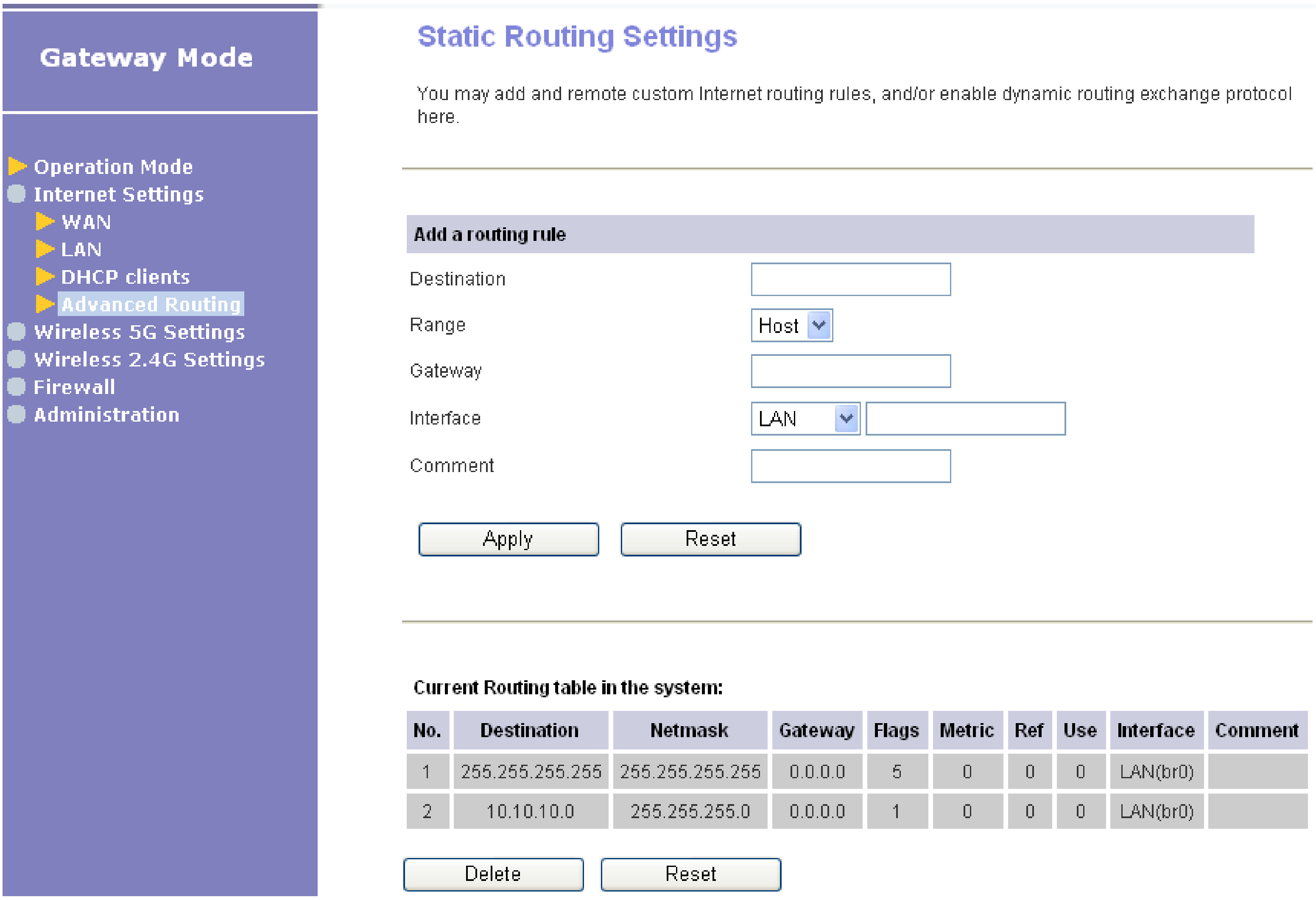
You could monitor DHCP clients here.

DHCP Clients

Hostname	MAC Address	IP Address	Expires in

11 Advanced Routing Settings

User can set a route rule(table) in here.



Static Routing Settings

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

Add a routing rule

Destination	
Range	Host
Gateway	
Interface	LAN
Comment	

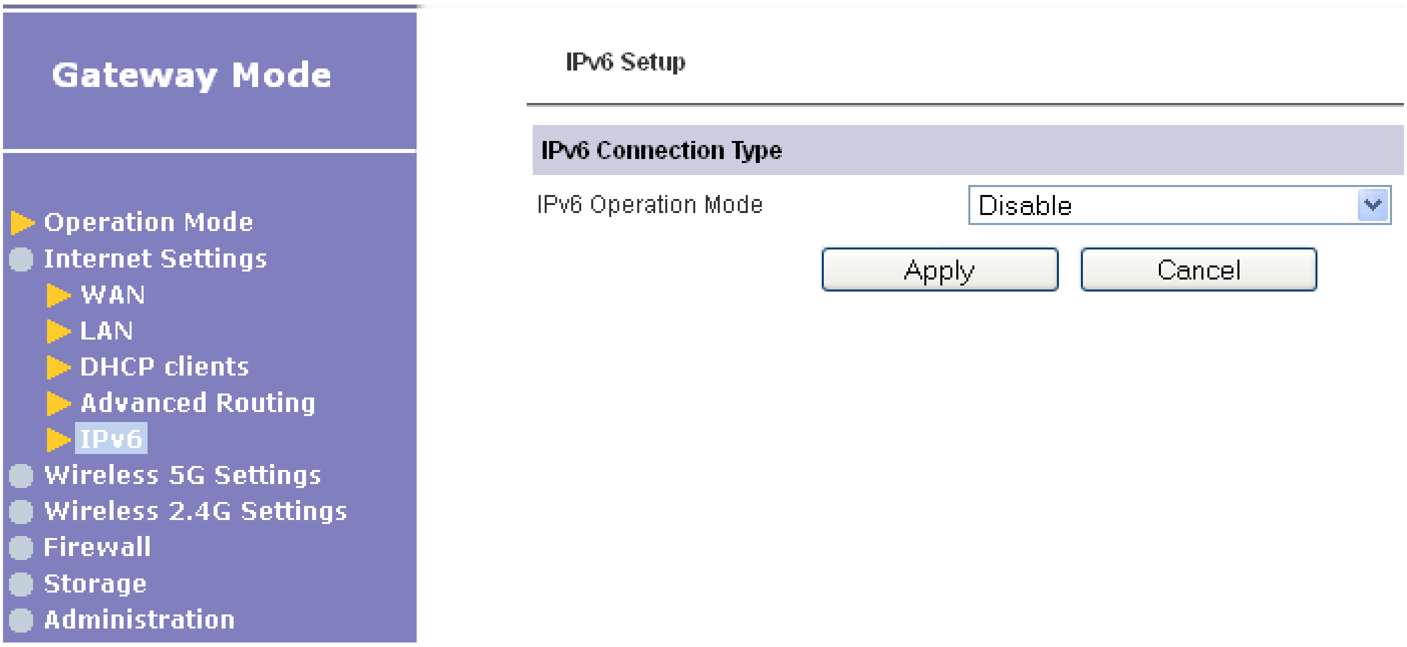
Current Routing table in the system:

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)	
2	10.10.10.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	

Field	Description
Destination	**The destination IP address.**
Range	**Host/Net, when select “Net”, there is another “Netmask” column need to fill out.**
Gateway	**The gateway for the routing.**
Interface	**Via LAN/WAN or User can define by custom.**
Comment	**Comment**

12 IPv6

User can configure IPv6 in here.



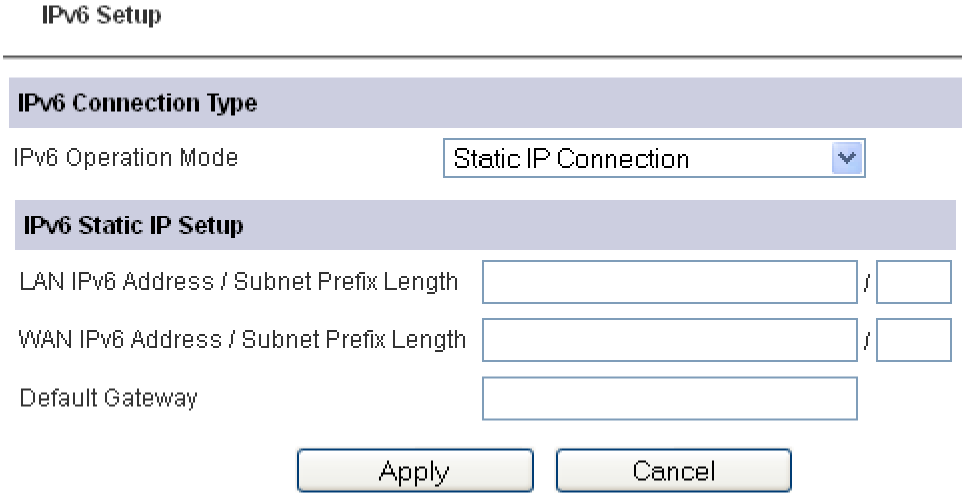
IPv6 Setup

IPv6 Connection Type

IPv6 Operation Mode: Disable

Static IP Connection

User can configure IPv6 Static IP Connection in here.



IPv6 Setup

IPv6 Connection Type

IPv6 Operation Mode: Static IP Connection

IPv6 Static IP Setup

LAN IPv6 Address / Subnet Prefix Length: /

WAN IPv6 Address / Subnet Prefix Length: /

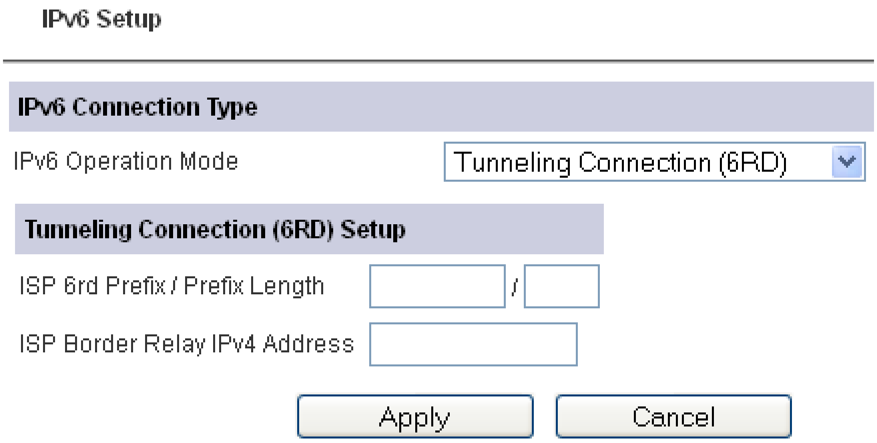
Default Gateway:

Field	Description
LAN IPv6 Address / Subnet Prefix Length	**Enter LAN IPv6 Address / Subnet Prefix Length provided by ISP**

WAN IPv6 Address / Subnet Prefix Length	**Enter WAN IPv6 Address / Subnet Prefix Length provided by ISP**
Default Gateway	**Enter Default Gateway provided by ISP**

Tunneling Connection (6RD)

User can configure IPv6 Tunneling Connection (6RD) in here.



IPv6 Setup

IPv6 Connection Type

IPv6 Operation Mode: Tunneling Connection (6RD)

Tunneling Connection (6RD) Setup

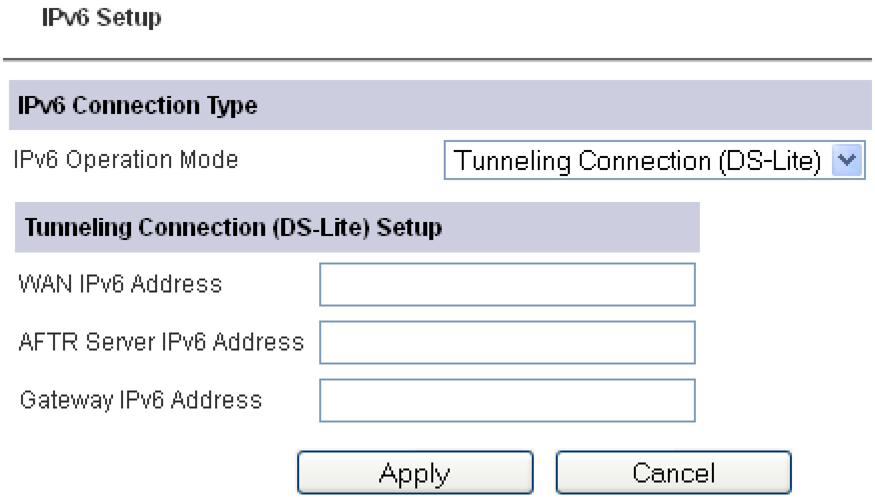
ISP 6rd Prefix / Prefix Length: /

ISP Border Relay IPv4 Address:

Field	Description
ISP 6rd Prefix / Prefix Length	**Enter ISP 6rd Prefix / Prefix Length provided by ISP**
ISP Border Relay IPv4 Address	**Enter ISP Border Relay IPv4 Address provided by ISP**

Tunneling Connection (DL-Lite)

User can configure IPv6 Tunneling Connection (DL-Lite) in here.



IPv6 Setup

IPv6 Connection Type

IPv6 Operation Mode: Tunneling Connection (DS-Lite)

Tunneling Connection (DS-Lite) Setup

WAN IPv6 Address

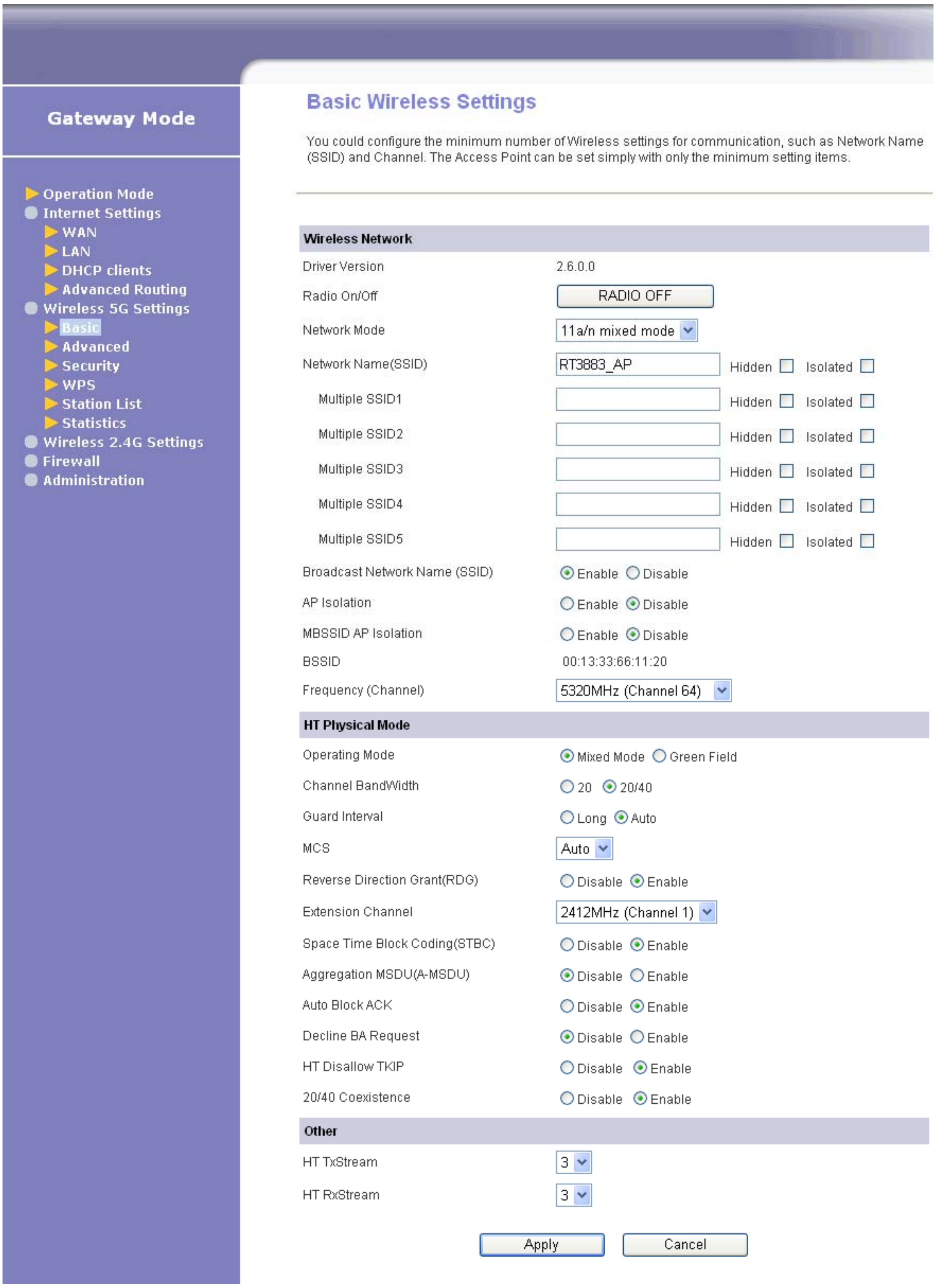
AFTR Server IPv6 Address

Gateway IPv6 Address

Field	Description
WAN IPv6 Address	**Enter WAN IPv6 Address provided by ISP**
AFTR Server IPv6 Address	**Enter AFTR Server IPv6 Address provided by ISP**
Gateway IPv6 Address	**Enter Gateway IPv6 Address provided by ISP**

13 Wireless 5G Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.



Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

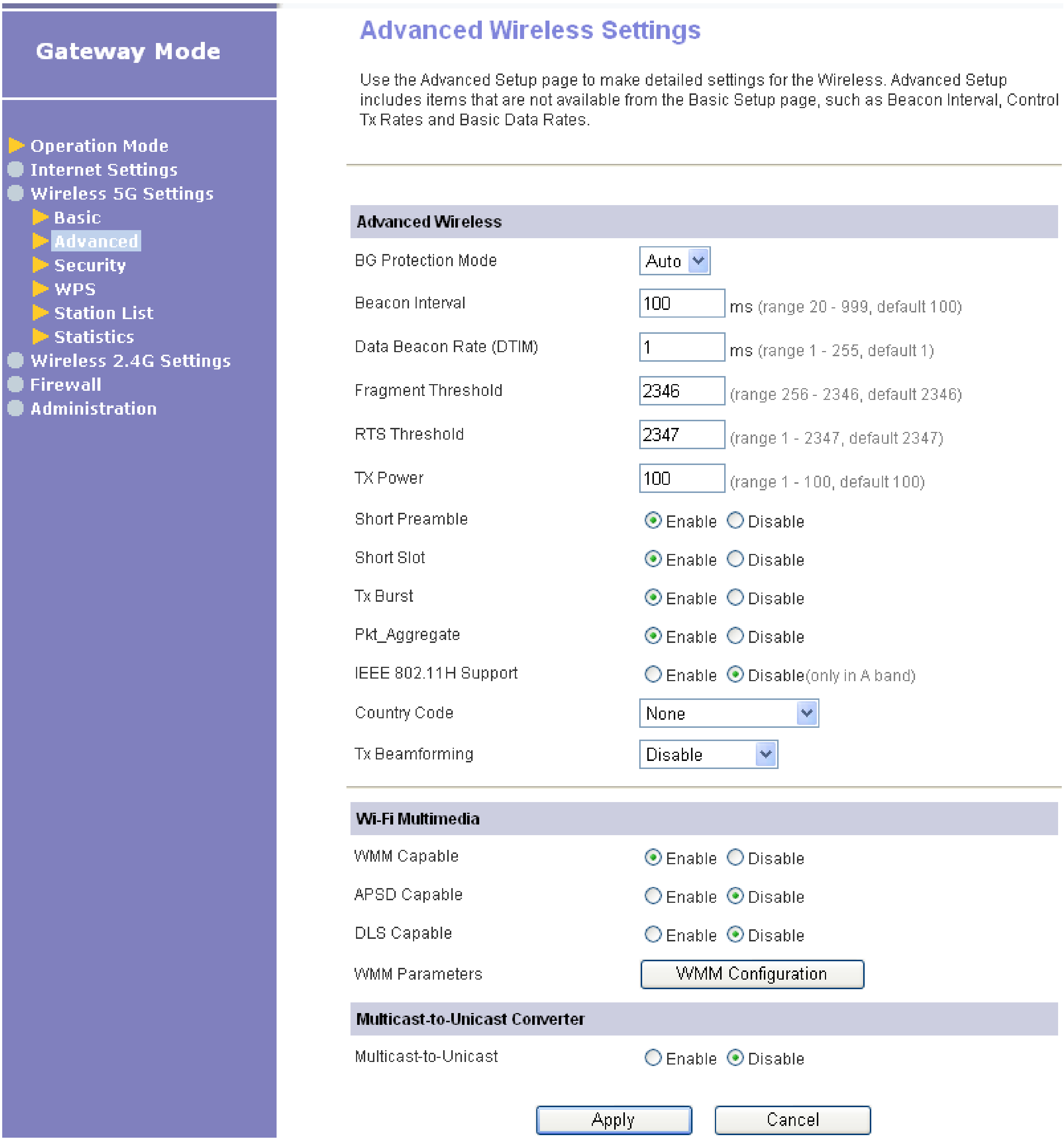
Wireless Network		
Driver Version	2.6.0.0	
Radio On/Off	RADIO OFF	
Network Mode	11a/n mixed mode	
Network Name(SSID)	RT3883_AP	Hidden □ Isolated □
Multiple SSID1		Hidden □ Isolated □
Multiple SSID2		Hidden □ Isolated □
Multiple SSID3		Hidden □ Isolated □
Multiple SSID4		Hidden □ Isolated □
Multiple SSID5		Hidden □ Isolated □
Broadcast Network Name (SSID)	● Enable ○ Disable	
AP Isolation	○ Enable ● Disable	
MBSSID AP Isolation	○ Enable ● Disable	
BSSID	00:13:33:66:11:20	
Frequency (Channel)	5320MHz (Channel 64)	
HT Physical Mode		
Operating Mode	● Mixed Mode ○ Green Field	
Channel BandWidth	○ 20 ● 20/40	
Guard Interval	○ Long ● Auto	
MCS	Auto	
Reverse Direction Grant(RDG)	○ Disable ● Enable	
Extension Channel	2412MHz (Channel 1)	
Space Time Block Coding(STBC)	○ Disable ● Enable	
Aggregation MSDU(A-MSDU)	● Disable ○ Enable	
Auto Block ACK	○ Disable ● Enable	
Decline BA Request	● Disable ○ Enable	
HT Disallow TKIP	○ Disable ● Enable	
20/40 Coexistence	○ Disable ● Enable	
Other		
HT TxStream	3	
HT RxStream	3	

Field	Description
Radio Off	**Enable/Disable the wireless.**
Network Mode	**There are 8 modes can choose, 11b/g mixed mode, 11b only, 11g only, 11b/g/n mixed mode, 11n only(2.4G), 11a only, 11a/n mixed mode and 11n only(5G).**
Network Name(SSID)	**set up the wireless ID, default is RT3883_AP.**
Multiple SSID 1 ~ 5	**You can set up to 5 SSID for this wireless network.**
Broadcast Network Name(SSID)	**Enable/Disable the SSID broadcast.**
AP Isolation	**Enable/Disable this function. Create a separate virtual network for your wireless network. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. You may want to utilize this feature if you have many guests that frequent your wireless network.**
MBSSID AP Isolation	**Enable/Disable this function.**
BSSID	**Displays the Basic Service Set Identity (BSSID) of this router. This parameter is the same as the MAC address of LAN port.**
Frequency (Channel)	**Select a Frequency (Channel)**
Operating Mode	**Select the Operating Mode**
Channel BandWidth	**Select the Channel BandWidth**
Guard Interval	**Select the Guard Interval**
MCS	**Select the MCS**
Reverse Direction Grant(RDG)	**Enable/Disable the Reverse Direction Grant(RDG)**
Extension Channel	**Enable/Disable the Extension Channel**
Space Time Block Coding(STBC)	**Enable/Disable the Space Time Block Coding(STBC)**
Aggregation MSDU(A-MSDU)	**Enable/Disable the Aggregation MSDU(A-MSDU)**
Auto Block ACK	**Enable/Disable the Auto Block ACK**
Decline BA Request	**Enable/Disable the Decline BA Request**

Field	Description
HT Disallow TKIP	**Enable/Disable the HT Disallow TKIP**
20/40 Coexistence	**Enable/Disable the 20/40 Coexistence**
HT TxStream	**Select the HT TxStream from the drop-down list**
HT RxStream	**Select the HT RxStream from the drop-down list**

14 Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.



Advanced Wireless Settings

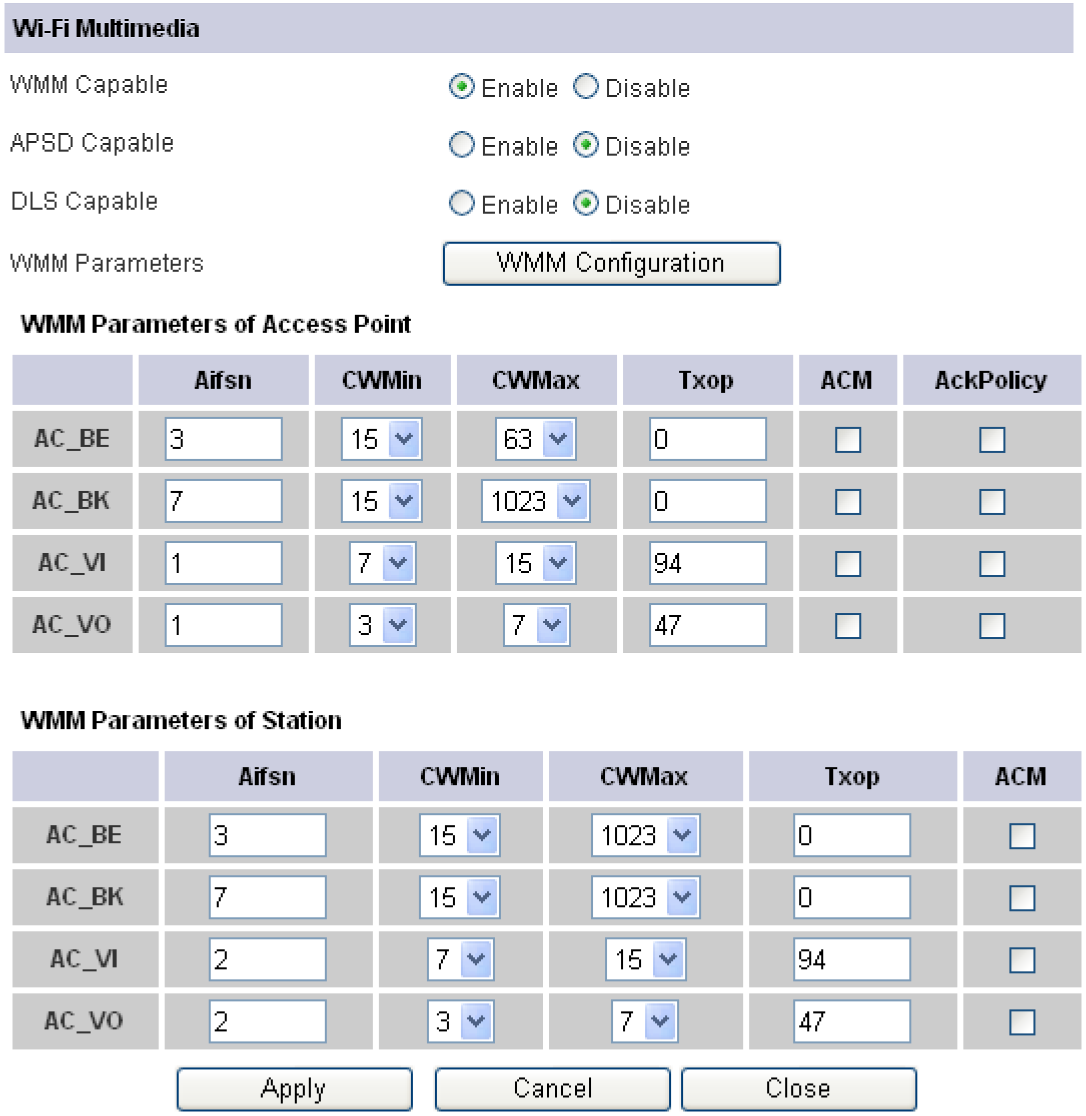
Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Advanced Wireless	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	● Enable ○ Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	● Enable ○ Disable
IEEE 802.11H Support	○ Enable ● Disable(only in A band)
Country Code	None
Tx Beamforming	Disable

Wi-Fi Multimedia	
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
DLS Capable	○ Enable ● Disable
WMM Parameters	WMM Configuration

Multicast-to-Unicast Converter	
Multicast-to-Unicast	○ Enable ● Disable

Advanced Wireless	
Field	Description
BG Protection Mode	**Some 802.11g wireless adapters support 802.11g protections, which allows the adapter search for 802.11b/g singles only. Select "Auto" to turns it on or off automatically, select "On" to support protection or select "Off" to disable this function.**
Beacon Interval	**Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. Default (100ms) is recommended.**
Data Beacon Rate(DTIM)	**Enter a value between 1 and 255 (default 1) for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.**
Fragment Threshold	**This value should remain at its default setting of 2346. If you experience a high packet error rate, you may slightly increase your fragmentation threshold within the value range of 0 to 2346. Setting the fragmentation threshold too low may result in poor performance.**
RTS Threshold	**Request To Send threshold. This value should remain at its default setting of 2347. If you encounter inconsistent data flow, only minor modifications to the value range between 1 and 2347 are recommended.**
Tx Power	**Transmit power. You can set the output power of wireless radio. This value should remain at its default setting of 100.**
Short Preamble	**The length of CRC blocks in the frames during the wireless communication.**
Short Slot	**Indicates that the 802.11g network is using a short slot time because there are no legacy (802.11b) stations present**
Tx Burst	**elect to enable or disable connecting to a Tx Burst supported device.**
Pkt_Aggregate	**To aggregate lots of packets into a big one before transmitting packets. This can reduce control packet overhead.**
IEEE 802.11H Support	**Enable/Disable.**
Country Code	**Select wireless country code. Six countries can choose.**
Tx Beamforming	**Enable/Disable the Tx Beamforming**



Wi-Fi Multimedia

WMM Capable ● Enable ○ Disable

APSD Capable ○ Enable ● Disable

DLS Capable ○ Enable ● Disable

WMM Parameters [WMM Configuration]

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	1023	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

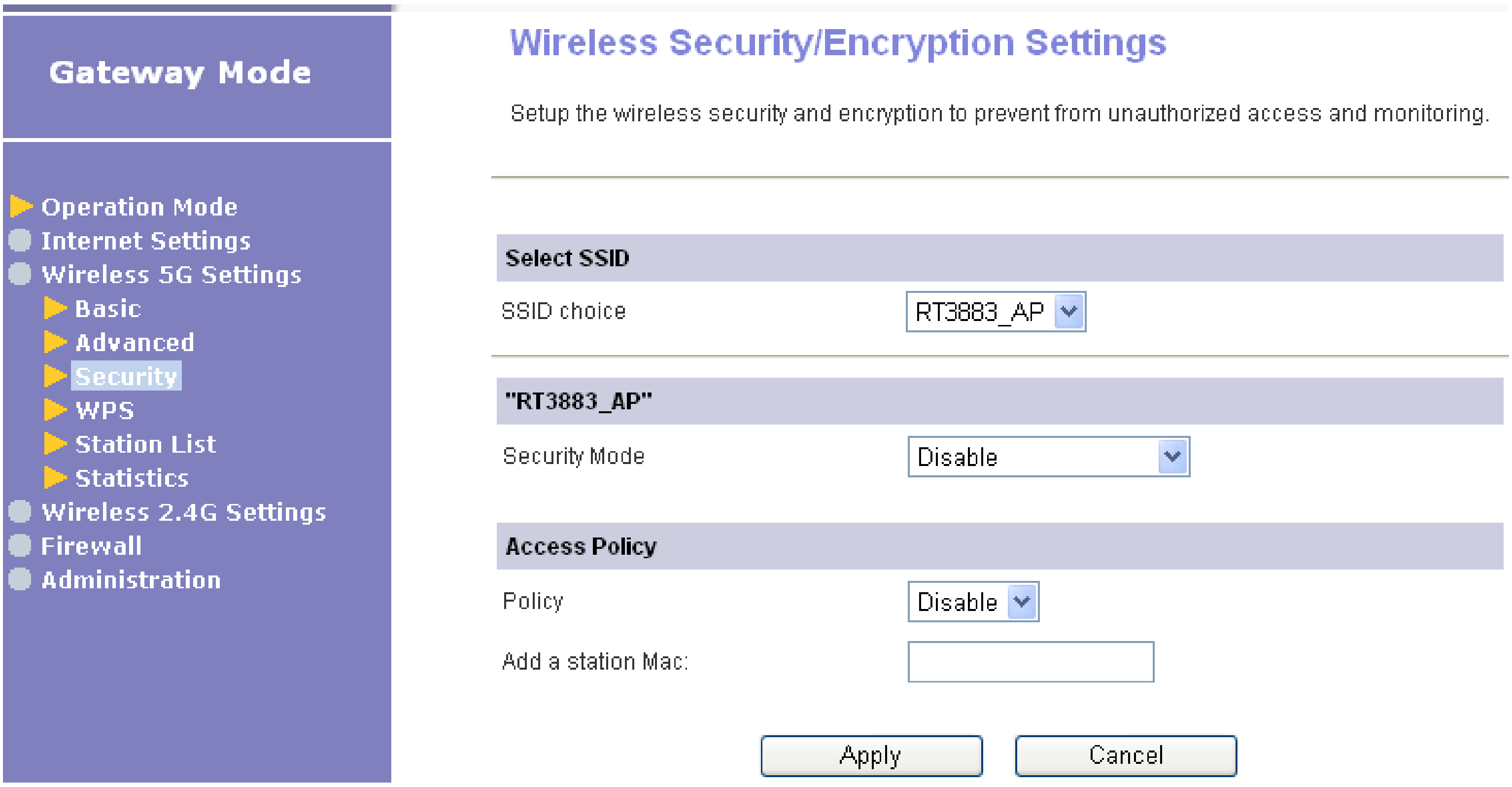
WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	□
AC_BK	7	15	1023	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

Wi-Fi Multimedia	
Field	Description
WMM Capable	**This will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network.**
APSD Capable	**Automatic Power saves Delivery. Select to enable / disable data flow using power saving mode during transmitting.**
DLS Capable	**Enable/Disable this function.**
WMM Parameters	**You can configure WMM parameters by clicking on the** [WMM Configuration] **button. The configuration window pops up (as shown below). Manually configure the parameters and click on the "Apply" button to execute.**
Multicast-to-Unicast	**It can receives Multicast streams from the network backbone, converts them to Unicast format, and routes them to the set-top-boxes of end-users over the last mile infrastructure (e.g. DSL, Ethernet, WiFi).**

15 Wireless Security/Encryption Settings

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



Wireless Security/Encryption Settings

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

Select SSID

SSID choice: RT3883_AP

"RT3883_AP"

Security Mode: Disable

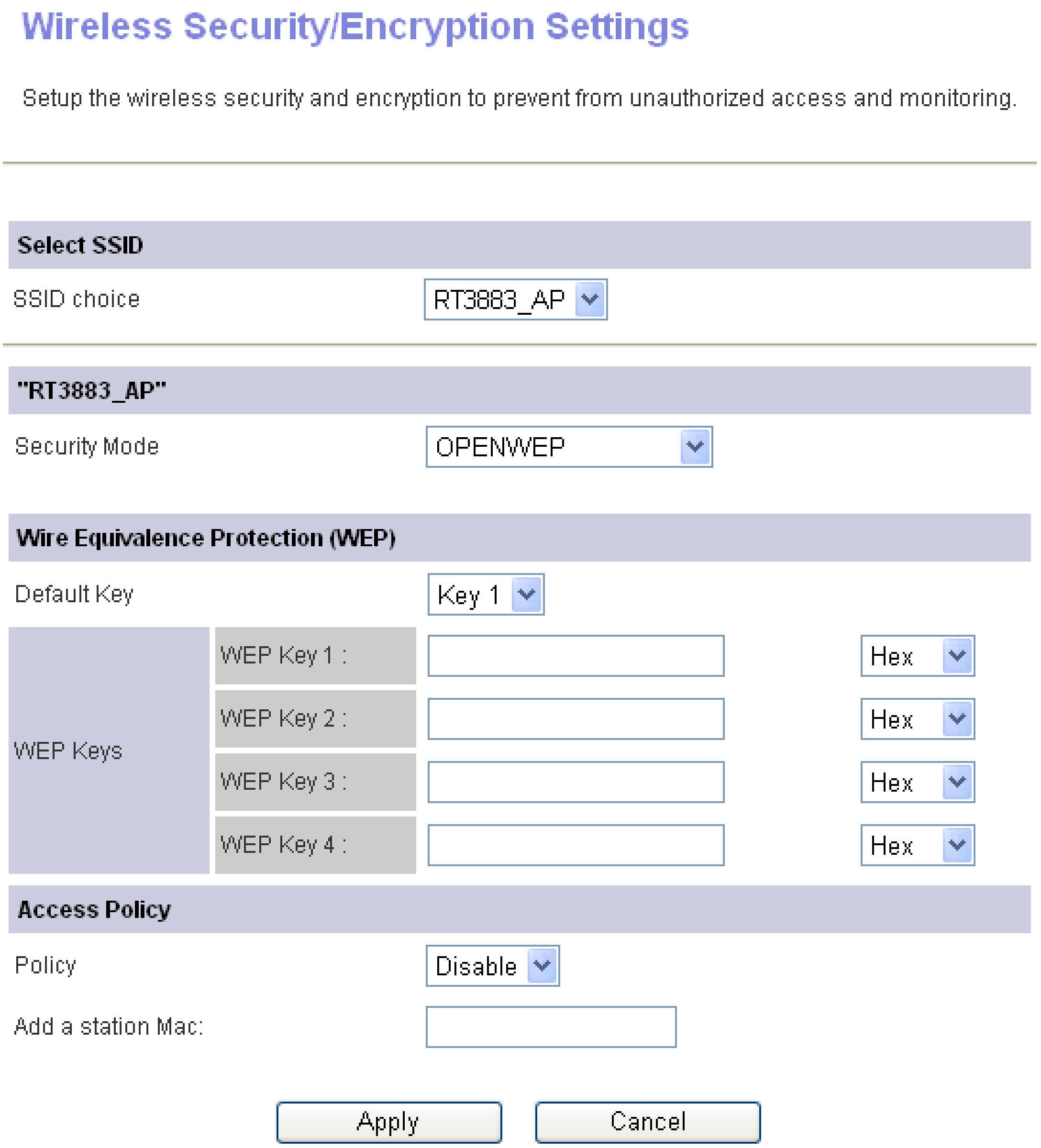
Access Policy

Policy: Disable

Add a station Mac:

Advanced Wireless	
Field	Description
SSID Choice	**Please choose a SSID you have set for this router in the Wireless Settings > Basic Settings from the drop-down list. The SSID will be shown on the wireless network for recognizing..**
Security Mode	**There are 10 modes for you to select: Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, and WPA-PSKWPA2-PSK, WPA1WPA2, 802.1x. Please refer to the following description.**
Policy	**Default is Disable, you can allow or Reject the wireless station.**
Add a station Mac	**Fill out the MAC address of wireless station you want to allow or reject.**

Security Mode -- OPENWEP / WEP Auto



Wireless Security/Encryption Settings

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

Select SSID

SSID choice: RT3883_AP

"RT3883_AP"

Security Mode: OPENWEP

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

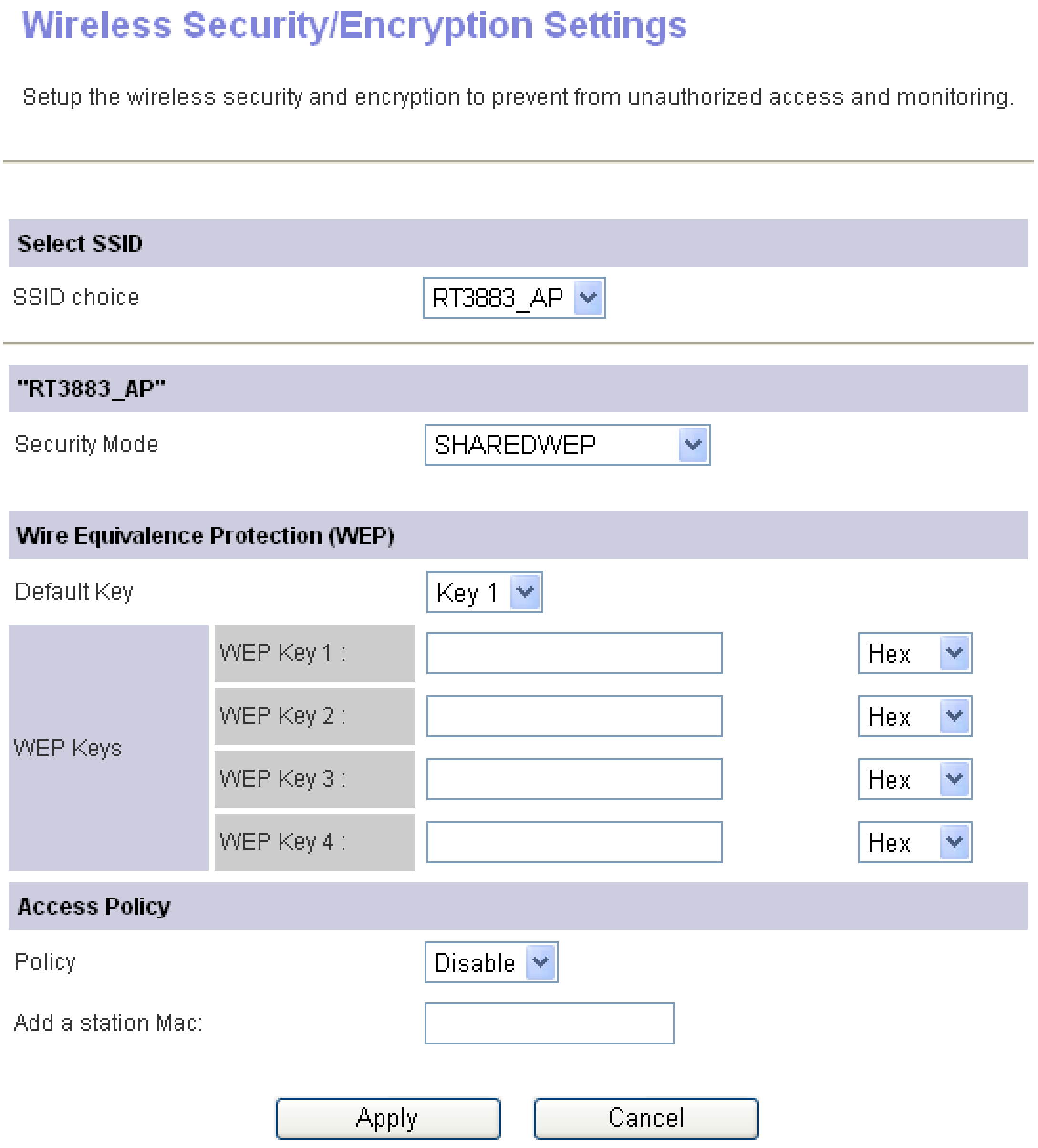
Access Policy

Policy: Disable

Add a station Mac:

Field	Description
Default Key	**Select to use the WEP key value of 1, 2, 3 or 4 as in the following settings.**
WEP Keys	**Select ASCII or Hex to setup the key value. ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F.**
Policy	**Default is Disable, you can allow or Reject the wireless station.**
Add a station Mac	**Fill out the MAC address of wireless station you want to allow or reject.**

Security Mode -- SHAREDWEP / WEP Auto



Wireless Security/Encryption Settings

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

Select SSID

SSID choice: RT3883_AP

"RT3883_AP"

Security Mode: SHAREDWEP

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

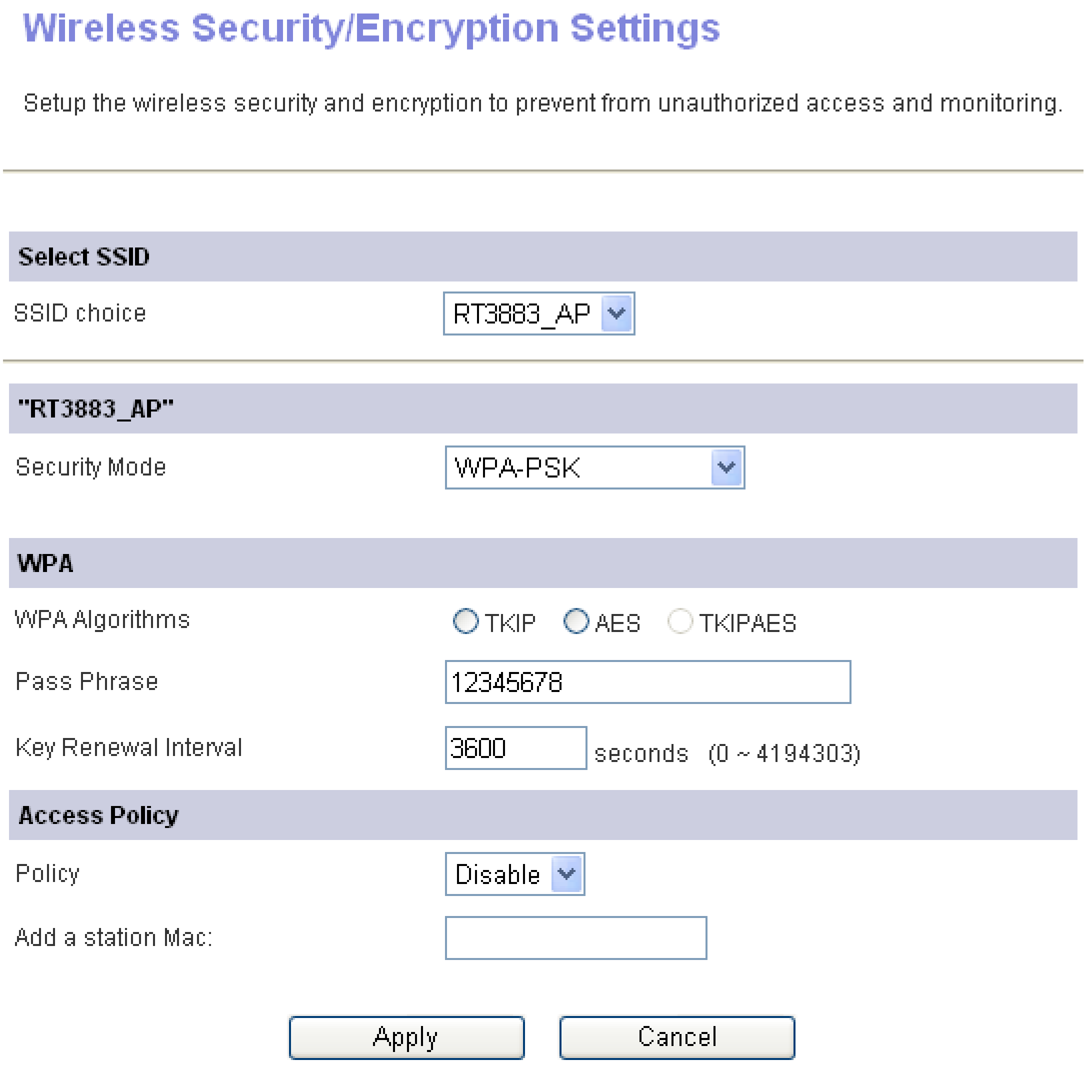
Access Policy

Policy: Disable

Add a station Mac:

Field	Description
Default Key	**Select to use the WEP key value of 1, 2, 3 or 4 as in the following settings.**
WEP Keys	**Select ASCII or Hex to setup the key value. ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F.**
Policy	**Default is Disable, you can allow or Reject the wireless station.**
Add a station Mac	**Fill out the MAC address of wireless station you want to allow or reject.**

Security Mode -- WPA-PSK / WPA2-PSK / WPAPSKWPA2PSK



Wireless Security/Encryption Settings

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

Select SSID

SSID choice: RT3883_AP

"RT3883_AP"

Security Mode: WPA-PSK

WPA

WPA Algorithms: ○ TKIP ○ AES ○ TKIPAES

Pass Phrase: 12345678

Key Renewal Interval: 3600 seconds (0 ~ 4194303)

Access Policy

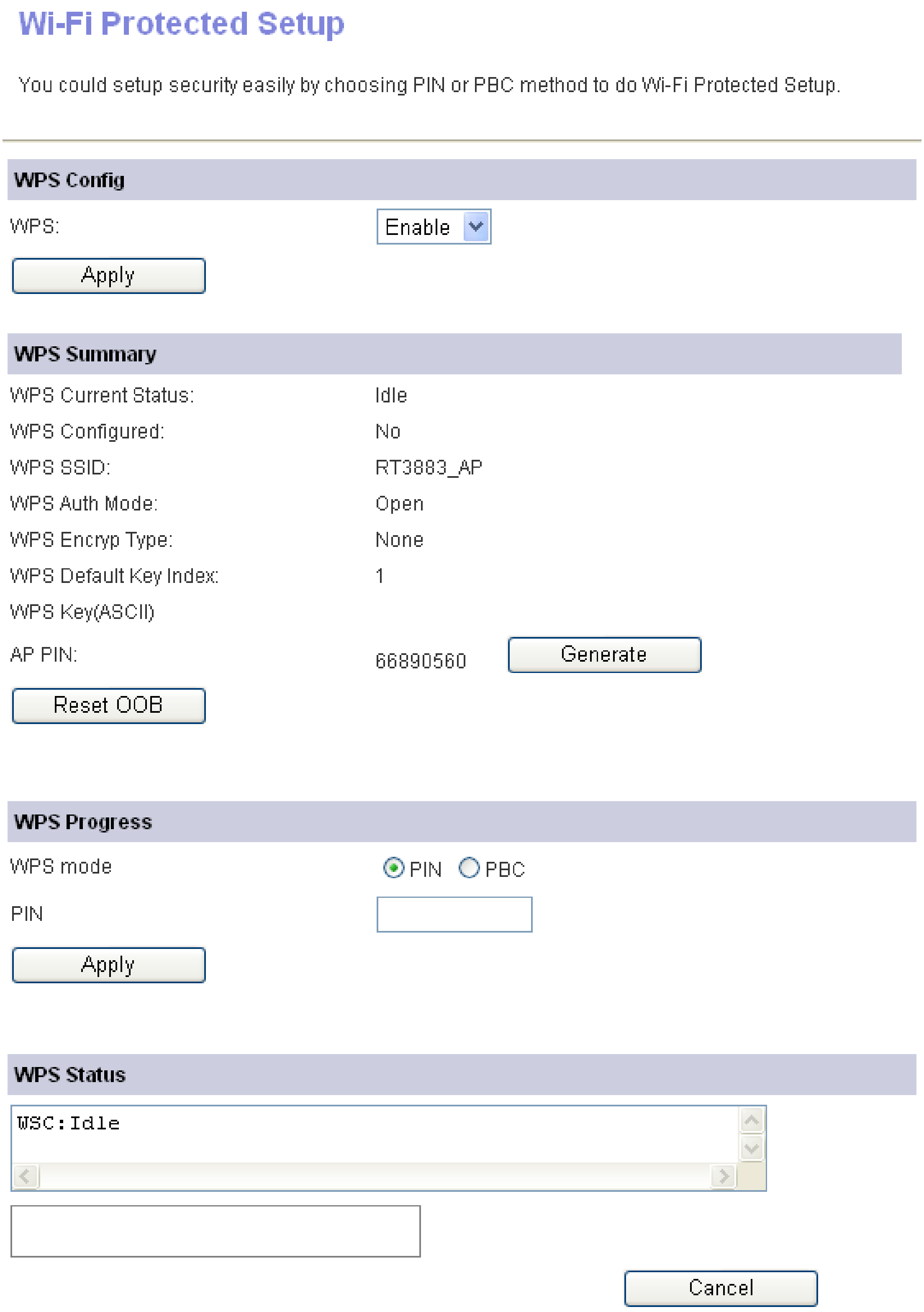
Policy: Disable

Add a station Mac:

Field	Description
WPA Algorithms	**Mark the option to enable modes of TKIP, AES, or TKIPAES (TKIPAES is only available in the security modes of WPA2-PSK and WPAPSKWPA2PSK)**
Pass Phrase	**Enter a pass phrase encryption key format (8~32 bytes).**
Key Renewal Interval	**Enter a value to setup the WPA key renewal interval. The device regenerates the key in every interval seconds that you have setup without disconnection.**
Policy	**Default is Disable, you can allow or Reject the wireless station.**
Add a station Mac	**Fill out the MAC address of wireless station you want to allow or reject.**

16 Wi-Fi Protected Setup (WPS)

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. This Router supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.



Wi-Fi Protected Setup

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Config

WPS:	Enable

WPS Summary

WPS Current Status:	Idle
WPS Configured:	No
WPS SSID:	RT3883_AP
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	66890560

WPS Progress

WPS mode	● PIN ○ PBC
PIN	

WPS Status

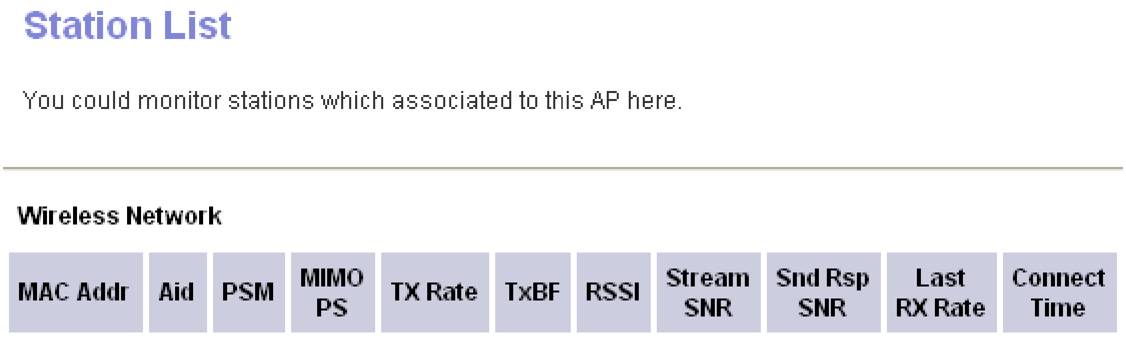
```
WSC:Idle
```

Field	Description
WPS	**Enable/Disable the WPS. Default setting is disable.**
WPS Summary	**Shows the information of WPS current status, configured, SSID, authentication mode, and pre-shared key. Click on Reset OOB button to Reset WPS AP to the OOB (out of box) configuration.**
WPS Progress	**Show the WPS current status.**

WPS mode	
Field	Description
PIN method (Personal Identification Number)	**read the PIN from either a sticker on the new STA or a display.**
PBC method (Push Button Communication)	**in which the user simply has to push a button, either an actual or virtual one, on both the AP and the new STA. (Users can simply push the**
PIN	**Users have to fill in the PIN code to enrollee device if selecting PIN mode as the WPS Config method.**

17 Station List

You could monitor stations which associated to this AP here.



Station List

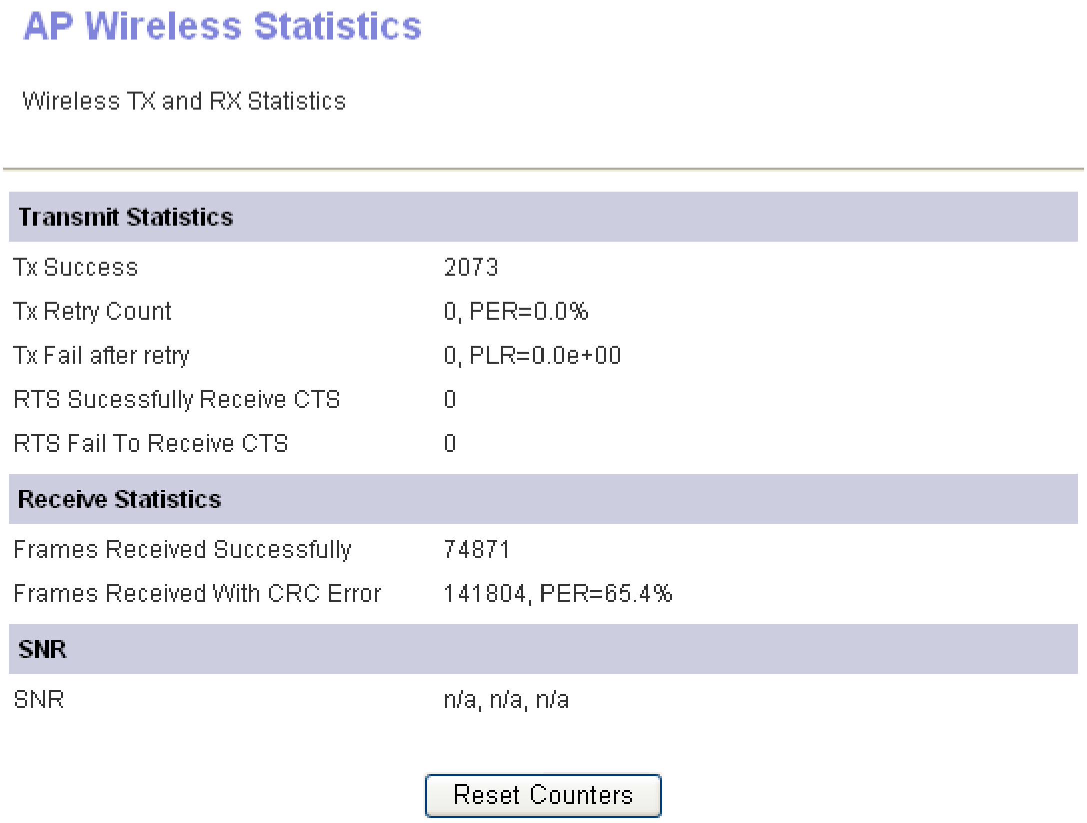
You could monitor stations which associated to this AP here.

Wireless Network

MAC Addr	Aid	PSM	MIMO PS	TX Rate	TxBF	RSSI	Stream SNR	Snd Rsp SNR	Last RX Rate	Connect Time

18 AP Wireless Statistics

Wireless TX and RX Statistics.



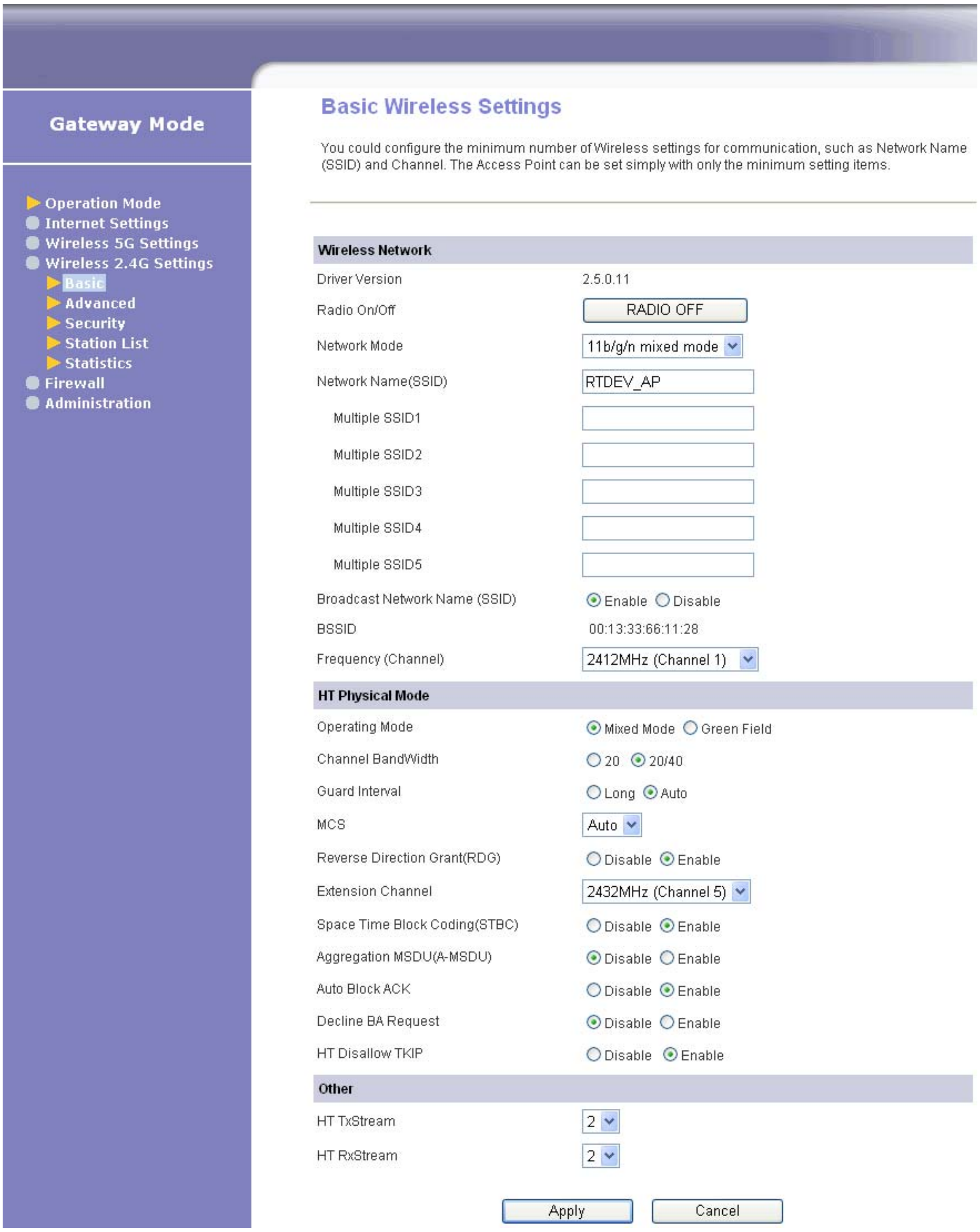
AP Wireless Statistics

Wireless TX and RX Statistics

Transmit Statistics	
Tx Success	2073
Tx Retry Count	0, PER=0.0%
Tx Fail after retry	0, PLR=0.0e+00
RTS Sucessfully Receive CTS	0
RTS Fail To Receive CTS	0
Receive Statistics	
Frames Received Successfully	74871
Frames Received With CRC Error	141804, PER=65.4%
SNR	
SNR	n/a, n/a, n/a

19 Wireless 2.4G Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.



Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

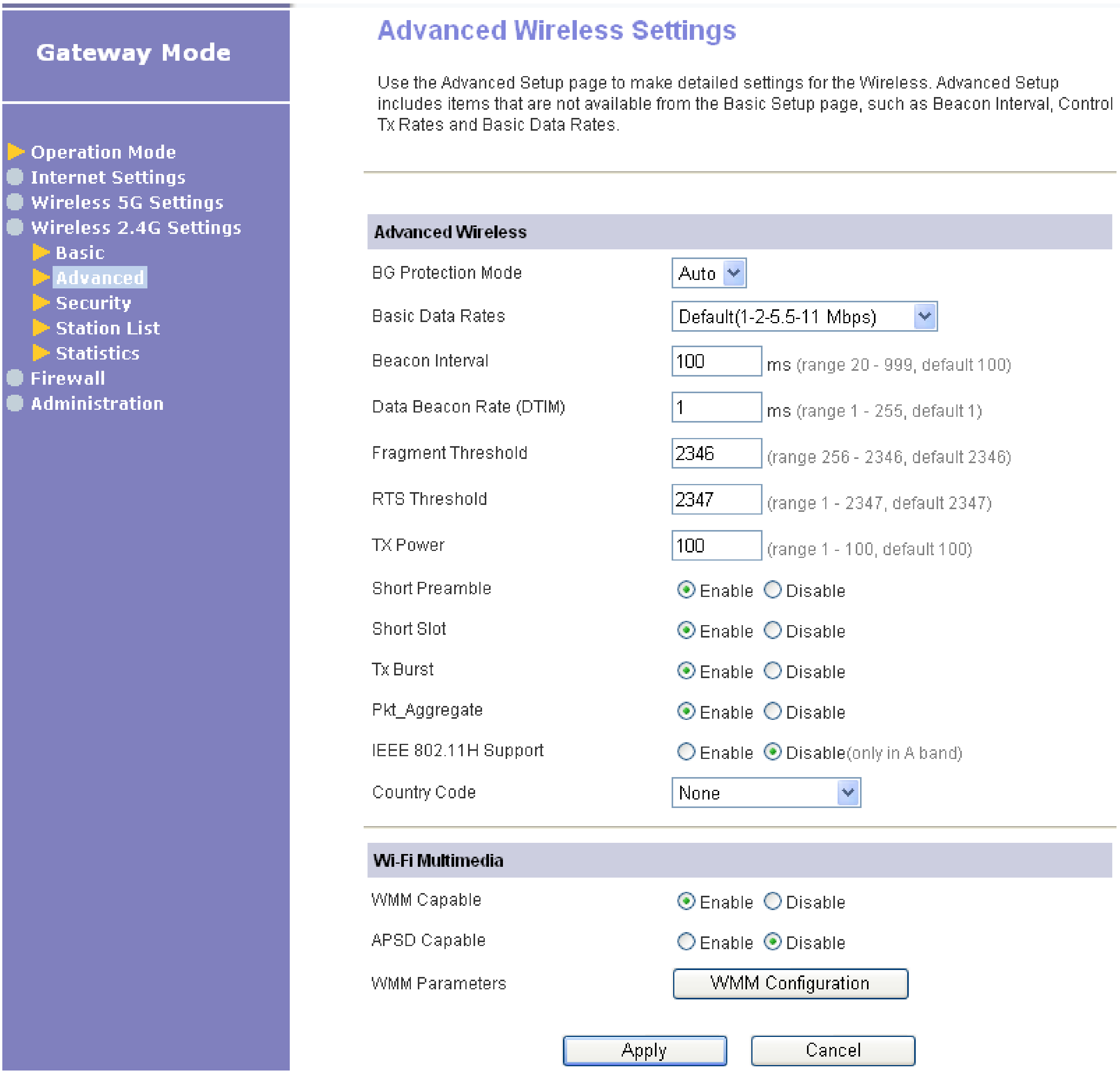
Wireless Network	
Driver Version	2.5.0.11
Radio On/Off	RADIO OFF
Network Mode	11b/g/n mixed mode
Network Name(SSID)	RTDEV_AP
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Broadcast Network Name (SSID)	● Enable ○ Disable
BSSID	00:13:33:66:11:28
Frequency (Channel)	2412MHz (Channel 1)
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Auto
MCS	Auto
Reverse Direction Grant(RDG)	○ Disable ● Enable
Extension Channel	2432MHz (Channel 5)
Space Time Block Coding(STBC)	○ Disable ● Enable
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
HT Disallow TKIP	○ Disable ● Enable
Other	
HT TxStream	2
HT RxStream	2

Field	Description
Radio Off	**Enable/Disable the wireless.**
Network Mode	**There are 8 modes can choose, 11b/g mixed mode, 11b only, 11g only, 11b/g/n mixed mode, 11n only(2.4G), 11a only, 11a/n mixed mode and 11n only(5G).**
Network Name(SSID)	**set up the wireless ID, default is RT3883_AP.**
Multiple SSID 1 ~ 5	**You can set up to 5 SSID for this wireless network.**
Broadcast Network Name(SSID)	**Enable/Disable the SSID broadcast.**
BSSID	**Displays the Basic Service Set Identity (BSSID) of this router. This parameter is the same as the MAC address of LAN port.**
Frequency (Channel)	**Select a Frequency (Channel)**
Operating Mode	**Select the Operating Mode**
Channel BandWidth	**Select the Channel BandWidth**
Guard Interval	**Select the Guard Interval**
MCS	**Select the MCS**
Reverse Direction Grant(RDG)	**Enable/Disable the Reverse Direction Grant(RDG)**
Extension Channel	**Enable/Disable the Extension Channel**
Space Time Block Coding(STBC)	**Enable/Disable the Space Time Block Coding(STBC)**
Aggregation MSDU(A-MSDU)	**Enable/Disable the Aggregation MSDU(A-MSDU)**
Auto Block ACK	**Enable/Disable the Auto Block ACK**
Decline BA Request	**Enable/Disable the Decline BA Request**

Field	Description
HT Disallow TKIP	**Enable/Disable the HT Disallow TKIP**
HT TxStream	**Select the HT TxStream from the drop-down list**
HT RxStream	**Select the HT RxStream from the drop-down list**

20 Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.



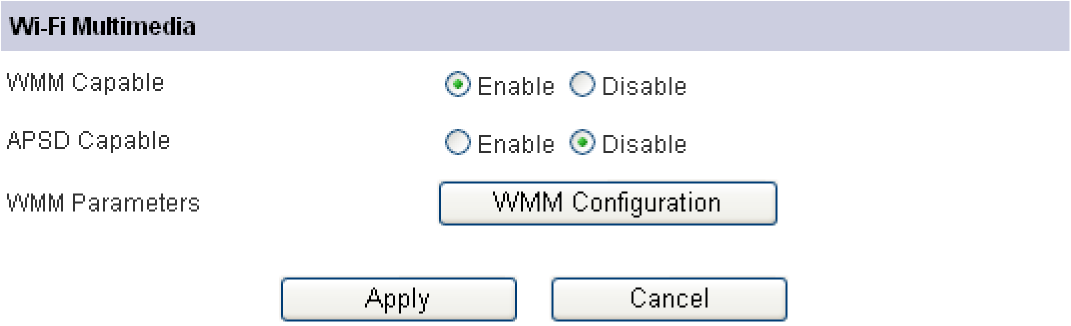
Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Advanced Wireless	
BG Protection Mode	Auto
Basic Data Rates	Default(1-2-5.5-11 Mbps)
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	● Enable ○ Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	● Enable ○ Disable
IEEE 802.11H Support	○ Enable ● Disable(only in A band)
Country Code	None

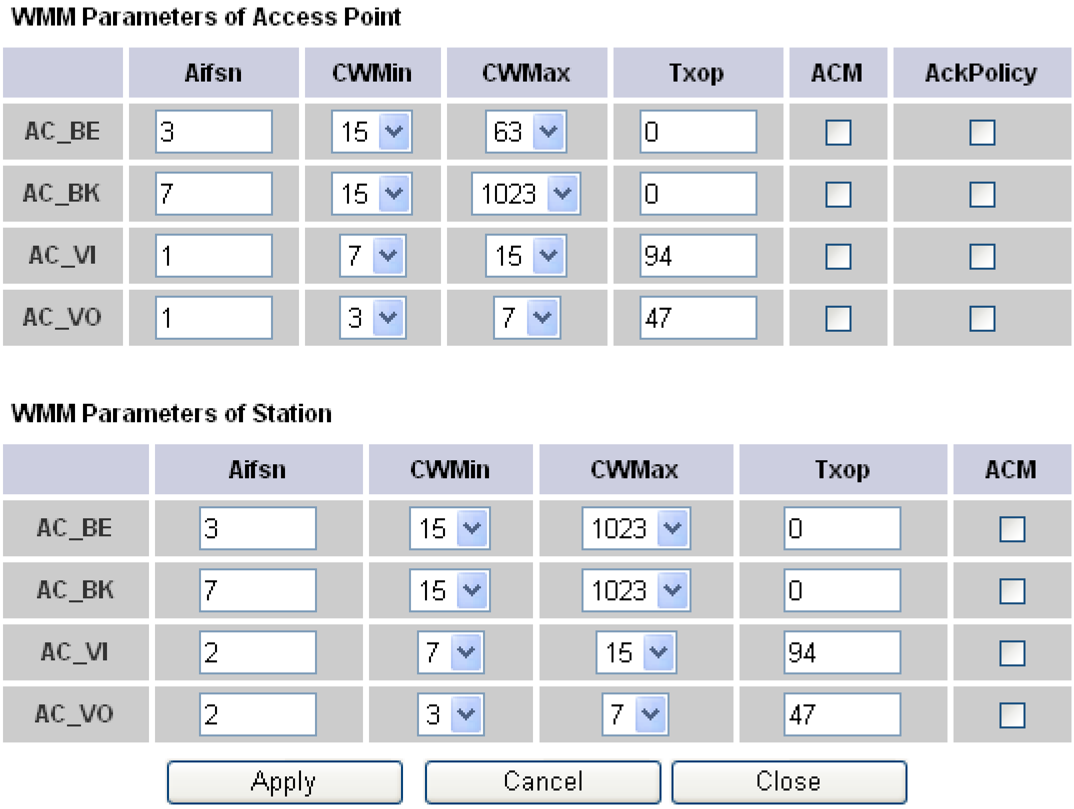
Wi-Fi Multimedia	
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
WMM Parameters	WMM Configuration

Advanced Wireless	
Field	Description
BG Protection Mode	**Some 802.11g wireless adapters support 802.11g protections, which allows the adapter search for 802.11b/g singles only. Select "Auto" to turns it on or off automatically, select "On" to support protection or select "Off" to disable this function.**
Basic Data Rates	**Configure the Basic Data Rates**
Beacon Interval	**Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. Default (100ms) is recommended.**
Data Beacon Rate(DTIM)	**Enter a value between 1 and 255 (default 1) for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.**
Fragment Threshold	**This value should remain at its default setting of 2346. If you experience a high packet error rate, you may slightly increase your fragmentation threshold within the value range of 0 to 2346. Setting the fragmentation threshold too low may result in poor performance.**
RTS Threshold	**Request To Send threshold. This value should remain at its default setting of 2347. If you encounter inconsistent data flow, only minor modifications to the value range between 1 and 2347 are recommended.**
Tx Power	**Transmit power. You can set the output power of wireless radio. This value should remain at its default setting of 100.**
Short Preamble	**The length of CRC blocks in the frames during the wireless communication.**
Short Slot	**Indicates that the 802.11g network is using a short slot time because there are no legacy (802.11b) stations present**
Tx Burst	**elect to enable or disable connecting to a Tx Burst supported device.**
Pkt_Aggregate	**To aggregate lots of packets into a big one before transmitting packets. This can reduce control packet overhead.**
IEEE 802.11H Support	**Enable/Disable.**
Country Code	**Select wireless country code. Six countries can choose.**



Wi-Fi Multimedia

WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
WMM Parameters	WMM Configuration



WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

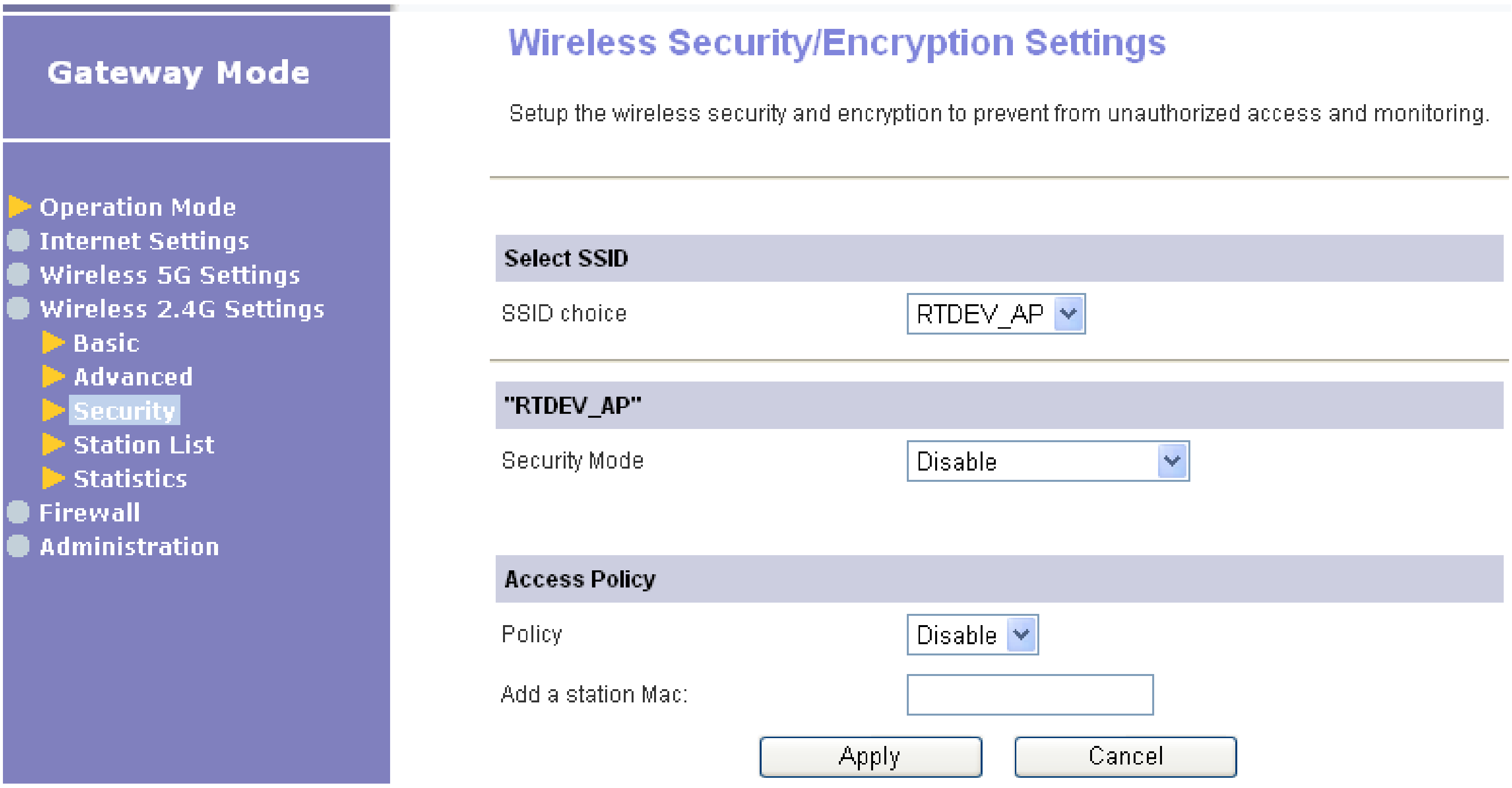
WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Wi-Fi Multimedia	
Field	Description
WMM Capable	**This will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network.**
APSD Capable	**Automatic Power saves Delivery. Select to enable / disable data flow using power saving mode during transmitting.**
DLS Capable	**Enable/Disable this function.**
WMM Parameters	**You can configure WMM parameters by clicking on the** WMM Configuration **button. The configuration window pops up (as shown below). Manually configure the parameters and click on the "Apply" button to execute.**
Multicast-to-Unicast	**It can receives Multicast streams from the network backbone, converts them to Unicast format, and routes them to the set-top-boxes of end-users over the last mile infrastructure (e.g. DSL, Ethernet, WiFi).**

21 Wireless Security/Encryption Settings

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



Wireless Security/Encryption Settings

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

Select SSID

SSID choice: RTDEV_AP

"RTDEV_AP"

Security Mode: Disable

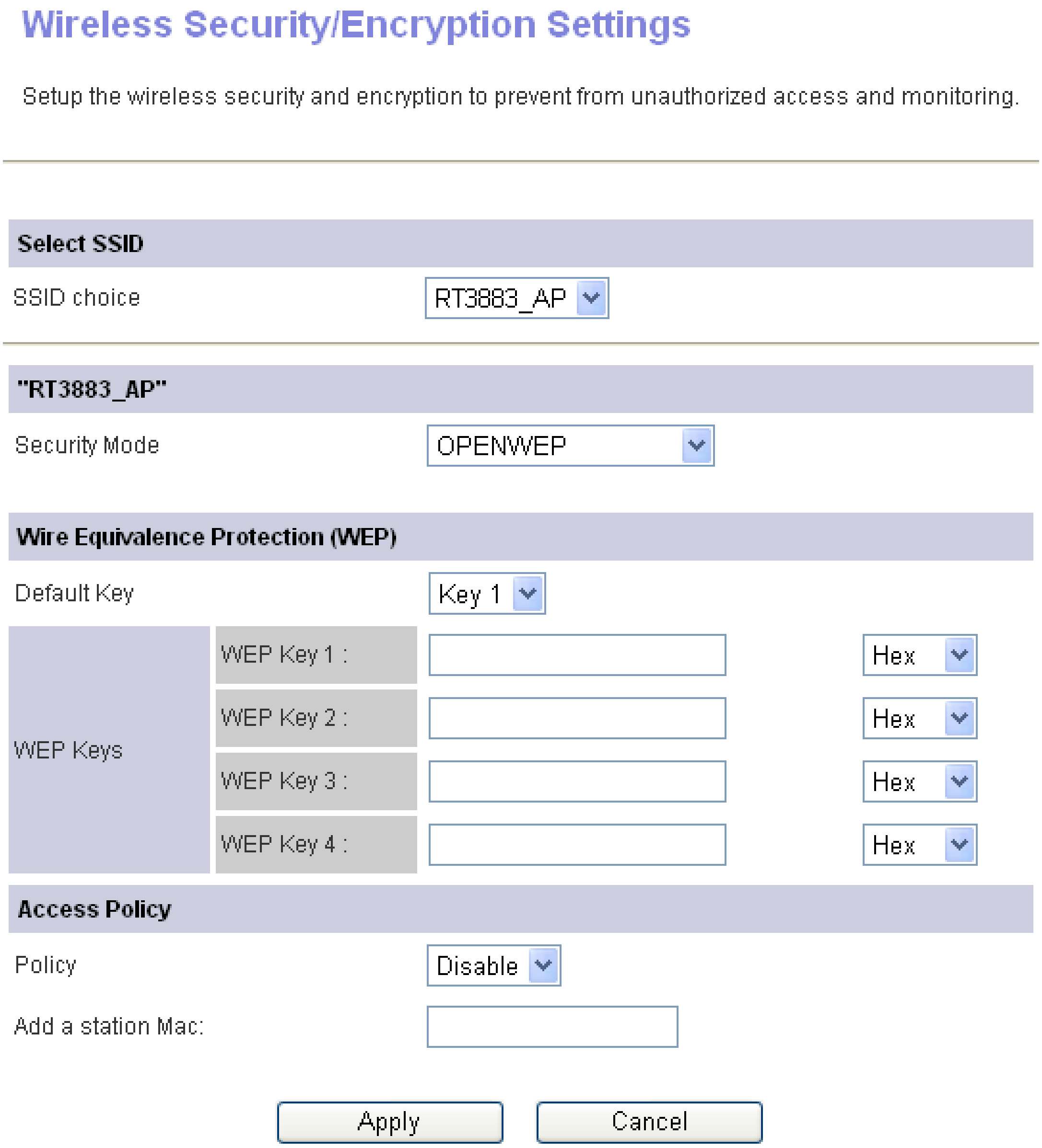
Access Policy

Policy: Disable

Add a station Mac:

Advanced Wireless	
Field	Description
SSID Choice	**Please choose a SSID you have set for this router in the Wireless Settings > Basic Settings from the drop-down list. The SSID will be shown on the wireless network for recognizing..**
Security Mode	**There are 10 modes for you to select: Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, and WPA-PSKWPA2-PSK, WPA1WPA2, 802.1x. Please refer to the following description.**
Policy	**Default is Disable, you can allow or Reject the wireless station.**
Add a station Mac	**Fill out the MAC address of wireless station you want to allow or reject.**

Security Mode -- OPENWEP / WEP Auto



Wireless Security/Encryption Settings

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

Select SSID

SSID choice: RT3883_AP

"RT3883_AP"

Security Mode: OPENWEP

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

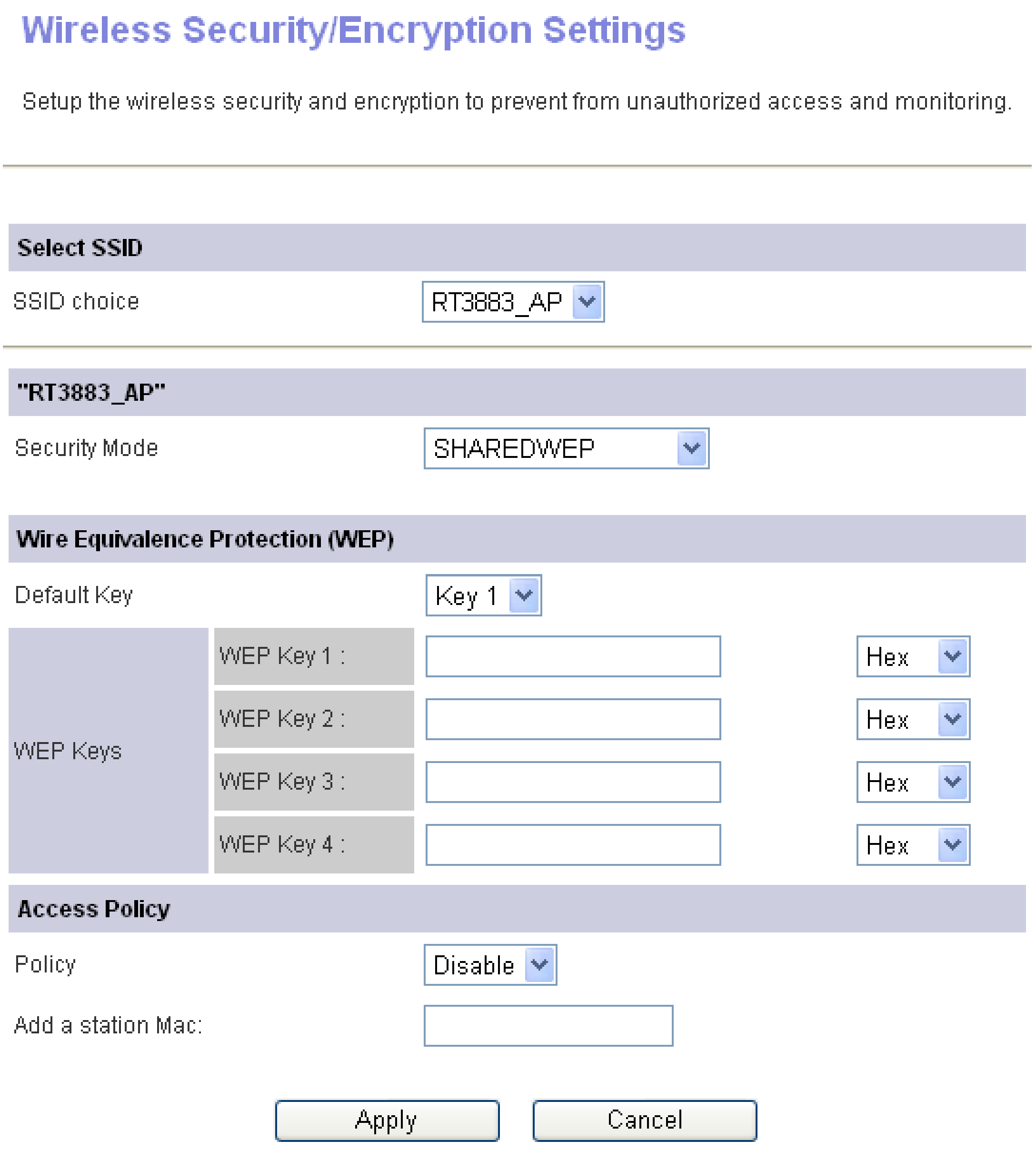
Access Policy

Policy: Disable

Add a station Mac:

Field	Description
Default Key	**Select to use the WEP key value of 1, 2, 3 or 4 as in the following settings.**
WEP Keys	**Select ASCII or Hex to setup the key value. ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F.**
Policy	**Default is Disable, you can allow or Reject the wireless station.**
Add a station Mac	**Fill out the MAC address of wireless station you want to allow or reject.**

Security Mode -- SHAREDWEP / WEP Auto



Wireless Security/Encryption Settings

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

Select SSID

SSID choice: RT3883_AP

"RT3883_AP"

Security Mode: SHAREDWEP

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

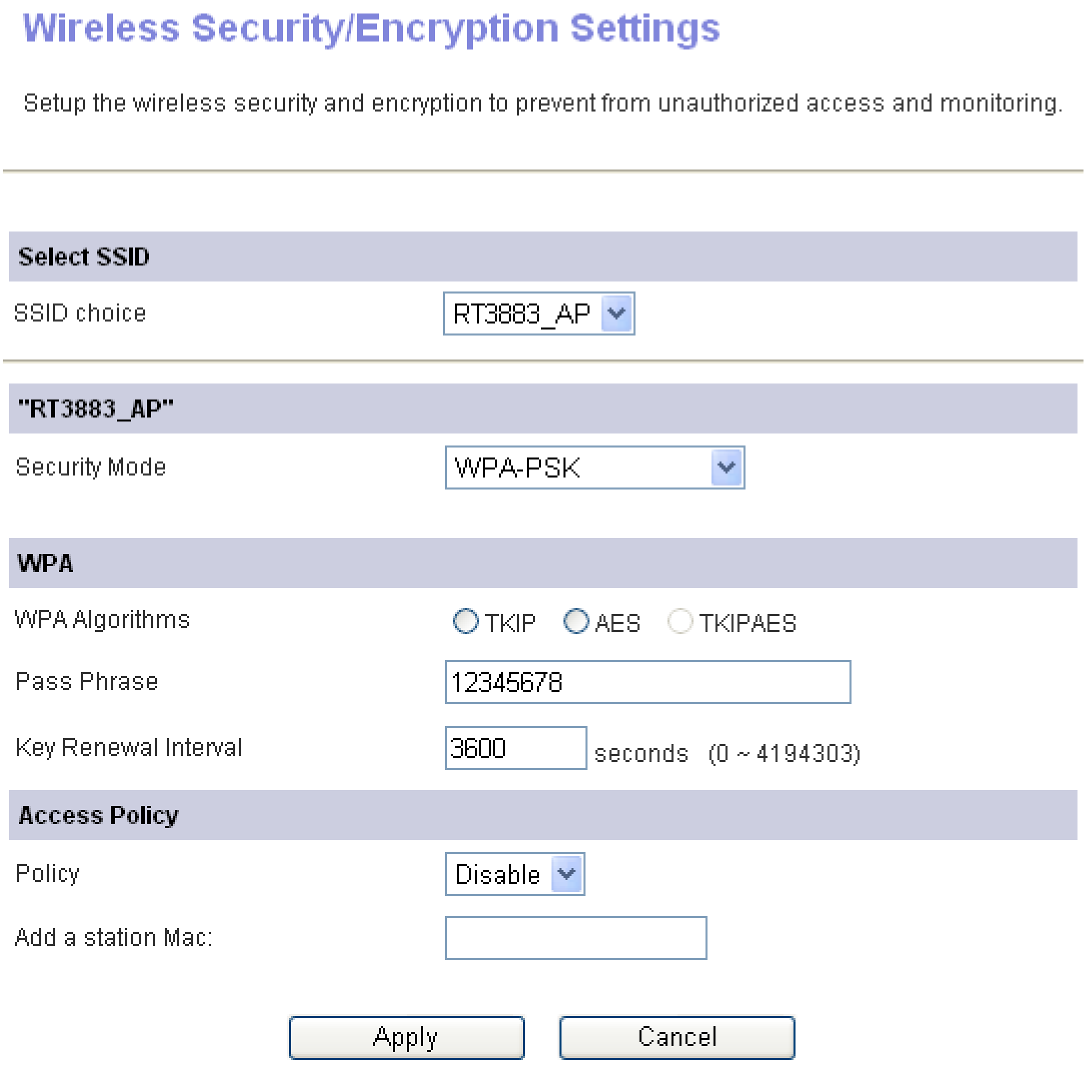
Access Policy

Policy: Disable

Add a station Mac:

Field	Description
Default Key	**Select to use the WEP key value of 1, 2, 3 or 4 as in the following settings.**
WEP Keys	**Select ASCII or Hex to setup the key value. ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F.**
Policy	**Default is Disable, you can allow or Reject the wireless station.**
Add a station Mac	**Fill out the MAC address of wireless station you want to allow or reject.**

Security Mode -- WPA-PSK / WPA2-PSK / WPAPSKWPA2PSK



Wireless Security/Encryption Settings

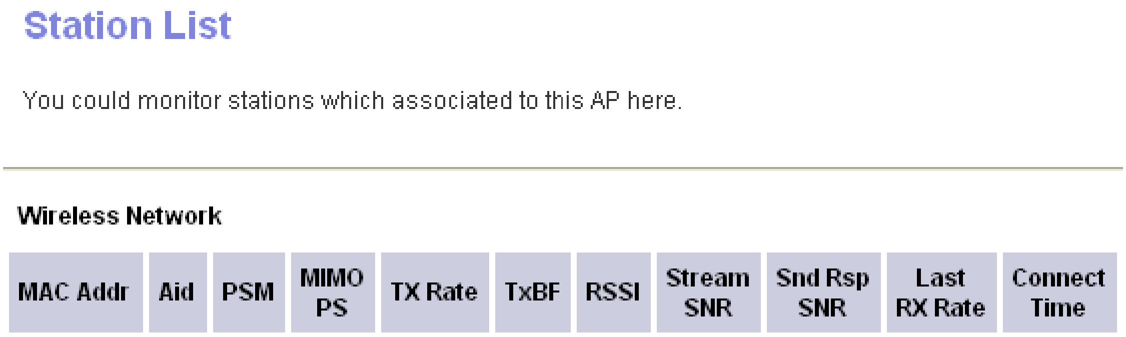
Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	RT3883_AP
"RT3883_AP"	
Security Mode	WPA-PSK
WPA	
WPA Algorithms	○ TKIP ○ AES ○ TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds (0 ~ 4194303)
Access Policy	
Policy	Disable
Add a station Mac:	

Field	Description
WPA Algorithms	**Mark the option to enable modes of TKIP, AES, or TKIPAES (TKIPAES is only available in the security modes of WPA2-PSK and WPAPSKWPA2PSK)**
Pass Phrase	**Enter a pass phrase encryption key format (8~32 bytes).**
Key Renewal Interval	**Enter a value to setup the WPA key renewal interval. The device regenerates the key in every interval seconds that you have setup without disconnection.**
Policy	**Default is Disable, you can allow or Reject the wireless station.**
Add a station Mac	**Fill out the MAC address of wireless station you want to allow or reject.**

22 Station List

You could monitor stations which associated to this AP here.



Station List

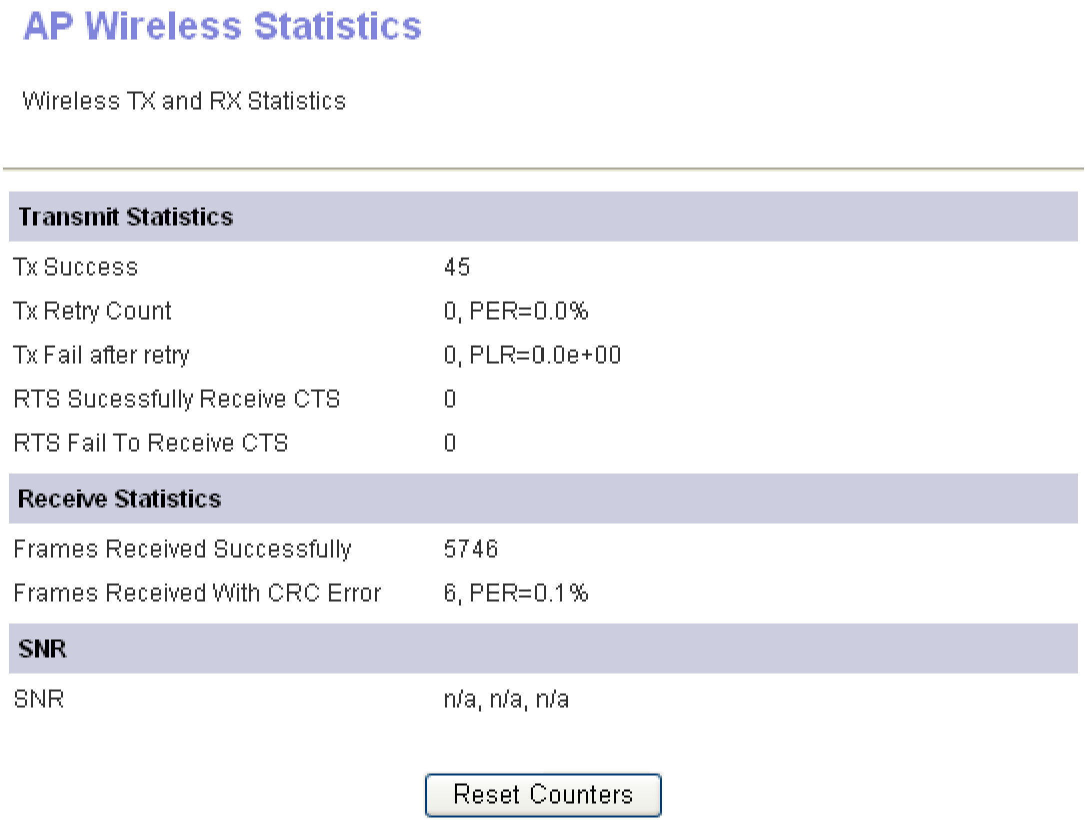
You could monitor stations which associated to this AP here.

Wireless Network

MAC Addr	Aid	PSM	MIMO PS	TX Rate	TxBF	RSSI	Stream SNR	Snd Rsp SNR	Last RX Rate	Connect Time

23 AP Wireless Statistics

Wireless TX and RX Statistics.



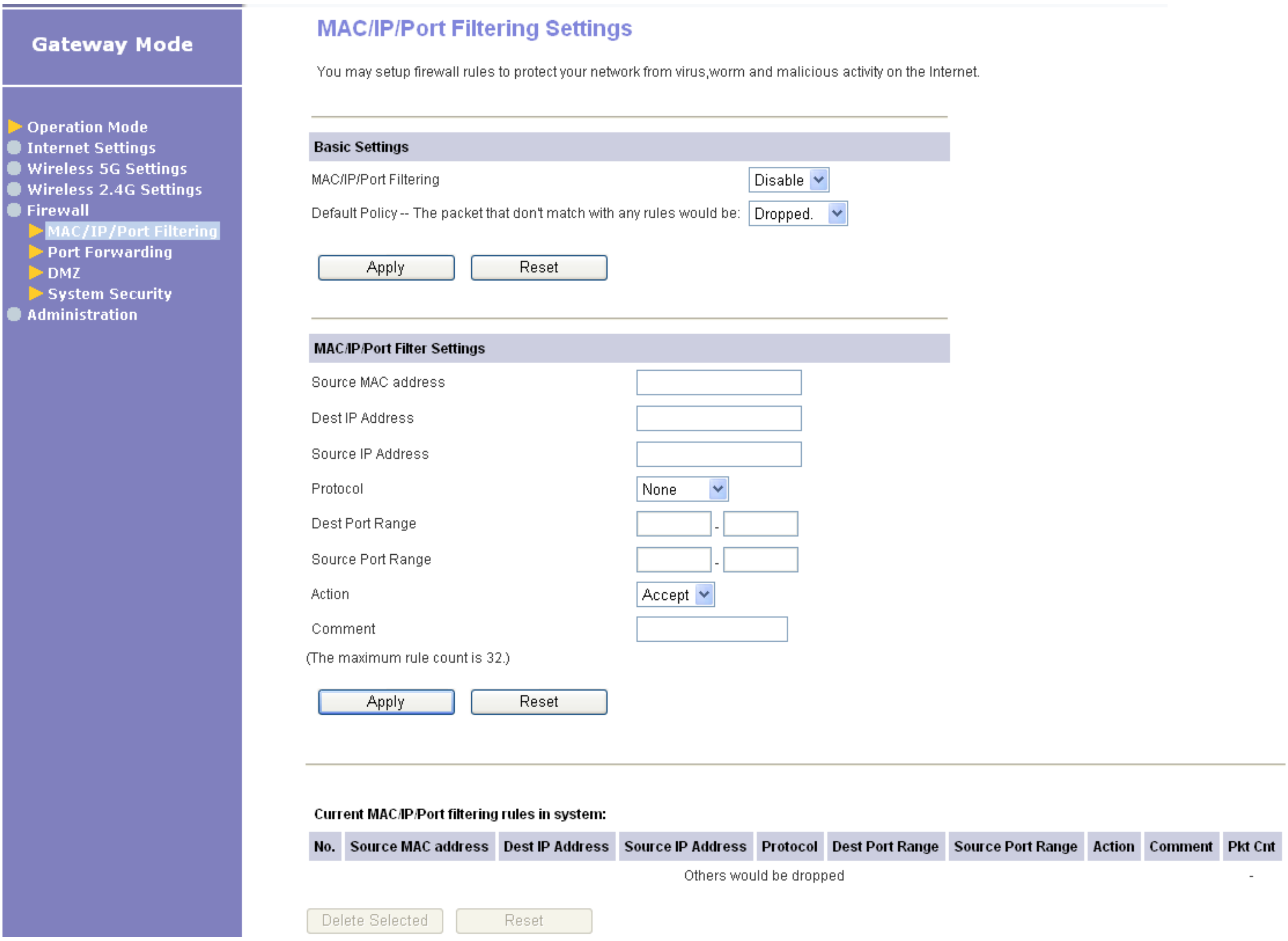
AP Wireless Statistics

Wireless TX and RX Statistics

Transmit Statistics	
Tx Success	45
Tx Retry Count	0, PER=0.0%
Tx Fail after retry	0, PLR=0.0e+00
RTS Sucessfully Receive CTS	0
RTS Fail To Receive CTS	0
Receive Statistics	
Frames Received Successfully	5746
Frames Received With CRC Error	6, PER=0.1%
SNR	
SNR	n/a, n/a, n/a

24 MAC/IP/Port Filtering Settings

The Wireless Router could filter the outgoing packets for security or management consideration. You can set up the filter against the IP addresses to block specific internal users from accessing the Internet. The firewall could not only obstruct outside intruders from intruding your system, but also restricting the LAN users. Port filter restricts certain type of data packets from your LAN to Internet through the router.



MAC/IP/Port Filtering Settings

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

Basic Settings

MAC/IP/Port Filtering: Disable

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

Apply | Reset

MAC/IP/Port Filter Settings

Source MAC address:

Dest IP Address:

Source IP Address:

Protocol: None

Dest Port Range: -

Source Port Range: -

Action: Accept

Comment:

(The maximum rule count is 32.)

Apply | Reset

Current MAC/IP/Port filtering rules in system:

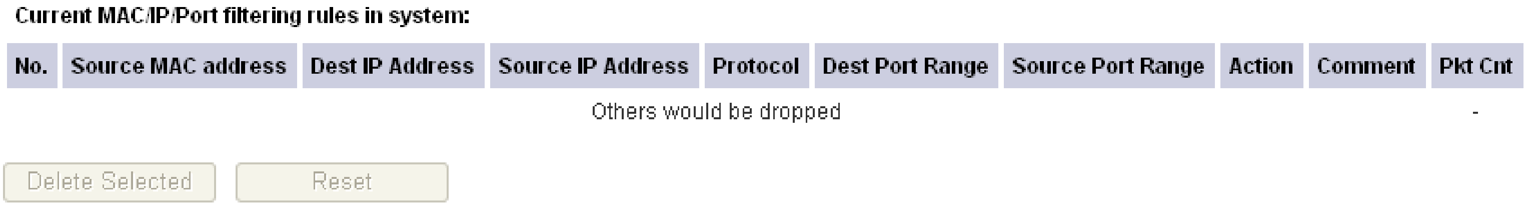
No.	Source MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
				Others would be dropped					-

Delete Selected | Reset

Basic Settings:	
Field	Description
MAC/IP/Port Filtering	**Enable/Disable the function.**
Default Policy - The packet that don't match with any rules would be	**Dropped/Accepted.**

MAC/IP/Port Filtering Settings	
Field	Description
MAC address	**Fill out the MAC address that you wish to filter.**
Dest IP Address	**Fill in the destination IP address that you wish to filter.**
Source IP Address	**Fill in the source IP address that you wish to filter.**
Protocol	**Select the protocol type of TCP, UDP or ICMP.**
Dest Port Range	**Fill in the destination port range that you wish to filter.**
Action	**Accept or Drop the action.**
Comment	**Input any text to describe this mapping, up to 16 alphanumerical characters.**

MAC / IP / Port Filter Rule List: Lists the MAC / IP / Port Filter Settings you have added before. Click on the list to change configuration, or the delete button to delete the list.

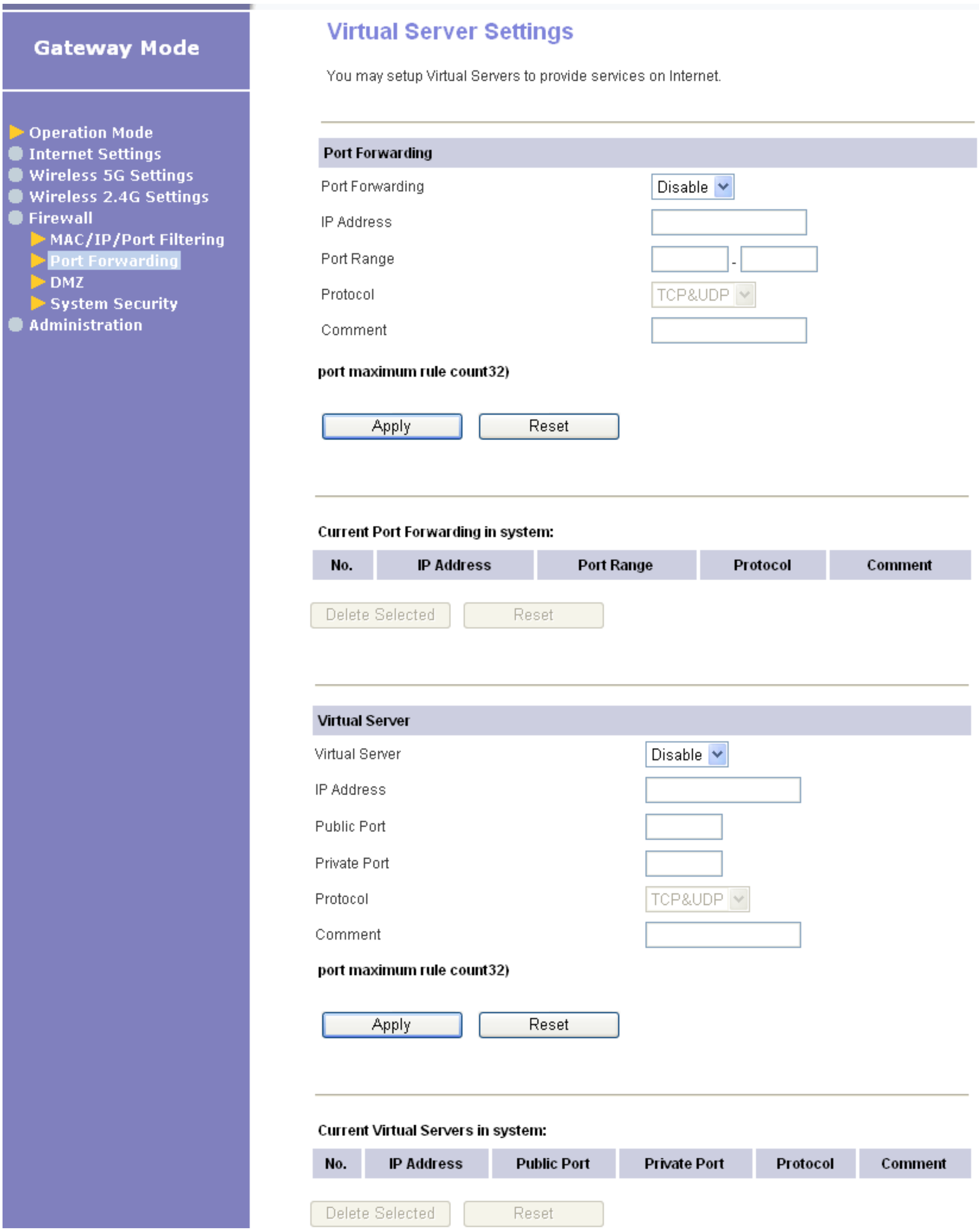


Current MAC/IP/Port filtering rules in system:

No.	Source MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be dropped									-

25 Port Forwarding Setting

Virtual Server help redirect requests from computers on the LAN to a server set up on the LAN. You can setup an Internet service on the computer on local network, without exposing it on Internet directly. You can also build many sets of port redirection, to provide many different Internet services on different local computers via a single Internet IP address.



Virtual Server Settings

You may setup Virtual Servers to provide services on Internet.

Port Forwarding	
Port Forwarding	Disable
IP Address	
Port Range	-
Protocol	TCP&UDP
Comment	

port maximum rule count32)

Current Port Forwarding in system:

No.	IP Address	Port Range	Protocol	Comment

Virtual Server	
Virtual Server	Disable
IP Address	
Public Port	
Private Port	
Protocol	TCP&UDP
Comment	

port maximum rule count32)

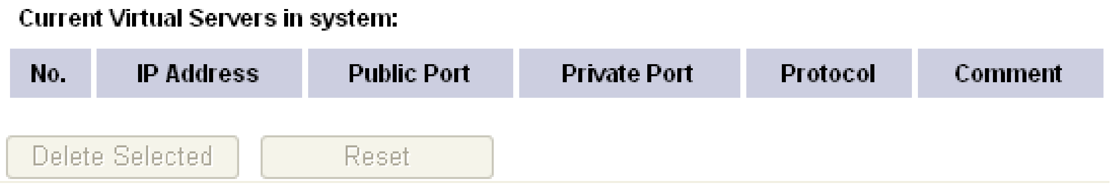
Current Virtual Servers in system:

No.	IP Address	Public Port	Private Port	Protocol	Comment

Port Forwarding	
Field	Description
Port Forwarding	**Enable/Disable.**
IP Address	**Fill in the IP of your LAN Server.**
Public Port	**Fill in the Public Port that you wish to filter.**
Private Port	**Fill in the Private Port that you wish to filter.**
Protocol	**Select the protocol type of TCP, UDP or Both.**
Comment	**Input any text to describe this mapping, up to 16 alphanumerical characters.**

Virtual Server	
Field	Description
Virtual Server	**Enable/Disable.**
IP Address	**Fill in the IP of your LAN Server.**
Port Range	**Fill in the port range that you wish to filter.**
Protocol	**Select the protocol type of TCP, UDP or Both.**
Comment	**Input any text to describe this mapping, up to 16 alphanumerical characters.**

Virtual Server Mapping List: Lists the Virtual Server Settings you have added before. Click on the list to change configuration, or the Delete button to delete the list.

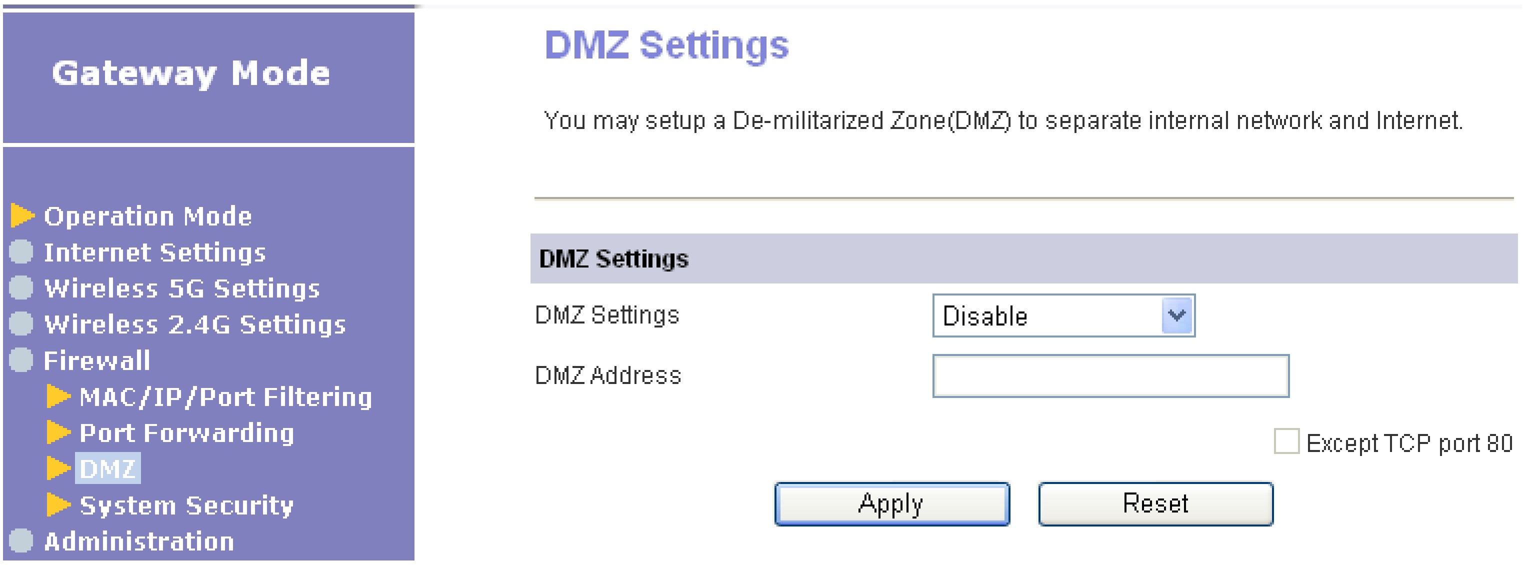


Current Virtual Servers in system:

No.	IP Address	Public Port	Private Port	Protocol	Comment

26 DMZ Settings

The virtual DMZ (Demilitarized Zone) is used to enable protocols, which need to open ports on the router. The router will forward all unspecified incoming traffic to the host specified in this page. To configure it, mark to enable virtual DMZ and then enter the Host IP (private IP address) and click **Apply** to enact the setting.



DMZ Settings

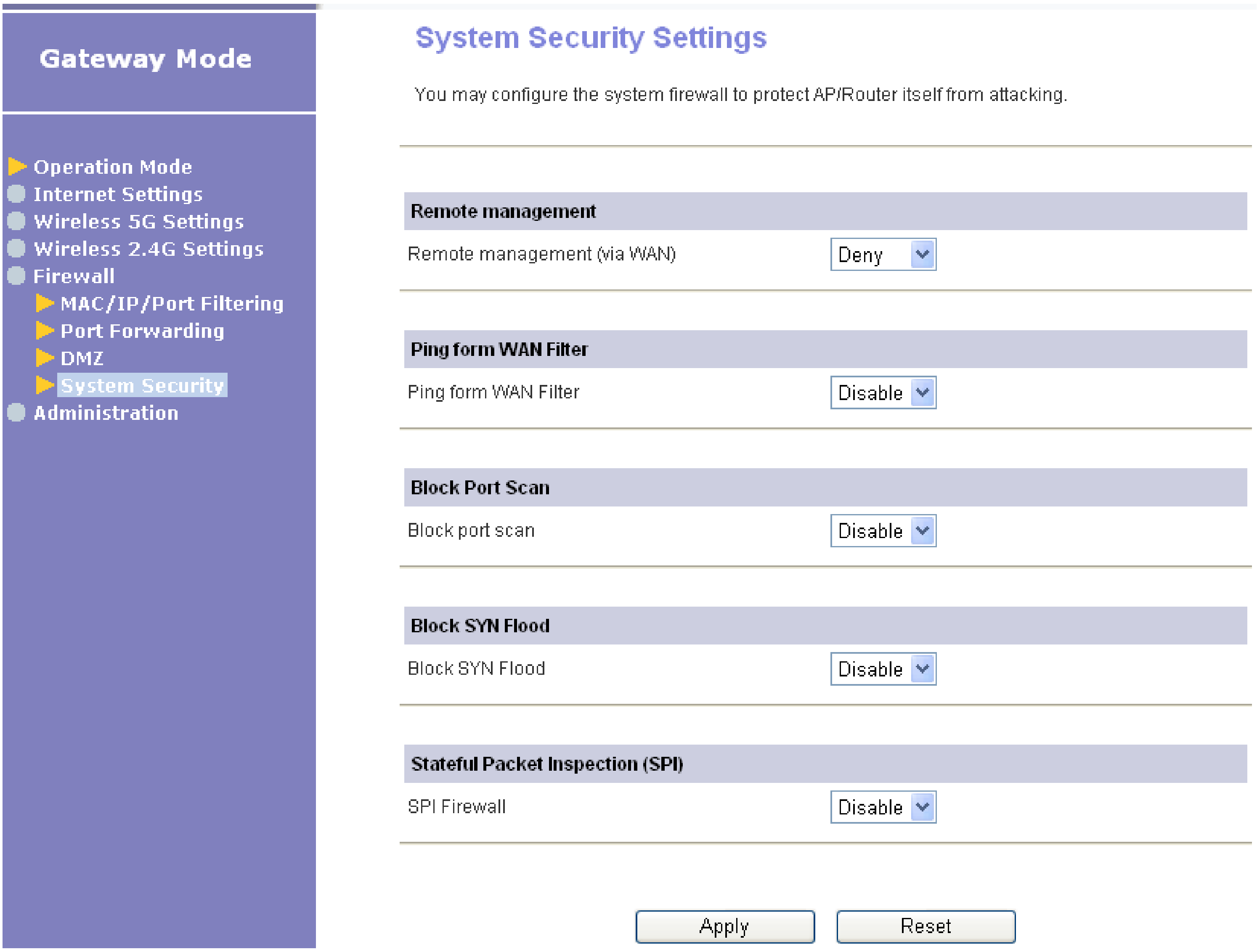
You may setup a De-militarized Zone(DMZ) to separate internal network and Internet.

DMZ Settings	
DMZ Settings	Disable
DMZ Address	

□ Except TCP port 80

27 System Security Settings

You may configure the system firewall to protect AP/Router itself from attacking.redirection, to provide many different Internet services on different local computers via a single Internet IP address.



System Security Settings

You may configure the system firewall to protect AP/Router itself from attacking.

Remote management

Remote management (via WAN): Deny

Ping form WAN Filter

Ping form WAN Filter: Disable

Block Port Scan

Block port scan: Disable

Block SYN Flood

Block SYN Flood: Disable

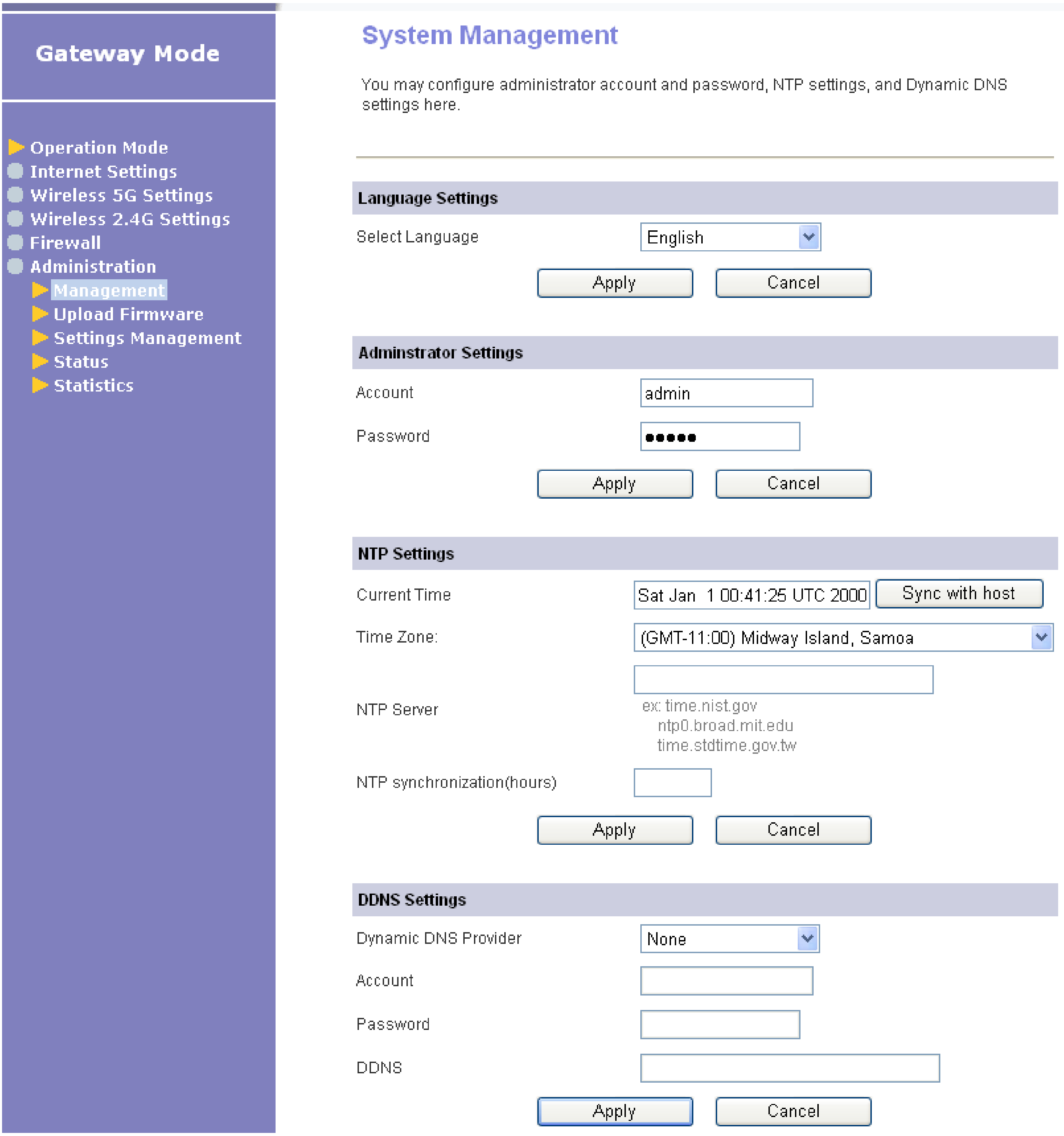
Stateful Packet Inspection (SPI)

SPI Firewall: Disable

Field	Description
Remote Management via WAN	**Allow/Deny.**
Ping from WAN filter	**Disable/Enable.**
Block Port Scan	**Disable/Enable.**
Block SYN Flood	**Disable/Enable.**
Stateful Packet Inspection (SPI)	**Disable/Enable.**

28 System Management

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



System Management

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

Language Settings

Select Language	English

Adminstrator Settings

Account	admin
Password	●●●●●

NTP Settings

Current Time	Sat Jan 1 00:41:25 UTC 2000
Time Zone:	(GMT-11:00) Midway Island, Samoa
NTP Server	ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw
NTP synchronization(hours)	

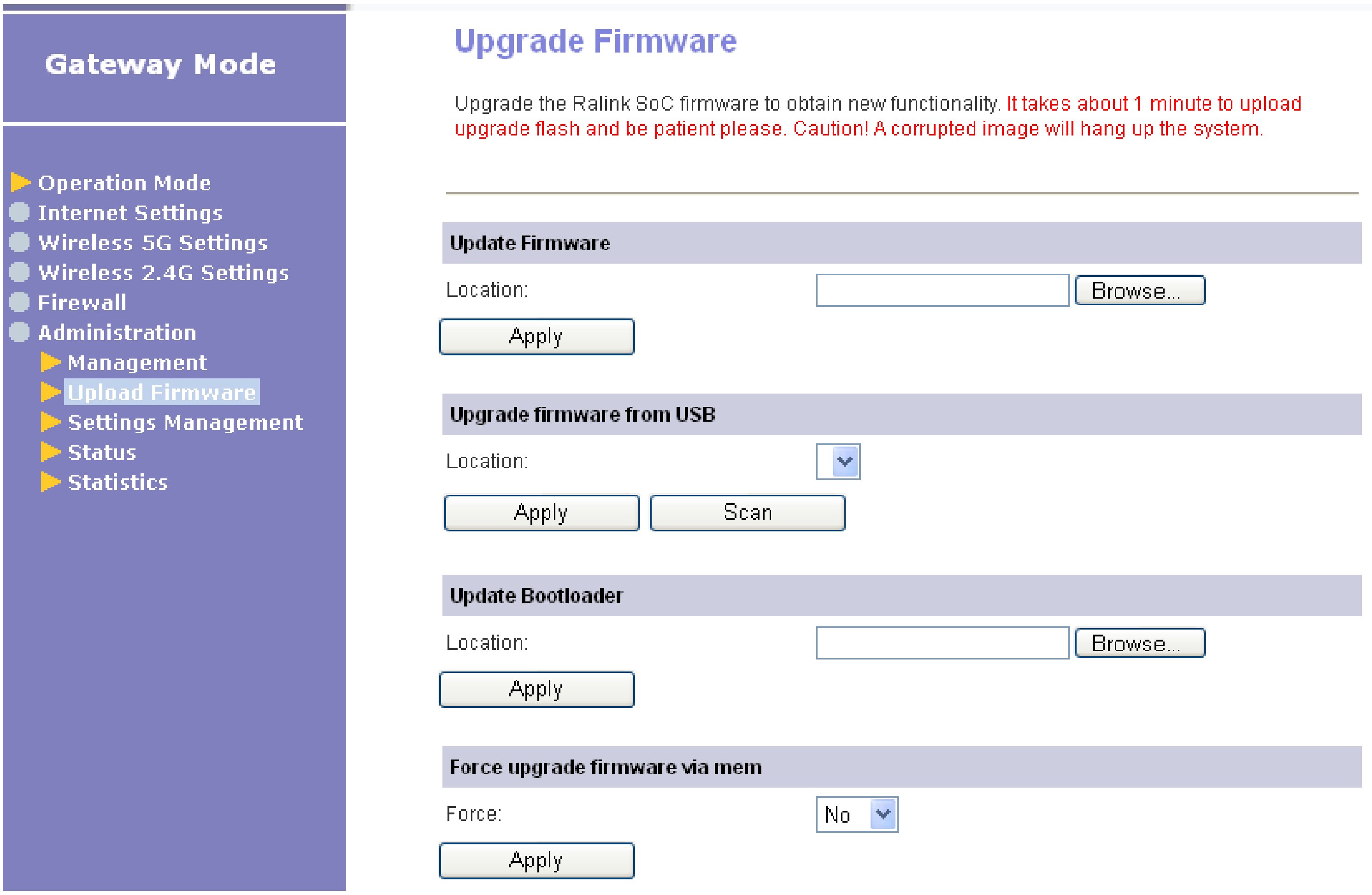
DDNS Settings

Dynamic DNS Provider	None
Account	
Password	
DDNS	

Field	Description
Language Settings	**Can select language which you want.**
Administrator Settings	**Set the account and password to set and manage the Wireless Device.**
NTP Settings	**Can set the NTP server here.**
Dynamic DNS Provider	**The website that provides DDNS service. Please select from the drop-down list.**
Account	**DDNS login account. For DynDNS users, please fill in your user name; for No-IP users, please fill in your email address.**
Password	**The password of your DDNS service account.**
DDNS	**The hostname that you have applied for the device.**

29 Upgrade Firmware

Upgrade the firmware to obtain new functionality. It takes about 1 minute to upload and upgrade flash and be patient please. Caution! A corrupted image will hang up the system.



Upgrade Firmware

Upgrade the Ralink SoC firmware to obtain new functionality. It takes about 1 minute to upload upgrade flash and be patient please. Caution! A corrupted image will hang up the system.

Update Firmware

Location: Browse...

Apply

Upgrade firmware from USB

Location:

Apply Scan

Update Bootloader

Location: Browse...

Apply

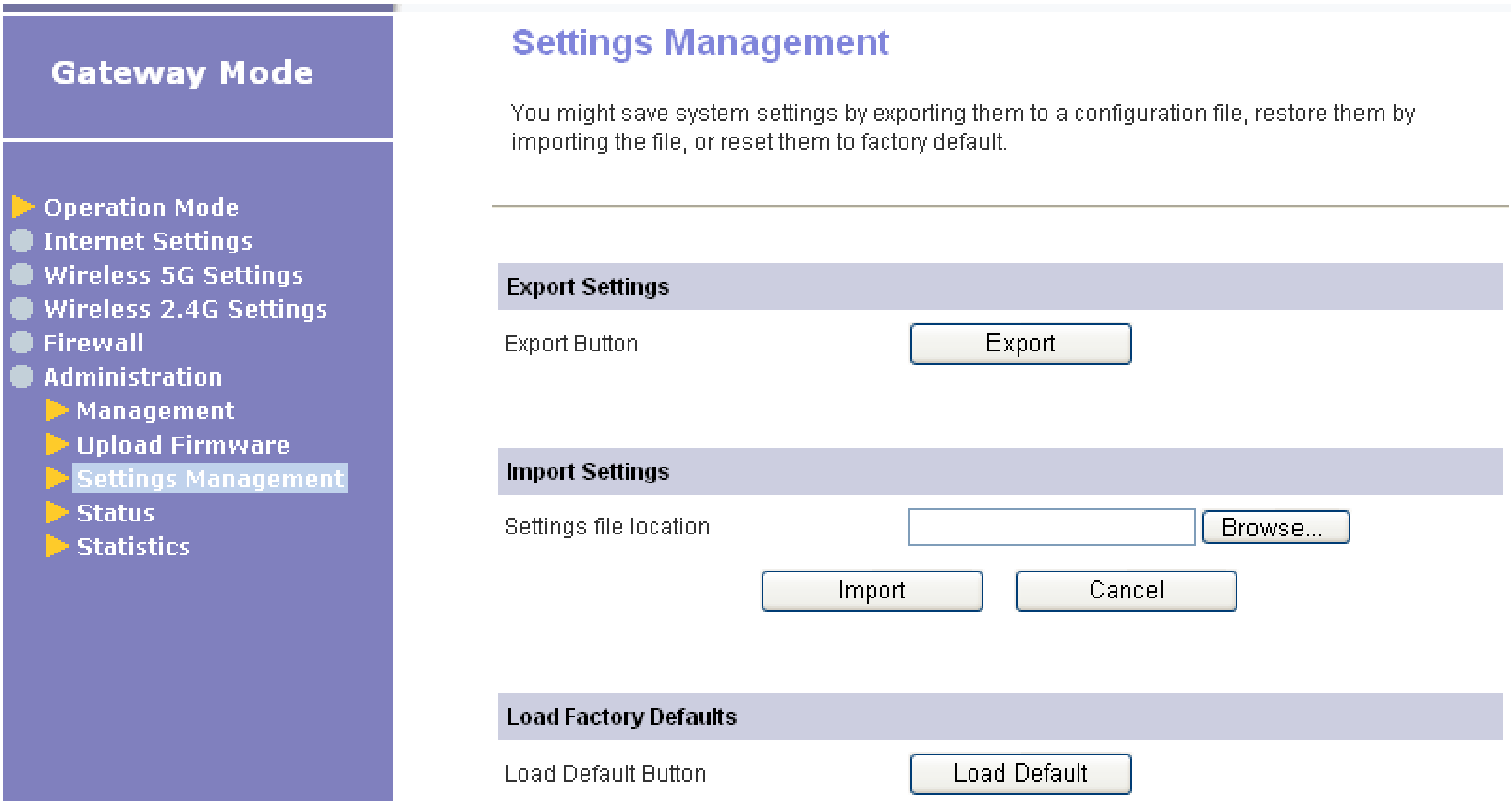
Force upgrade firmware via mem

Force: No

Apply

30 Settings Management

You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.



Settings Management

You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.

Export Settings

Export Button [Export]

Import Settings

Settings file location [ ] [Browse...]

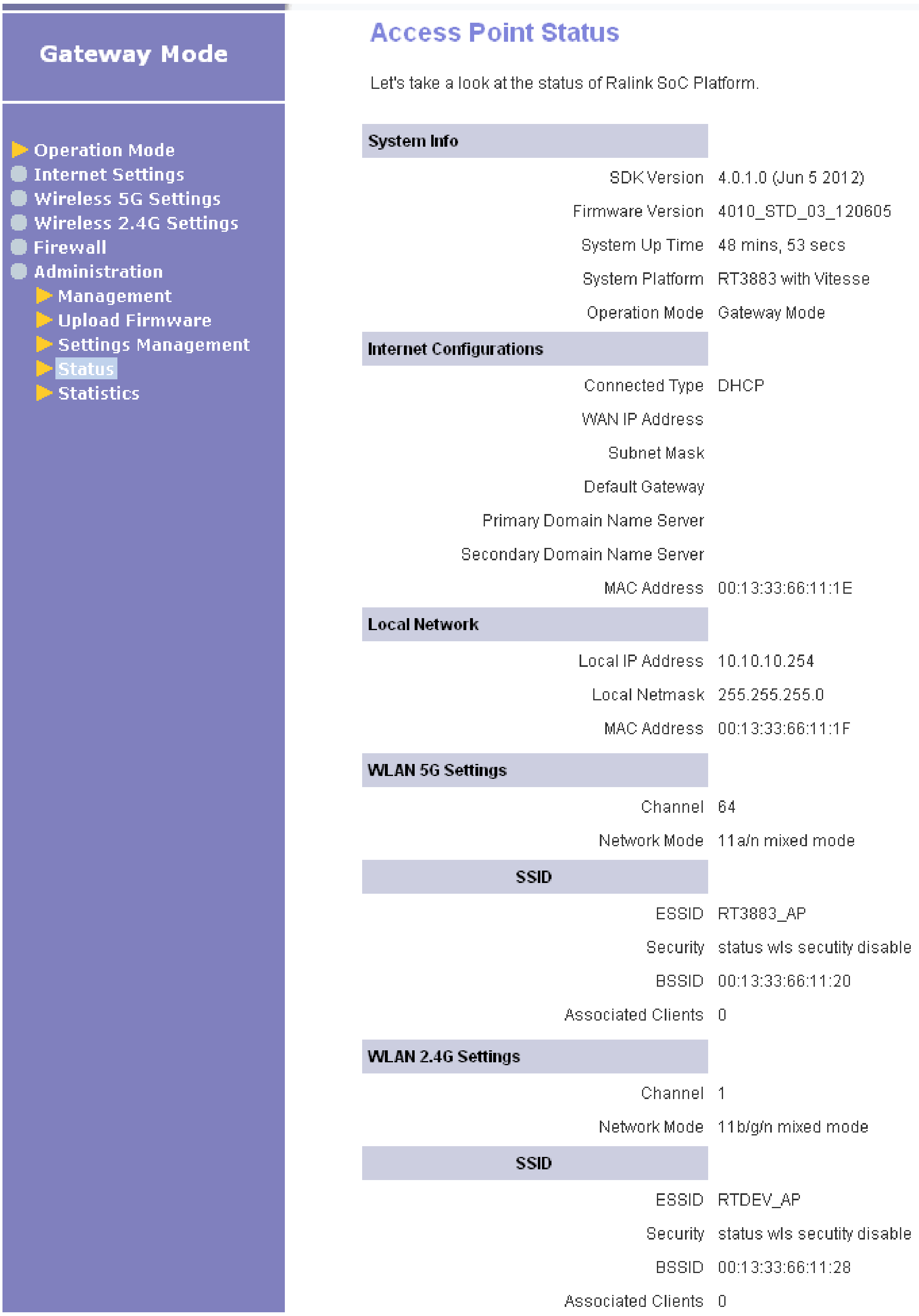
[Import] [Cancel]

Load Factory Defaults

Load Default Button [Load Default]

31 Access Point Status

You can check the device status in this page, System Info, Internet Configuration and LAN settings.



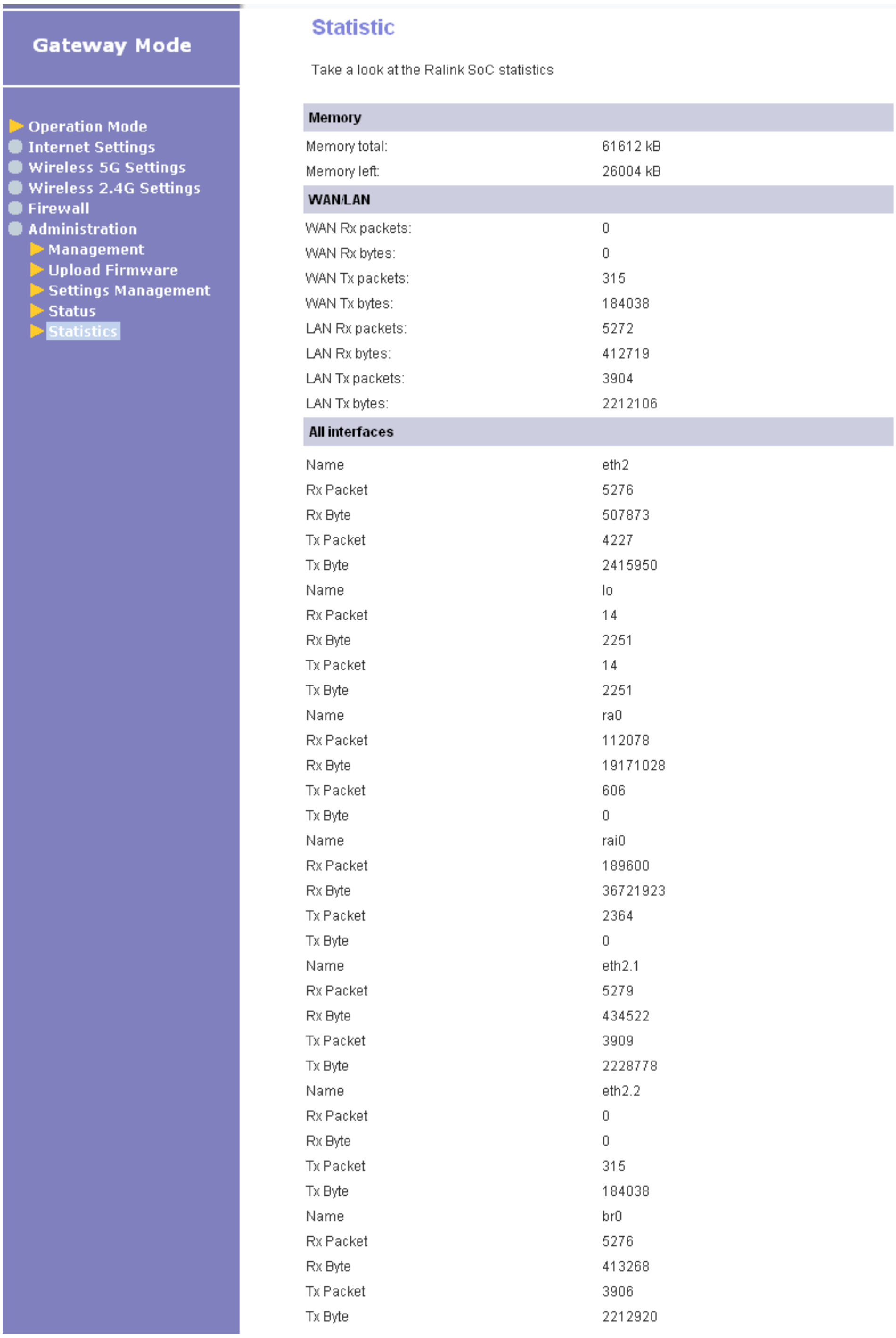
Access Point Status

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

System Info	
SDK Version	4.0.1.0 (Jun 5 2012)
Firmware Version	4010_STD_03_120605
System Up Time	48 mins, 53 secs
System Platform	RT3883 with Vitesse
Operation Mode	Gateway Mode
Internet Configurations	
Connected Type	DHCP
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	
Secondary Domain Name Server	
MAC Address	00:13:33:66:11:1E
Local Network	
Local IP Address	10.10.10.254
Local Netmask	255.255.255.0
MAC Address	00:13:33:66:11:1F
WLAN 5G Settings	
Channel	64
Network Mode	11a/n mixed mode
SSID	
ESSID	RT3883_AP
Security	status wls secutity disable
BSSID	00:13:33:66:11:20
Associated Clients	0
WLAN 2.4G Settings	
Channel	1
Network Mode	11b/g/n mixed mode
SSID	
ESSID	RTDEV_AP
Security	status wls secutity disable
BSSID	00:13:33:66:11:28
Associated Clients	0

32 Statistic

This page allows users to get information of data transferring condition, and monitor the status and performance of this router including interface, receiving/sending packets, and receiving/sending errors.



Statistic

Take a look at the Ralink SoC statistics

Memory	
Memory total:	61612 kB
Memory left:	26004 kB

WAN/LAN	
WAN Rx packets:	0
WAN Rx bytes:	0
WAN Tx packets:	315
WAN Tx bytes:	184038
LAN Rx packets:	5272
LAN Rx bytes:	412719
LAN Tx packets:	3904
LAN Tx bytes:	2212106

All interfaces	
Name	eth2
Rx Packet	5276
Rx Byte	507873
Tx Packet	4227
Tx Byte	2415950
Name	lo
Rx Packet	14
Rx Byte	2251
Tx Packet	14
Tx Byte	2251
Name	ra0
Rx Packet	112078
Rx Byte	19171028
Tx Packet	606
Tx Byte	0
Name	rai0
Rx Packet	189600
Rx Byte	36721923
Tx Packet	2364
Tx Byte	0
Name	eth2.1
Rx Packet	5279
Rx Byte	434522
Tx Packet	3909
Tx Byte	2228778
Name	eth2.2
Rx Packet	0
Rx Byte	0
Tx Packet	315
Tx Byte	184038
Name	br0
Rx Packet	5276
Rx Byte	413268
Tx Packet	3906
Tx Byte	2212920

A Configuring your Computers

This appendix provides instructions for configuring the Internet settings on your computers to work with the Wireless Gateway.

Configuring Ethernet PCs

Before you begin

By default, the Wireless Gateway automatically assigns the required Internet settings to your PCs. You need to configure the PCs to accept this information when it is assigned.

Note

In some cases, you may want to assign Internet information manually to some or all of your computers rather than allow the Wireless Gateway to do so. See *Assigning static Internet information to your PCs* for instructions.

- If you have connected your LAN PCs via Ethernet to the Wireless Gateway, follow the instructions that correspond to the operating system installed on your PC:
  - Windows® XP PCs
  - Windows 2000 PCs
  - Windows Me PCs
  - Windows 95, 98 PCs
  - Windows NT 4.0 workstations

Windows® XP PCs

1. In the Windows task bar, click the *Start* button, and then click *Control Panel*.
2. Double-click the Network Connections icon.
3. In the *LAN or High-Speed Internet* window, right-click on the icon corresponding to your network interface card (NIC) and select *Properties*. (Often, this icon is labeled *Local Area Connection*).

   The *Local Area Connection* dialog box is displayed with a list of currently installed network items.
4. Ensure that the check box to the left of the item labeled *Internet Protocol TCP/IP* is checked and click *Properties*.
5. In the *Internet Protocol (TCP/IP) Properties* dialog box, click the radio button labeled *Obtain an IP address automatically*. Also click the radio button labeled *Obtain DNS server address automatically*.
6. Click *OK* twice to confirm your changes, and then close the Control Panel.

Windows 2000 PCs

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
2. Double-click the Network and Dial-up Connections icon.

3. In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*.

   The *Local Area Connection Properties* dialog box is displayed with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.

4. If Internet Protocol (TCP/IP) does not display as an installed component, click *Install…*
5. In the *Select Network Component* Type dialog box, select *Protocol*, and then click *Add…*
6. Select *Internet Protocol (TCP/IP)* in the Network Protocols list, and then click *OK*.

   You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.

7. If prompted, click *OK* to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the Wireless Gateway:

8. In the *Control Panel*, double-click the Network and Dial-up Connections icon.
9. In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*.
10. In the Local Area Connection Properties dialog box, select *Internet Protocol (TCP/IP),* and then click *Properties*.
11. In the *Internet Protocol (TCP/IP) Properties* dialog box, click the radio button labeled *Obtain an IP address automatically.* Also click the radio button labeled *Obtain DNS server address automatically*.
12. Click *OK* twice to confirm and save your changes, and then close the Control Panel.

Windows Me PCs

1. In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
2. Double-click the Network and Dial-up Connections icon.
3. In the *Network and Dial-up Connections* window, right-click the Network icon, and then select *Properties*.

   The *Network Properties* dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 11.

4. If Internet Protocol (TCP/IP) does not display as an installed component, click *Add…*
5. In the *Select Network Component Type* dialog box, select *Protocol*, and then click *Add…*
6. Select *Microsoft* in the Manufacturers box.
7. Select *Internet Protocol (TCP/IP)* in the Network Protocols list, and then click *OK*.

   You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.

8. If prompted, click *OK* to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the Wireless Gateway:

9. In the *Control Panel*, double-click the Network and Dial-up Connections icon.
10. In *Network and Dial-up Connections window*, right-click the Network icon, and then select *Properties*.
11. In the *Network Properties* dialog box, select *TCP/IP*, and then click *Properties*.
12. In the TCP/IP Settings dialog box, click the radio button labeled **Server** *assigned IP address*. Also click the radio button labeled *Server assigned name server address*.
13. Click *OK* twice to confirm and save your changes, and then close the *Control Panel*.

Windows 95, 98 PCs

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
2. Double-click the Network icon.

   The *Network* dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 9.

3. If TCP/IP does not display as an installed component, click *Add…*

   The *Select Network Component Type* dialog box displays.

4. Select *Protocol*, and then click *Add…*

   The Select Network Protocol dialog box displays.

5. Click on *Microsoft* in the Manufacturers list box, and then click *TCP/IP* in the Network Protocols list box.
6. Click *OK* to return to the Network dialog box, and then click *OK* again.

   You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.

7. Click *OK* to restart the PC and complete the TCP/IP installation.

Next, configure the PCs to accept IP information assigned by the Wireless Gateway:

8. Open the Control Panel window, and then click the Network icon.
9. Select the network component labeled TCP/IP, and then click *Properties*.

   If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.

10. In the TCP/IP Properties dialog box, click the IP Address tab.
11. Click the radio button labeled *Obtain an IP address automatically*.
12. Click the DNS Configuration tab, and then click the radio button labeled *Obtain an IP address automatically*.
13. Click *OK* twice to confirm and save your changes.

    You will be prompted to restart Windows.

14. Click *Yes*.

Windows NT 4.0 workstations

First, check for the IP protocol and, if necessary, install it:

1. In the Windows NT task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
2. In the Control Panel window, double click the Network icon.
3. In the *Network dialog* box, click the *Protocols* tab.

   The *Protocols* tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to step 9.

4. If TCP/IP does not display as an installed component, click *Add…*
5. In the *Select Network Protocol* dialog box, select *TCP/IP*, and then click *OK*.

   You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.

   After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.

6. Click *Yes* to continue, and then click *OK* if prompted to restart your computer.

Next, configure the PCs to accept IP information assigned by the Wireless Gateway:

7. Open the Control Panel window, and then double-click the Network icon.
8. In the *Network* dialog box, click the *Protocols* tab.
9. In the *Protocols* tab, select *TCP/IP*, and then click *Properties*.
10. In the *Microsoft TCP/IP Properties* dialog box, click the radio button labeled *Obtain an IP address from a DHCP server.*
11. Click *OK* twice to confirm and save your changes, and then close the Control Panel.

Assigning static Internet information to your PCs

If you are a typical user, you will not need to assign static Internet information to your LAN PCs because your ISP automatically assigns this information for you.

In some cases however, you may want to assign Internet information to some or all of your PCs directly (often called "statically"), rather than allowing the Wireless Gateway to assign it. This option may be desirable (but not required) if:

- You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).
- You maintain different subnets on your LAN (subnets are described in Appendix B).

Before you begin, you must have the following information available:

- The IP address and subnet mask of each PC
- The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the Wireless Gateway. By default, the LAN port is assigned the IP address *10.10.10.2*. (You can change this number or another number can be assigned by your ISP. See *Addressing* for more information.)
- The IP address of your ISP's Domain Name System (DNS) server.

On each PC to which you want to assign static information, follow the instructions relating only to checking for and/or installing the IP protocol. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server and default gateway, click the radio buttons that enable you to enter the information manually.

Note

Your PCs must have IP addresses that place them in the same subnet as the Wireless Gateway's LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in Addressing to change the LAN port IP address accordingly.

B IP Addresses, Network Masks, and Subnets

IP Addresses

Note

This section refers only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.

This section assumes basic knowledge of binary numbers, bits, and bytes.

IP addresses, the Internet's version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called *dotted decimal notation*. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

Structure of an IP address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group.

Similarly, IP addresses contain two kinds of information:

- *Network ID*
  Identifies a particular network within the Internet or intranet
- *Host ID*
  Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's *class* (see following section). The table below shows the structure of an IP address.

	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)
Class B: 129.88.16.49 (network = 129.88, host = 16.49)
Class C: 192.60.201.11 (network = 192.60.201, host = 11)

Network classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Class B networks are smaller but still quite large, each able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Some important notes regarding IP addresses:

- The class can be determined easily from field1:

field1 = 1-126:	Class A
field1 = 128-191:	Class B
field1 = 192-223:	Class C

  (field1 values not shown are reserved for special uses)
- A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

Subnet masks

Definition
mask

A mask *looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: bits set to 1 mean "this bit is part of the network ID" and bits set to 0 mean "this bit is part of the host ID."*

Subnet masks are used to define *subnets* (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask:

255.255.255.128

It's easier to see what's happening if we write this in binary:

11111111. 11111111. 11111111.10000000

As with any class C address, all of the bits in field1 through field3 are part of the network ID, but note how the mask specifies that the first bit in field4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field4 for its host IDs, which range from 1 to 126 hosts (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111. 11111111.
11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 1 to 62.

Note

Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask*. These masks are:*

Class A:	*255.0.0.0*
Class B:	*255.255.0.0*
Class C:	*255.255.255.0*

These are called default *because they are used when a network is initially configured, at which time it has no subnets.*

C UPnP Control Point Software on Windows ME/XP

This appendix provides instructions for configuring the UPnP on your computers to work with the Wireless Gateway.

UPnP is an architecture for pervasive peer-to-peer network connectivity of intelligent appliances, Wireless devices, and PCs of all form factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public spaces, or attached to the Internet. UPnP is a distributed, open networking architecture that leverages TCP/IP and the Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and public spaces.

UPnP is more than just a simple extension of the plug and play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors. This means a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS servers are optional and are used only if available on the network. Finally, a device can leave a network smoothly and automatically without leaving any unwanted state behind.

UPnP Control Point Software on Windows ME

To install the control point software on Windows ME:

1. In the Control Panel, select "Add/Remove Programs".

2. In the "Add/Remove Programs Properties" dialog box, select the "Windows Setup" tab. In the "Components" list, double click on the "Communications" entry.

3. In the "Communications" dialog box, scroll down the "Components" list to display the UPnP entry. Select the entry, click "OK".

4. Click "OK" to finish the "Add/Remove Programs" dialog.

5. Reboot your system.

Once you have installed the UPnP software and you have rebooted (and your network includes the IGD system), you should be able to see the IGD controlled device on your network.

UPnP Control Point Software on Windows XP with Firewall

On Windows XP versions earlier than SP2, Firewall support is provided by the Windows XP Internet Connection Firewall. You cannot use the Windows XP Internet Connection Firewall support on a system that you intend to use as a UPnP control point. If this feature is enabled, although the control point system may display controlled devices in the list of network devices, the control point system cannot participate in UPnP communication. (This restriction also applies to controlled devices running on Windows XP systems earlier than SP2.)

On Windows XP SP2 and later, Firewall support is provided by Windows Firewall. Unlike earlier versions, Windows XP SP2 can be used on a system that you intend to use as a UPnP control point.

To turn off the Firewall capability on any version of Windows XP, follow the steps below:

1. In the Control Panel, select "Network and Internet Connections".

2. In the "Network and Internet Connections" dialog box, select "Network Connections".

3. In the "Network Connections" dialog box, right-click on the local area connection entry for your network; this will display a menu. Select the "Properties" menu entry.

4. In the "Local Area Connection Properties" dialog box, select the "Advanced" tab. Disable the Internet Connection Firewall by de-selecting the entry with the following label:

"Protect my computer and network by limiting or preventing access to the computer from the Internet".

5. Click "OK".

SSDP requirements

You must have SSDP Discovery Service enabled on your Windows XP system to use the UPnP Control point software.

SSDP Discovery Service is enabled on a default installation of Windows XP. To check if it is enabled on your system, look in Control Panel > Administrative Tools > Services).

Installation procedure

To install the Control point software on Windows XP, follow the steps below:

1. In the Control Panel, select "Add/Remove Programs".

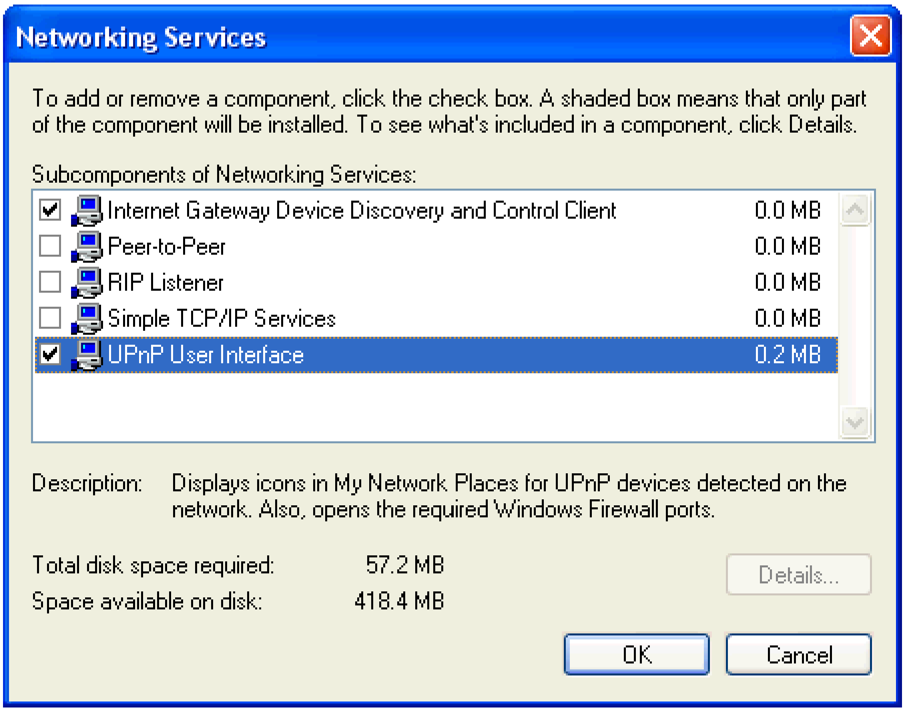
2. In the "Add or Remove Programs" dialog box, click the "Add / Remove Windows Components" button.

3. In the "Windows Component Wizard" dialog box, scroll down the list to display the "Networking Services" entry. Highlight (select) the entry, and click on the "Details" button.

4. The “Networking Services” window is displayed.

The subcomponents shown in the Networking Services window will be different depending on if you are using Windows XP, Windows XP (SP1), or Windows XP (SP2).

If you are using Windows XP SP2, the Networking Services window will display the following list of sub-components:



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

☑	Internet Gateway Device Discovery and Control Client	0.0 MB
☐	Peer-to-Peer	0.0 MB
☐	RIP Listener	0.0 MB
☐	Simple TCP/IP Services	0.0 MB
☑	UPnP User Interface	0.2 MB

Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.

Total disk space required: 57.2 MB

Space available on disk: 418.4 MB

5. Select the following entries from the “Networking Services” window and then click "OK":

If you are using **Windows XP**, select:

- "Universal Plug and Play".

If you are using **Windows XP SP1**, select:

- "Internet Gateway Device discovery and Control Client".
- "Universal Plug and Play".

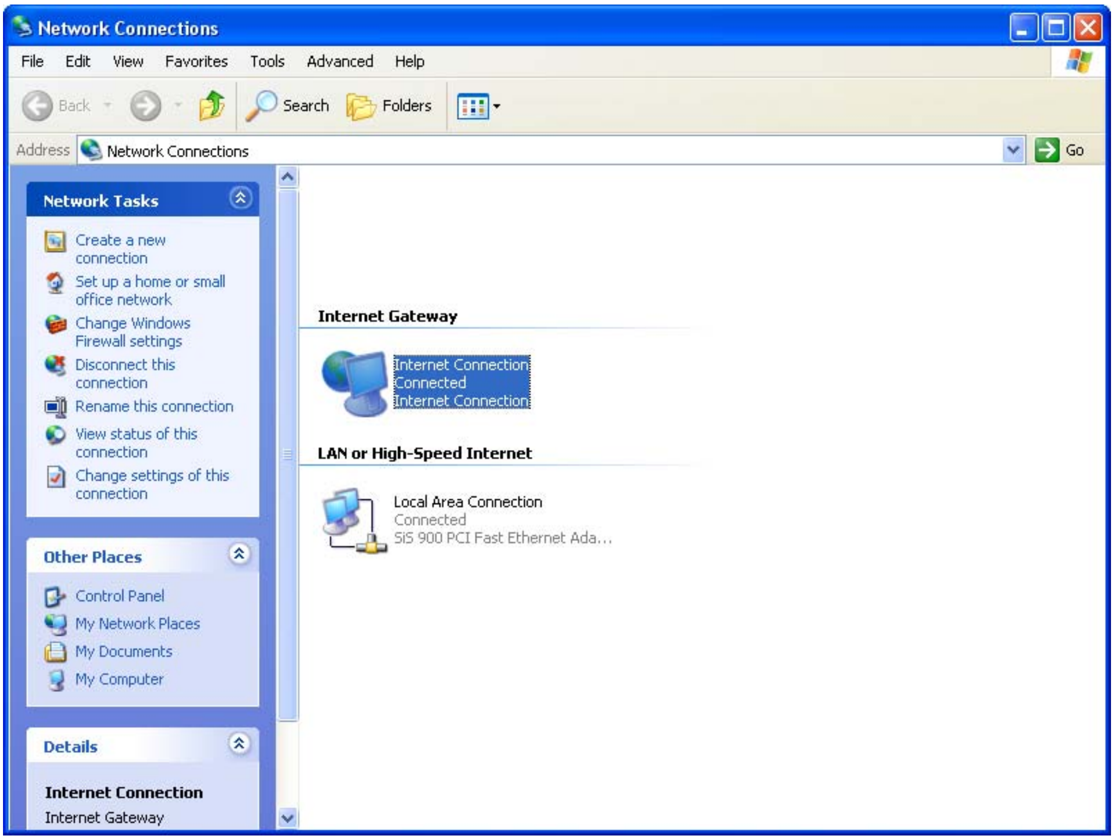
If you are using **Windows XP SP2**, select:

- "Internet Gateway Device discovery and Control Client".
- "UPnP User Interface".

6. Reboot your system.

Once you have installed the UPnP software and you have rebooted (and your network includes the IGD system), you should be able to see the IGD controlled device on your network.

For example, from the Network Connections window you should see the Internet Gateway Device:



Internet Connection
Internet Gateway

Internet Gateway

Internet Connection
Connected
Internet Connection

LAN or High-Speed Internet

Local Area Connection
Connected
SiS 900 PCI Fast Ethernet Ada...

D Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the Wireless Gateway, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

Troubleshooting Suggestions

Problem	Troubleshooting Suggestion
LEDs	
Power LED does not illuminate after product is turned on.	Verify that you are using the power cable provided with the device and that it is securely connected to the Wireless Gateway and a wall socket/power strip.
LINK LAN LED does not illuminate after Ethernet cable is attached.	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the Wireless Gateway. Make sure the PC and/or hub is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled CAT 5. A 10Mbit/sec network may tolerate lower quality cables.
Internet Access	
My PC cannot access the Internet	Use the ping utility (discussed in the following section) to check whether your PC can communicate with the device's LAN IP address (by default 10.10.10.2). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: • Check that the gateway IP address on the computer is your public IP address (see Current Status for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically. • Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically.
My LAN PCs cannot display web pages on the Internet.	Verify that the DNS server IP address specified on the PCs is correct for your ISP, as discussed in the item above. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the Wireless Gateway is correct, then You can use the ping utility, to test connectivity with your ISP's DNS server.
Web pages	

Problem	Troubleshooting Suggestion
I forgot/lost my user ID or password.	If you have not changed the password from the default, try using "admin" the user ID and "admin " as password. Otherwise, you can reset the device to the default configuration by pressing the Reset Default button on the Rare panel of the device (see *Rare Panel*). Then, type the default User ID and password shown above. **WARNING:** Resetting the device removes any custom settings and returns all settings to their default values.
I cannot access the web pages from my browser.	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the device's LAN IP address (by default 10.10.10.2). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer or Netscape Navigator v4.0 or later. Verify that the PC's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the Wireless Gateway.
My changes to the web pages are not being retained.	Be sure to use the *Confirm Changes/Apply* function after any changes.

Diagnosing Problem using IP Utilities

ping

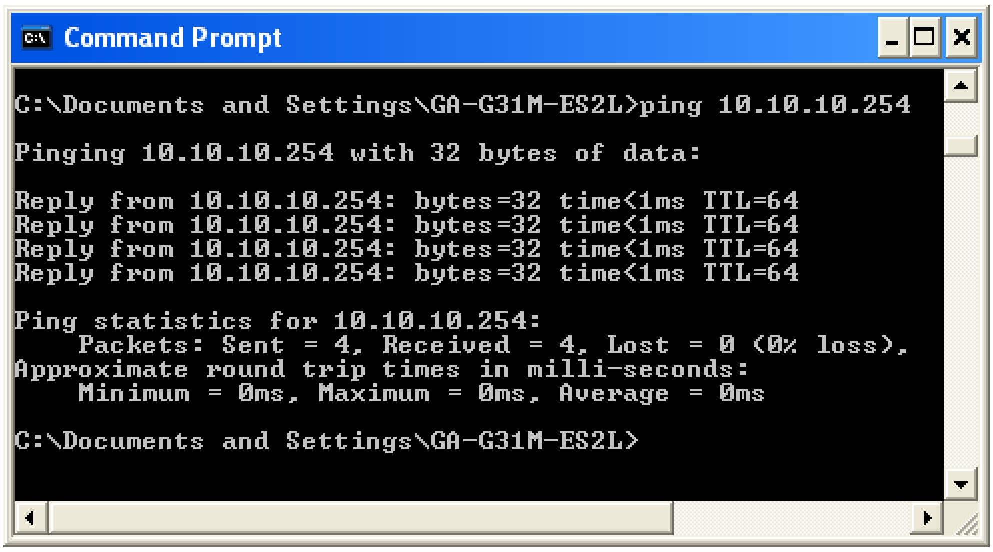
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

On Windows-based computers, you can execute a ping command from the Start menu. Click the *Start* button, and then click *Run*. In the *Open* text box, type a statement such as the following:

ping 10.10.10.254

Click *OK*. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the message, a *Command Prompt* window is displayed:



```
C:\Documents and Settings\GA-G31M-ES2L>ping 10.10.10.254

Pinging 10.10.10.254 with 32 bytes of data:

Reply from 10.10.10.254: bytes=32 time<1ms TTL=64
Reply from 10.10.10.254: bytes=32 time<1ms TTL=64
Reply from 10.10.10.254: bytes=32 time<1ms TTL=64
Reply from 10.10.10.254: bytes=32 time<1ms TTL=64

Ping statistics for 10.10.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\GA-G31M-ES2L>
```

Figure 7: Using the ping Utility

If the target computer cannot be located, you will receive the message *Request timed out*.

Using the ping command, you can test whether the path to the Wireless Gateway is working (using the preconfigured default LAN IP address 10.10.10.2) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for *www.yahoo.com* (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the *nslookup* command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

nslookup

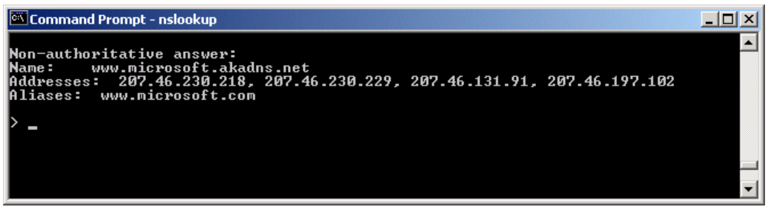
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP’s DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the nslookup command from the *Start* menu. Click the *Start* button, and then click *Run*. In the *Open* text box, type the following:

Nslookup

Click *OK*. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the Internet address that you are interested in, such as *www.microsoft.com*.

The window will display the associate IP address, if known, as shown below:



```
Non-authoritative answer:
Name:    www.microsoft.akadns.net
Addresses:  207.46.230.218, 207.46.230.229, 207.46.131.91, 207.46.197.102
Aliases:  www.microsoft.com

> _
```

Figure 8: Using the nslookup Utility

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the nslookup utility, type **exit** and press **[Enter]** at the command prompt.

E Glossary

10BASE-T

A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See *data rate, Ethernet*.

100BASE-T

A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See *data rate, Ethernet*.

ADSL

Asymmetric Digital Subscriber Line
The most commonly deployed "flavor" of DSL for home users is asymmetrical DSL. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.

analog

An analog signal is a signal that has had its frequency modified in some way, such as by amplifying its strength or varying its frequency, in order to add information to the signal. The voice component in DSL is an analog signal. See *digital*.

ATM

Asynchronous Transfer Mode
A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. See *data rate*.

authenticate

To verify a user's identity, such as by prompting for a password.

binary

The "base two" system of numbers, that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See *bit, IP address, network mask*.

bit

Short for "binary digit," a bit is a number that can have two values, 0 or 1. See *binary*.

bps

bits per second

bridging

Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing, which can add more intelligence to data transfers by using network addresses instead. The Wireless Gateway can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See *routing*.

broadband

A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.

broadcast

To send data to all computers on a network.

DHCP

Dynamic Host Configuration Protocol
DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.

DHCP relay

Dynamic Host Configuration Protocol relay
A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the Wireless Gateway's interfaces can be configured as a DHCP relay. See *DHCP*.

DHCP server

Dynamic Host Configuration Protocol server
A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See *DHCP*.

digital

Of data, having a form based on discrete values expressed as binary numbers (0's and 1's). The data component in DSL is a digital signal. See *analog*.

DNS

Domain Name System
The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, *www.yahoo.com* is the domain name associated with IP address 216.115.108.243. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See *domain name.*

domain name

A domain name is a user-friendly name used in place of its associated IP address. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site. See *DNS.*

download

To transfer data in the downstream direction, i.e., from the Internet to the user.

DSL

Digital Subscriber Line
A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.

encryption keys

See *network keys*

Ethernet

The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. *See also 10BASE-T, 100BASE-T, twisted pair*.

FTP

File Transfer Protocol
A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.

Gbps

Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.

host

A device (usually a computer) connected to a network.

HTTP

Hyper-Text Transfer Protocol
HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See *web browser, web site*.

Hub

A hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more directions. It connects an Ethernet bridge/router to a group of PCs on a LAN and allows communication to pass between the networked devices.

ICMP

Internet Control Message Protocol
An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.

IEEE

The Institute of Electrical and Electronics Engineers is a technical professional society that fosters the development of standards that often become national and international standards.

Internet

The global collection of interconnected networks used for both private and business communications.

intranet

A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.

IP

See TCP/IP.

IP address

Internet Protocol address
The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a *network ID* that identifies the particular network the host belongs to, and a *host ID* uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See *domain name, network mask*.

ISP

Internet Service Provider
A company that provides Internet access to its customers, usually for a fee.

LAN

Local Area Network
A network limited to a small geographic area, such as a home or small office.

LED

Light Emitting Diode
An electronic light-emitting device. The indicator lights on the front of the Wireless Gateway are LEDs.

MAC address

Media Access Control address
The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of hex characters, with each pair separated by colons. For example; *NN:NN:NN:NN:NN:NN*.

mask

See network mask.

Mbps

Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.

NAT

Network Address Translation
A service performed by many routers that translates your network's publicly known IP address into a *private* IP address for each computer on your LAN. Only your router and your

LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.

network

A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a *LAN*, or very large, such as the *Internet*.

network mask

A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See *binary, IP address, subnet*.

NIC

Network Interface Card
An adapter card that plugs into your computer and provides the physical interface to your network cabling. For Ethernet NICs this is typically an RJ-45 connector. See *Ethernet, RJ-45*.

packet

Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).

ping

Packet Internet (or Inter-Network) Groper
A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.

port

A physical access point to a device such as a computer or router, through which data flows into and out of the device.

PPP

Point-to-Point Protocol
A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the Wireless Gateway uses two forms of PPP called PPPoA and PPPoE. See *PPPoA, PPPoE*.

PPPoA

Point-to-Point Protocol over ATM
One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.

PPPoE

Point-to-Point Protocol over Ethernet
One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.

protocol

A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.

remote

In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.

RIP

Routing Information Protocol
The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.

RJ-11

Registered Jack Standard-11
The standard plug used to connect telephones, fax

machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.

RJ-45

Registered Jack Standard-45
The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.

routing

Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.

SDNS

Secondary Domain Name System (server)
A DNS server that can be used if the primary DSN server is not available. *See DNS*.

subnet

A subnet is a portion of a network. The subnet is distinguished from the larger network by a *subnet mask* that selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See *network mask*.

subnet mask

A mask that defines a subnet. See *network mask*.

TCP

See *TCP/IP*.

TCP/IP

Transmission Control Protocol/Internet Protocol
The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.

Telnet

An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.

TFTP

Trivial File Transfer Protocol
A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.

TKIP

Temporal Key Integrity Protocol (TKIP) provides WPA with a data encryption function. It ensures that a unique master key is generated for each packet, supports message integrity and sequencing rules and supports re-keying mechanisms.

triggers

Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, open secondary connections during normal operations, for example, a connection to a server is established using one port, but data transfers are performed on a separate connection. A trigger tells the device to expect these secondary sessions and how to handle them.

Once you set a trigger, the embedded IP address of each incoming packet is replaced by the correct host address so that NAT can translate packets to the correct destination. You can specify whether you want to carry out address replacement, and if so, whether to replace addresses on TCP packets only, UDP packets only, or both.

twisted pair The ordinary copper telephone wiring used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See *10BASE-T, 100BASE-T, Ethernet*.

unnumbered interfaces

An unnumbered interface is an IP interface that does not have a local subnet associated with it. Instead, it uses a *router-id* that serves as the source and destination address of packets sent to and from the router. Unlike the IP address of a normal interface, the router-id of an unnumbered interface is allowed to be the same as the IP address of another interface. For example, the WAN unnumbered interface of your device uses the same IP address of the LAN interface (10.10.10.2).

The unnumbered interface is temporary – PPP or DHCP will assign a 'real' IP address automatically.

upstream The direction of data transmission from the user to the Internet.

VC Virtual Circuit
A connection from your DSL router to your ISP.

VCI Virtual Circuit Identifier
Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. See *VC*.

VPI Virtual Path Identifier
Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. See *VC*.

WAN Wide Area Network
Any network spread over a large geographical area, such as a country or continent. With respect to the Wireless Gateway, WAN refers to the Internet.

Web browser A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See *HTTP, web site, WWW*.

Web page A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the *home page*. See *hyperlink, web site*.

Web site A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See *hyperlink, web page*.

WWW	World Wide Web Also called *(the) Web.* Collective term for all web sites anywhere in the world that can be accessed via the Internet.