LevelOne
User Manual

WBR-6013

Version : v1.0_20161221

Table of Contents

1 Introduction

Congratulations on becoming the owner of the WBR-6013. 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 WBR-6013, 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:

- 10/100Base-T 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
- User-friendly configuration program accessed via a web browser
- User-friendly configuration program accessed via EasySetup program

The WBR-6013 has the internal Ethernet switch allows for a direct connection to a 10/100Base-T Ethernet network via an RJ-45 interface, with LAN connectivity for both the WBR-6013 and a co-located PC or other Ethernet-based device.

Device Requirements

In order to use the WBR-6013, 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 (10/100Base-T 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 v4 or later, or Netscape v4 or later. Note that version 4 of each browser is the minimum version requirement – for optimum display quality, use Internet Explorer v5, or Netscape v6.1
b.EasySetup program: Graphical User Interface

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 WBR-6013 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

- Windows 98SE, Windows Me, Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1 and Windows 10

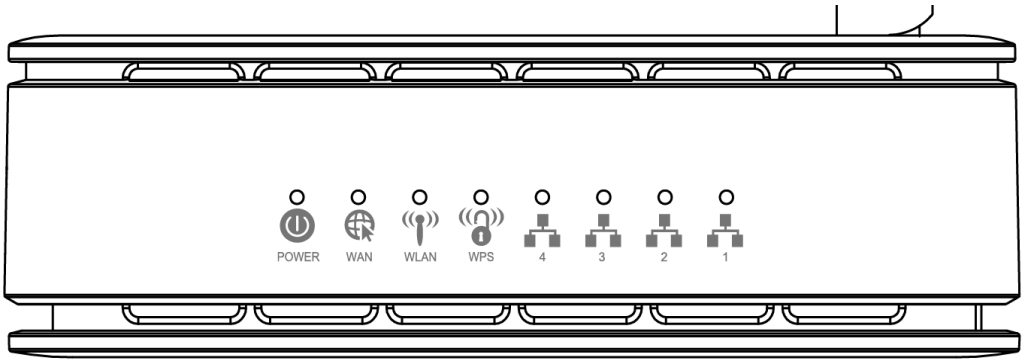
Package Contents

1. WBR-6013
2. Quick Installation Guide
3. Ethernet Cable (RJ-45)
4. Power Adapter

LED meanings & activations

Front Panel

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



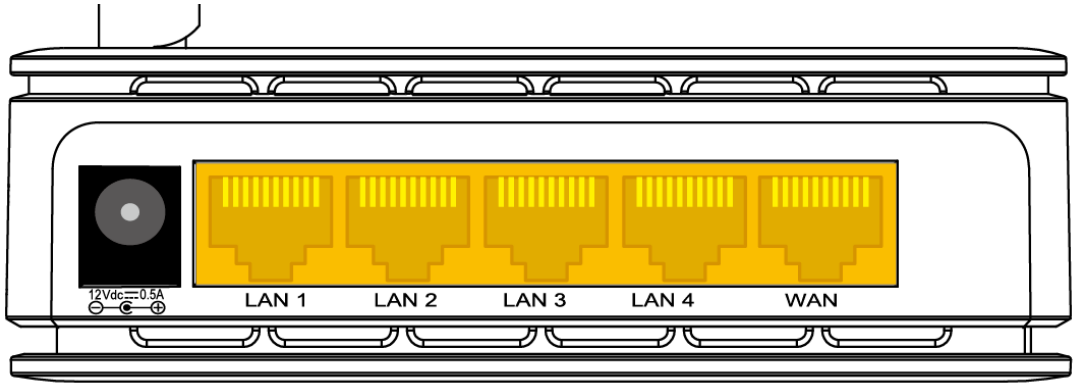
**** Actual Front Panel and ANTENNA may vary depending on model.***

Figure 1: Front Panel and LEDs

Label	Color	Function
POWER	green	On: device is powered on Off: device is powered off
WAN	green	On: WAN link established and active Off: No LAN link Blink: Valid Ethernet packet being transferred
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
LAN 1/2/3/4	green	On: LAN link established and active Off: No LAN link Blink: Valid Ethernet packet being transferred

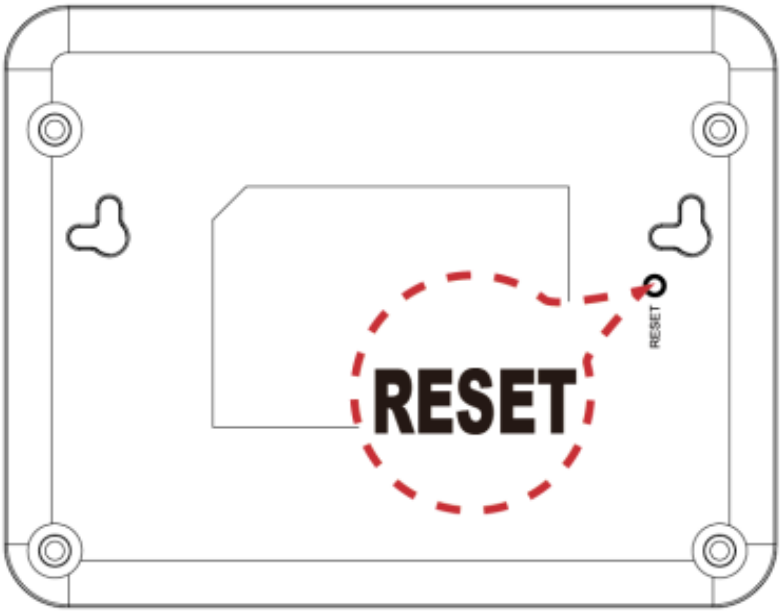
Rear and Right Panel and bottom Side

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



**** Actual Rear Panel and ANTENNA may vary depending on model.***

Figure 2: Rear Panel Connections



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

Figure 3: RESET button

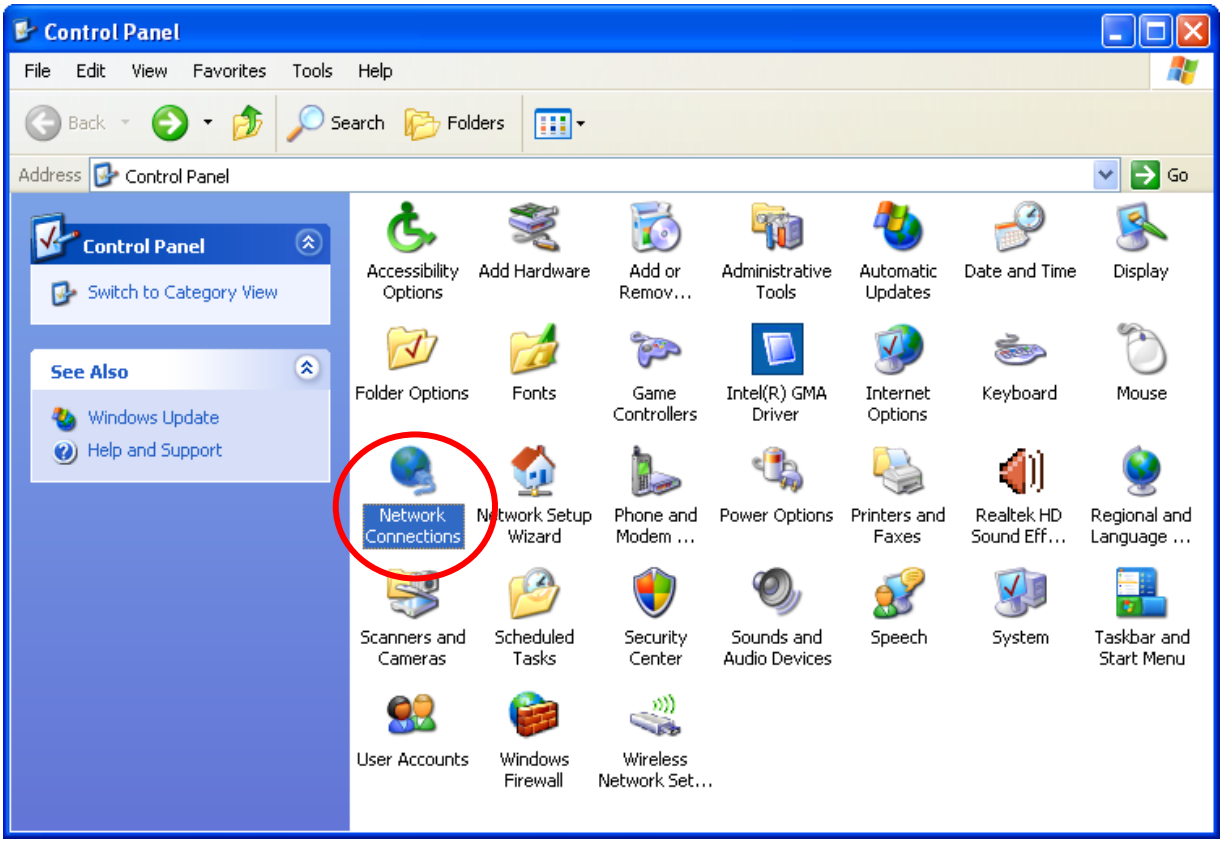
Label	Function
ANTENNA	2 fixed ANTENNA
POWER	Connects to the supplied power adaptor
ON/OFF SWITCH	Power on / off the device
LAN 4/3/2/1	Connects the device via LAN Ethernet to up to 4 PCs
WAN	Connects the device via WAN Ethernet to xDSL / Cable Modem
WPS	Press this button for at least 3 full seconds 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.
WLAN	Press this button for at least 3 full second to turn off/on wireless signals
RESET	Reset button. **RESET** the WBR-6013 to its default settings. Press this button for at least 6 full seconds to **RESET** device to its default settings.

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

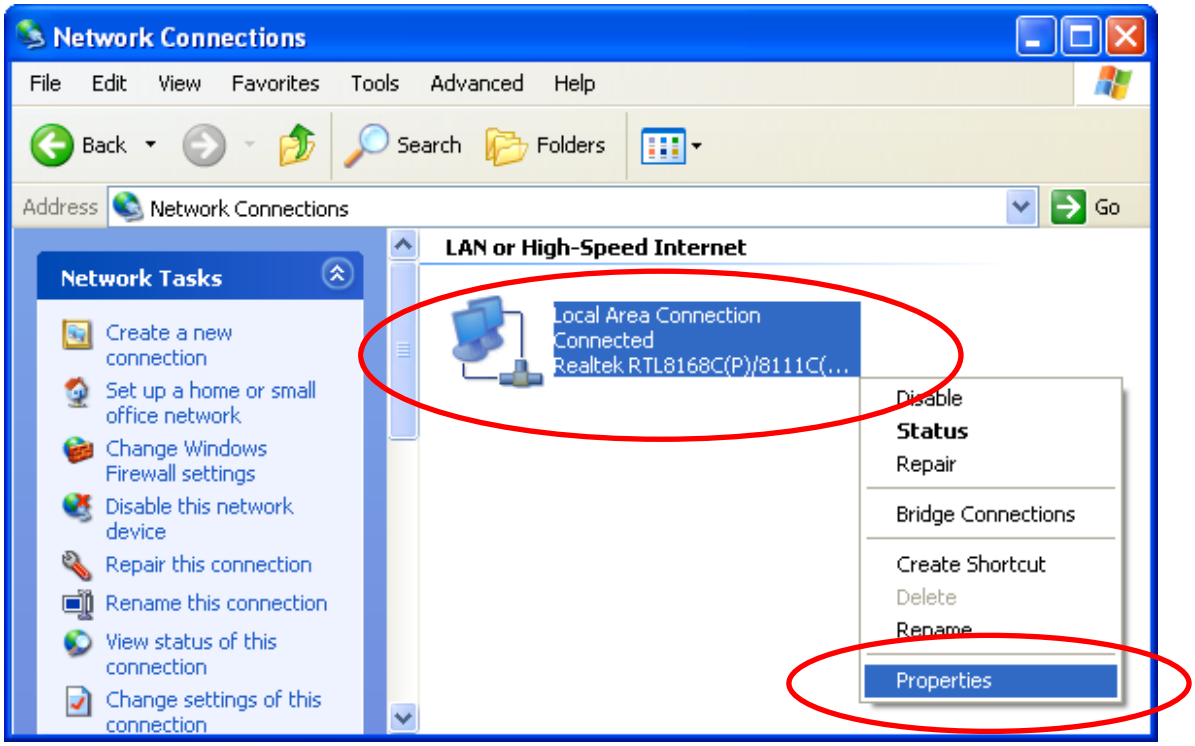
Before starting the WBR-6013 configuration, please kindly configure the PC computer as below, to have automatic IP address / DNS Server.

For Windows 98SE / ME / 2000 / XP

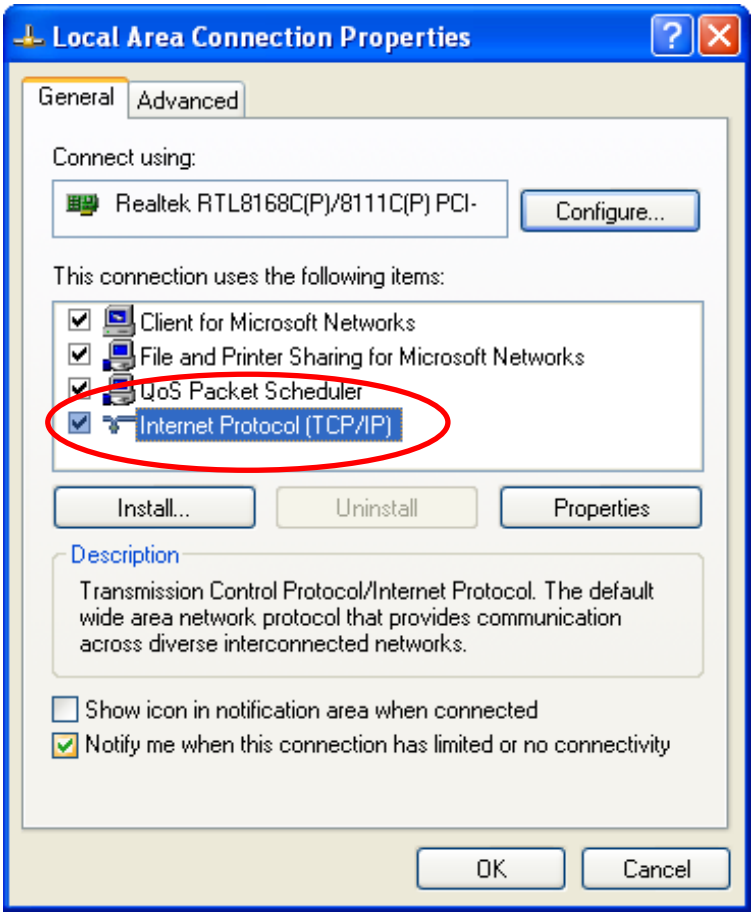
1. Click on "**Start**" -> "**Control Panel**" **(in Classic View)**. In the Control Panel, double click on "**Network Connections**" to continue.



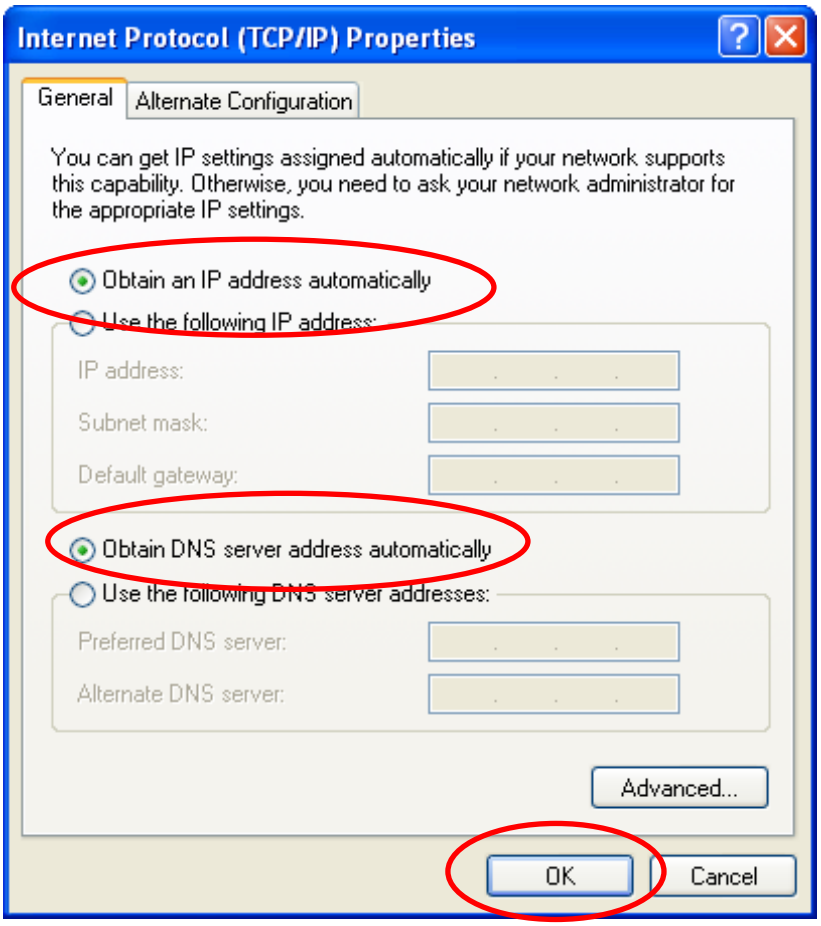
2. Single RIGHT click on "**Local Area connection**", then click "**Properties**".



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



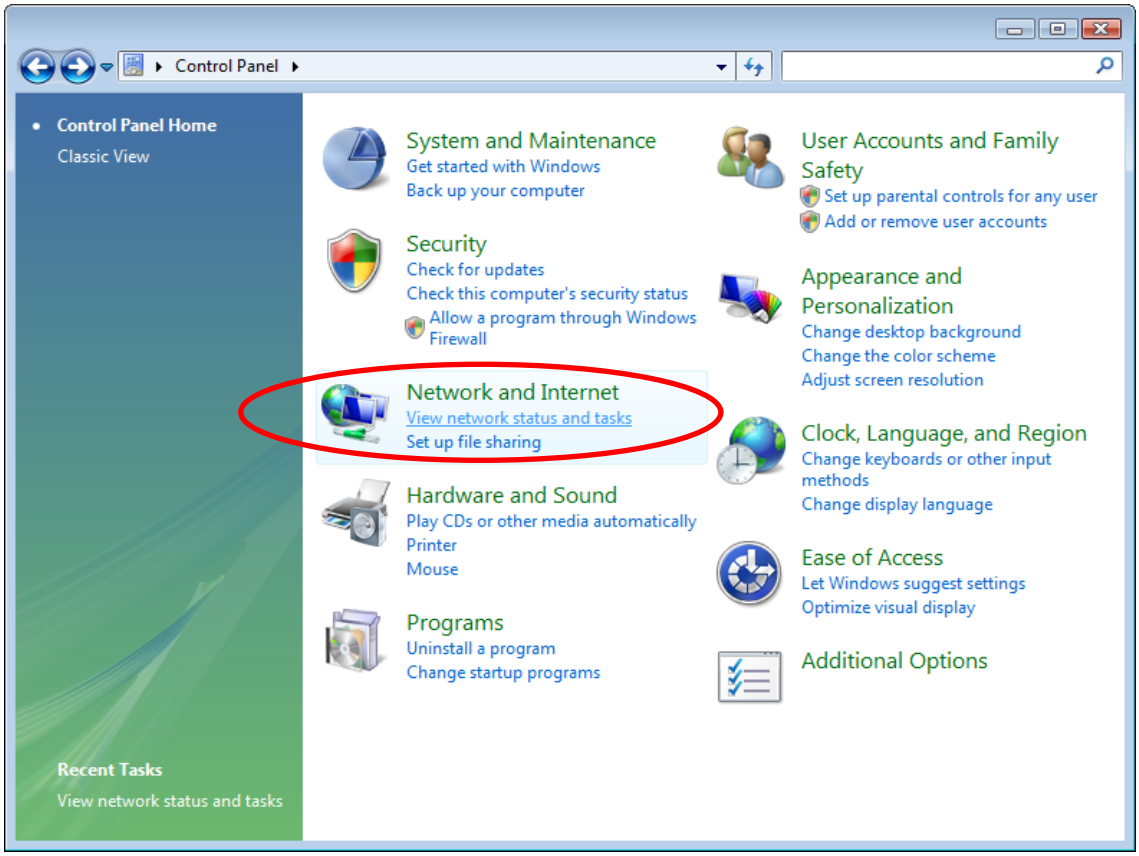
4. Check "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" then click on "**OK**" to continue.



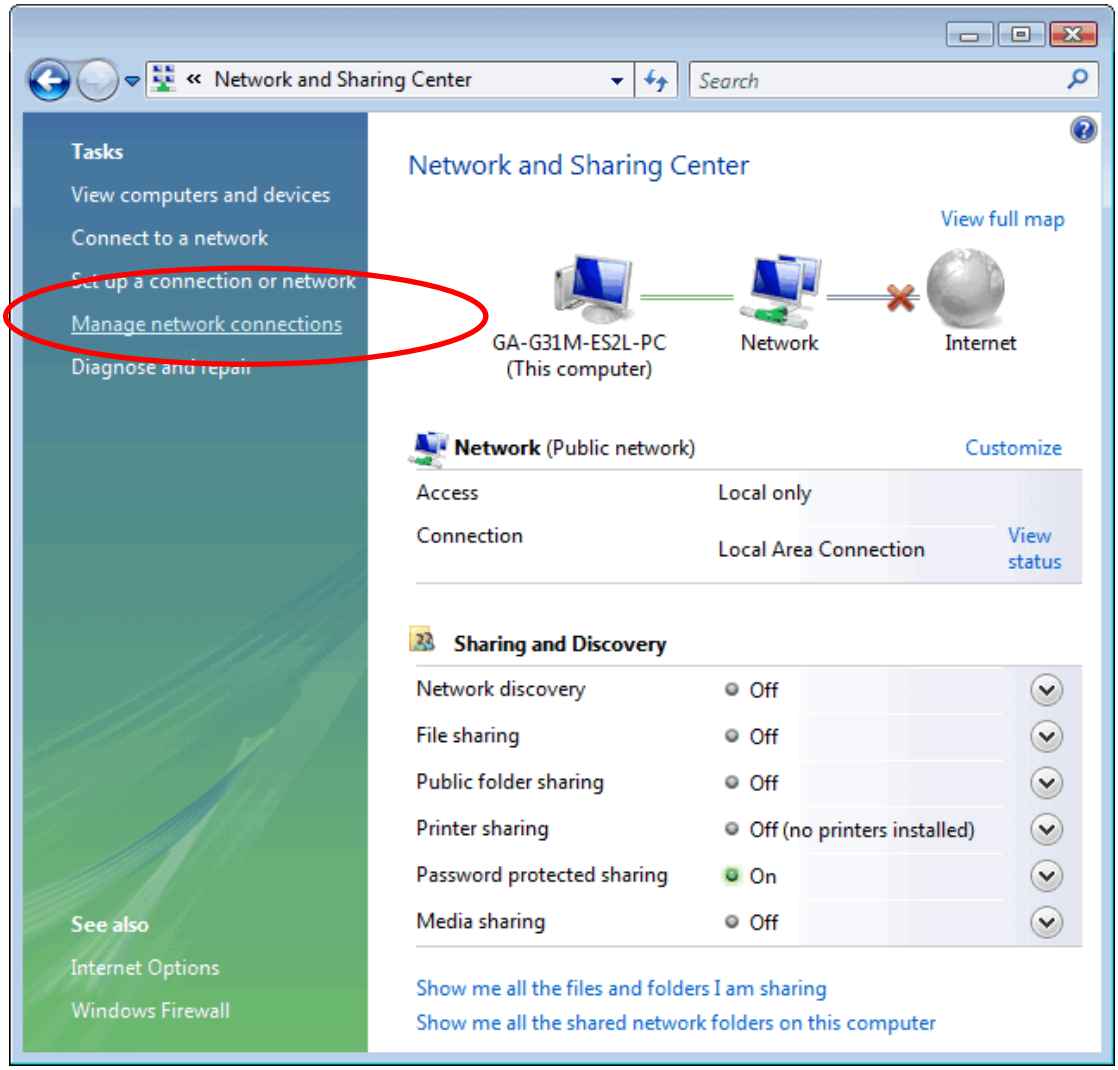
5. Click "**Show icon in notification area when connected**" (see screen image in 3. above) then Click on "**OK**" to complete the setup procedures.

For Windows Vista-32/64

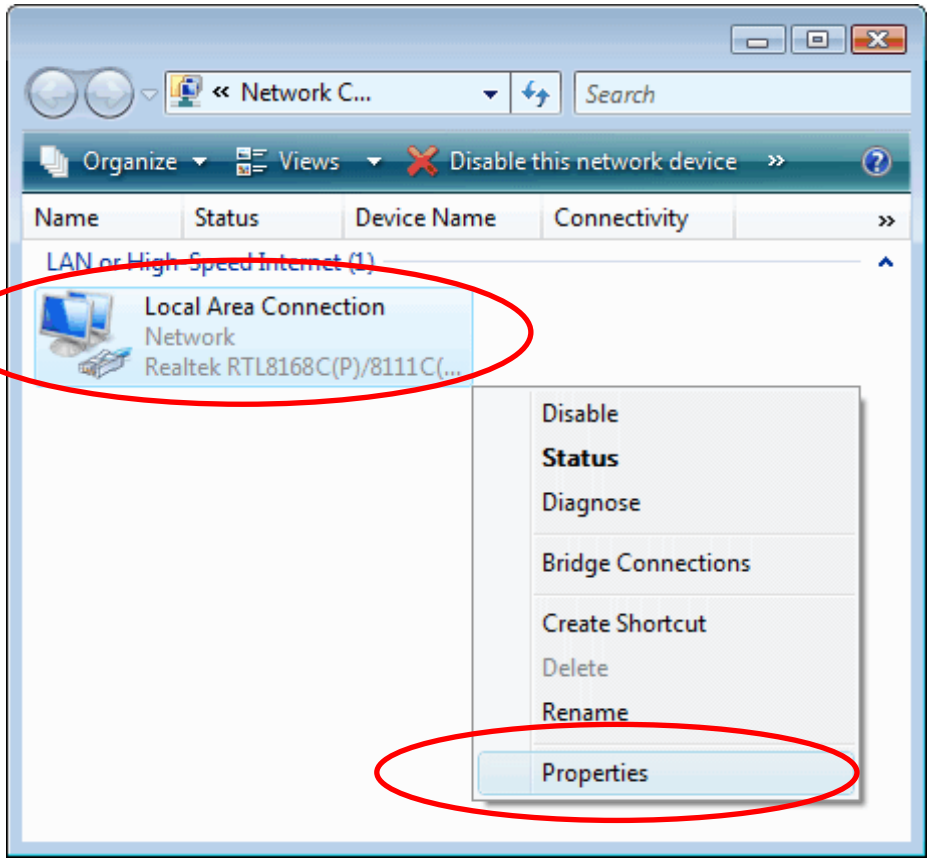
1. Click on “**Start**” -> “**Control Panel**” -> “**View network status and tasks**”.



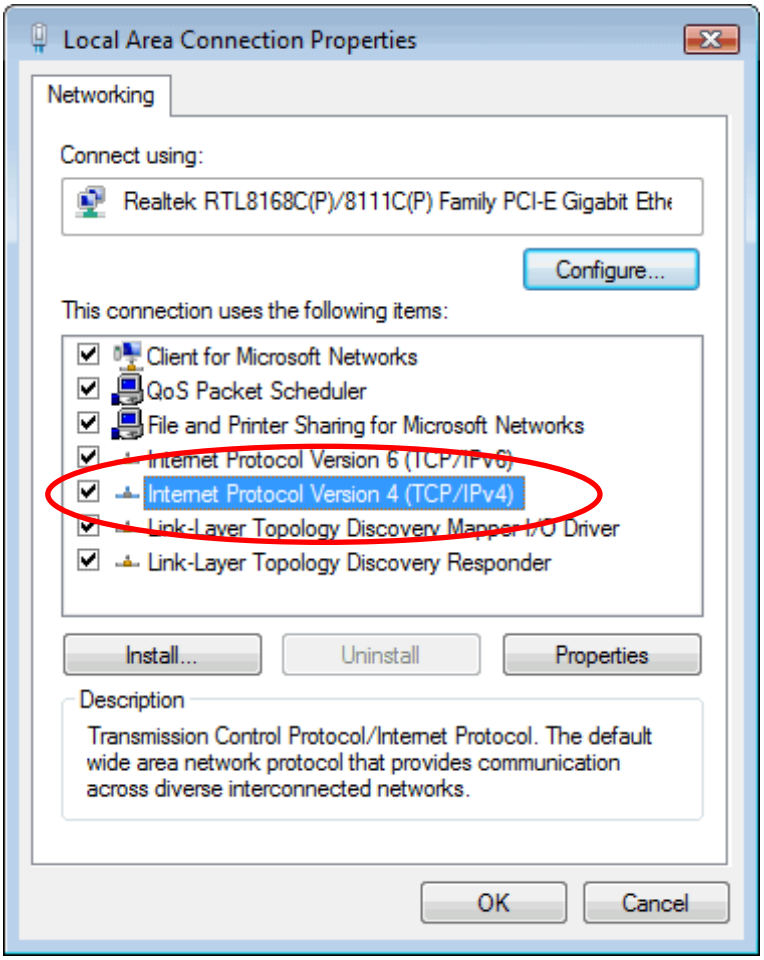
2. In the Manage network connections, click on "**Manage network connections**" to continue.



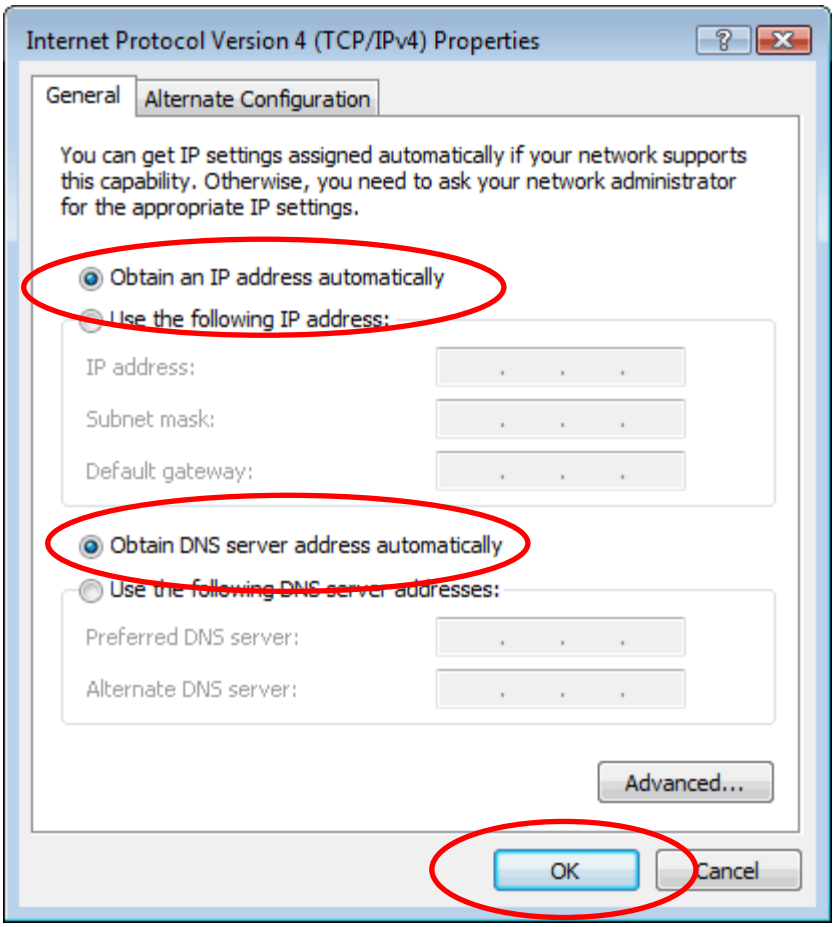
3. Single RIGHT click on "**Local Area connection**", then click "**Properties**".



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)**".

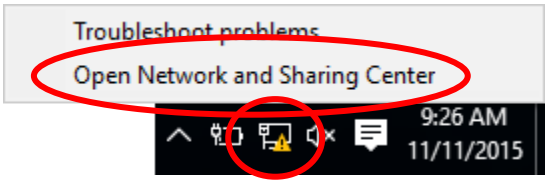


6. Check "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" then click on "**OK**" to continue.

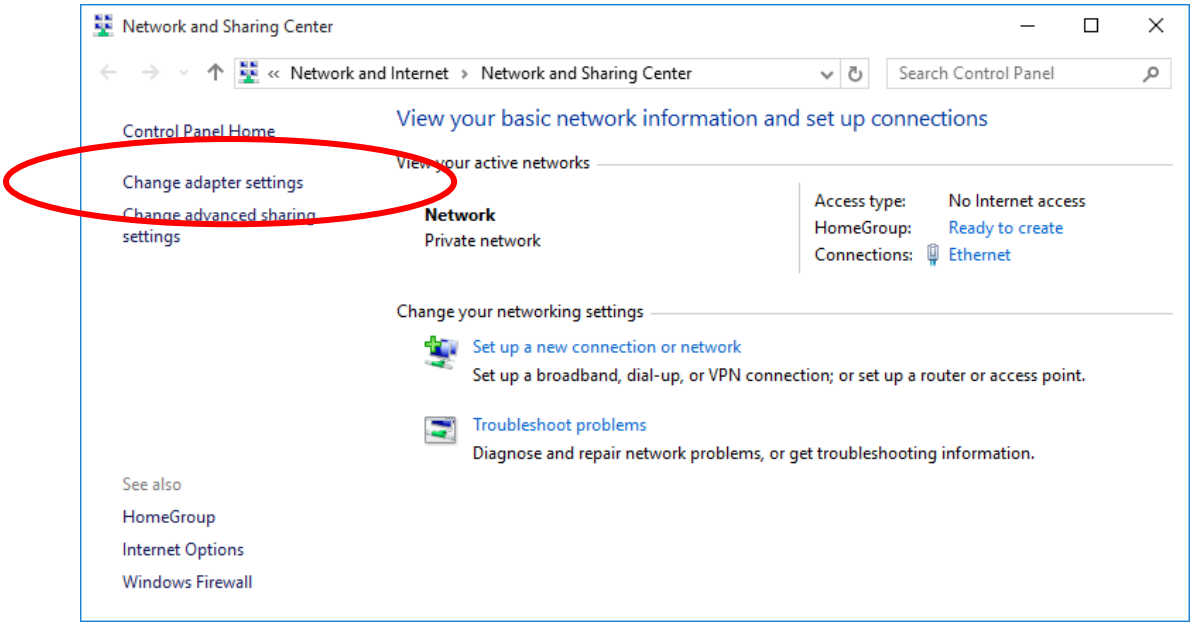


For Windows 7/8/8.1/10-32/64

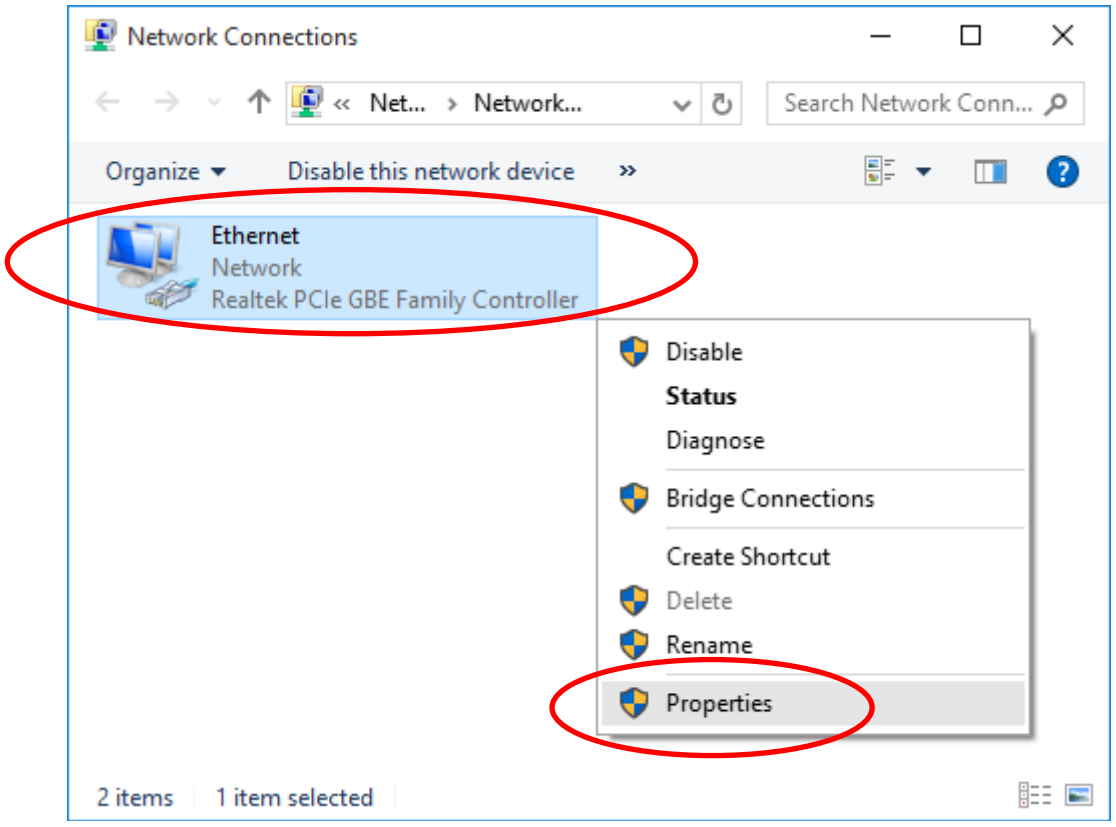
1. Right click on ***Network*** icon , then click "***Open Network and Sharing Center***".



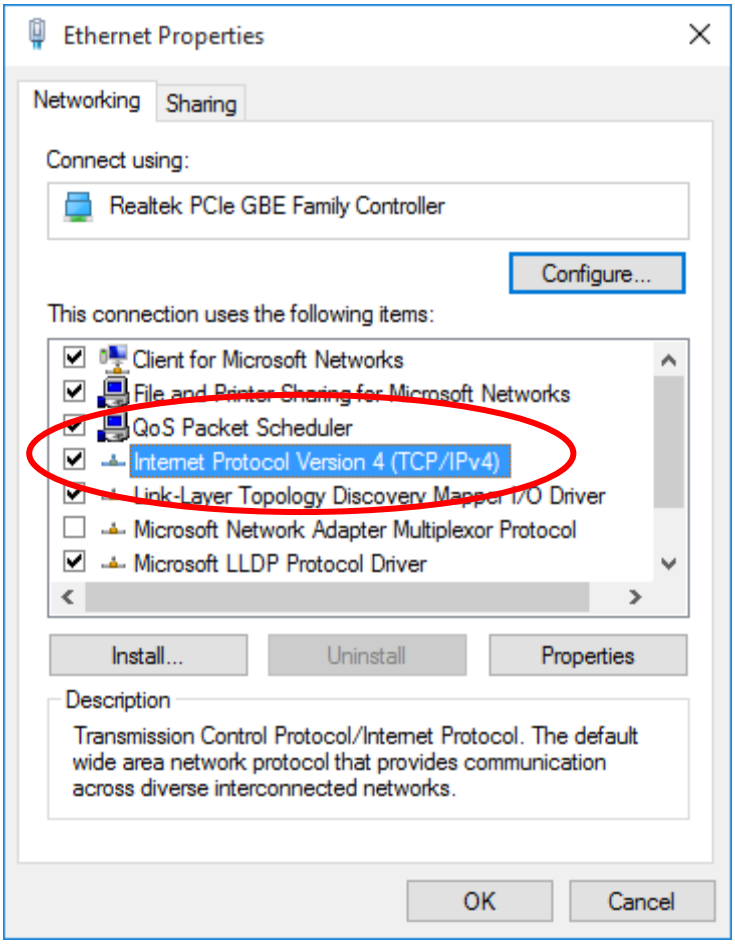
1. In the Control Panel Home, click on "**Change adapter settings**" to continue.



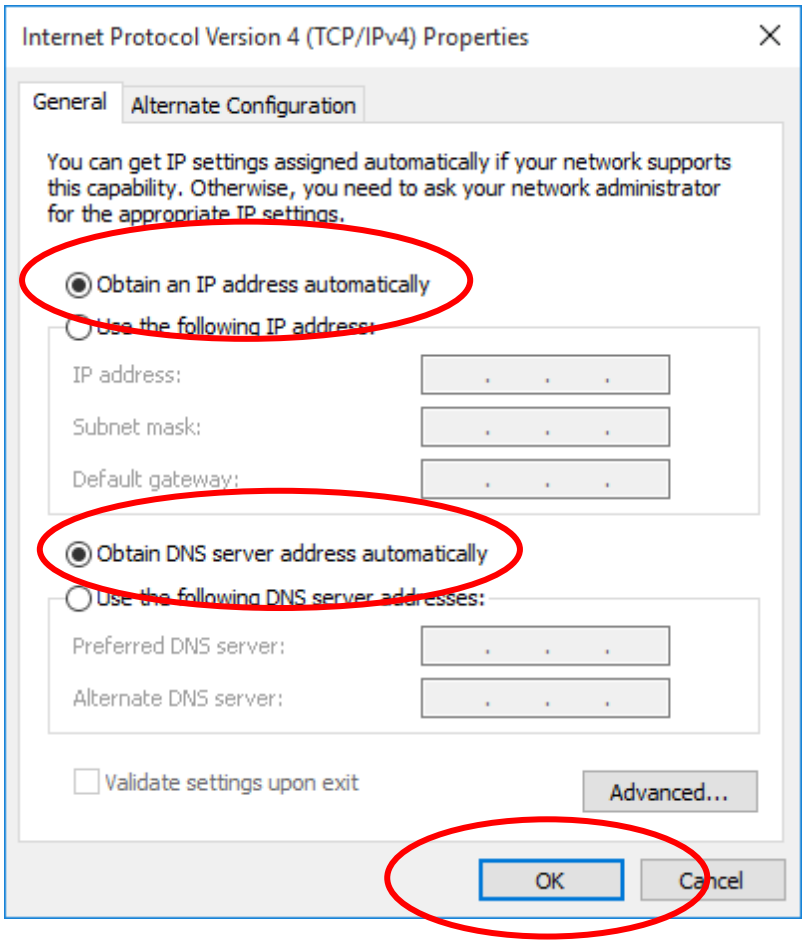
2. Single RIGHT click on “**Ethernet**", then click "**Properties**".



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



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



4 Connecting your device

This chapter provides basic instructions for connecting the WBR-6013 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 WBR-6013.*

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.

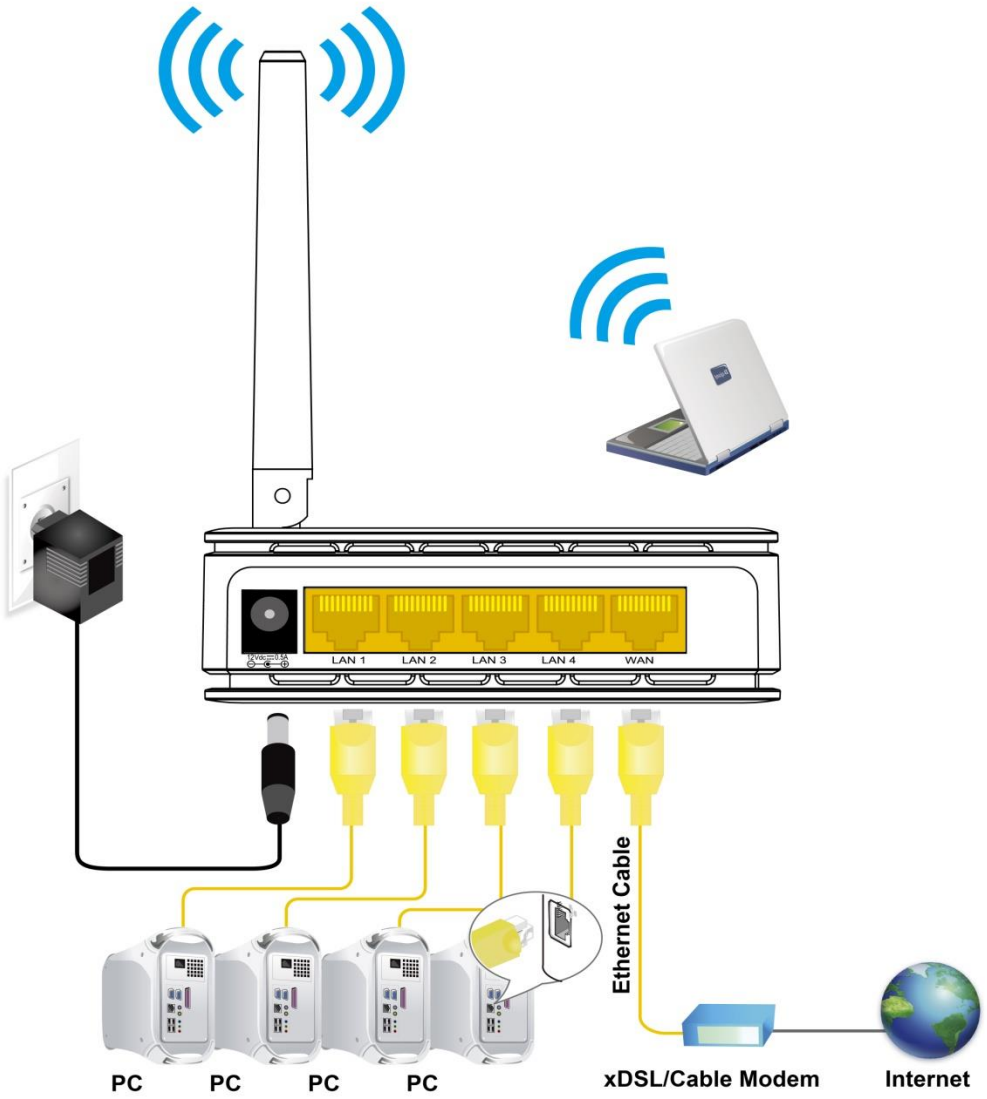


Figure 4: Overview of Hardware Connections

Step 1. Connect the Ethernet cable to WAN Port

Connect the RJ45 Ethernet cable from your xDSL/Cable Modem's Ethernet port to WBR-6013 WAN Port.

Step 2. Connect the Ethernet cable to LANPort

Connect the supplied RJ45 Ethernet cable from your PC's Ethernet port to any of the 4 WBR-6013 LAN Ports.

Step 3. Attach the power connector

Connect the power adapter to the power inlet "POWER" of the 802.11n WLAN Router and turn the power switch "ON/OFF SWITCH" of your WBR-6013 on.

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

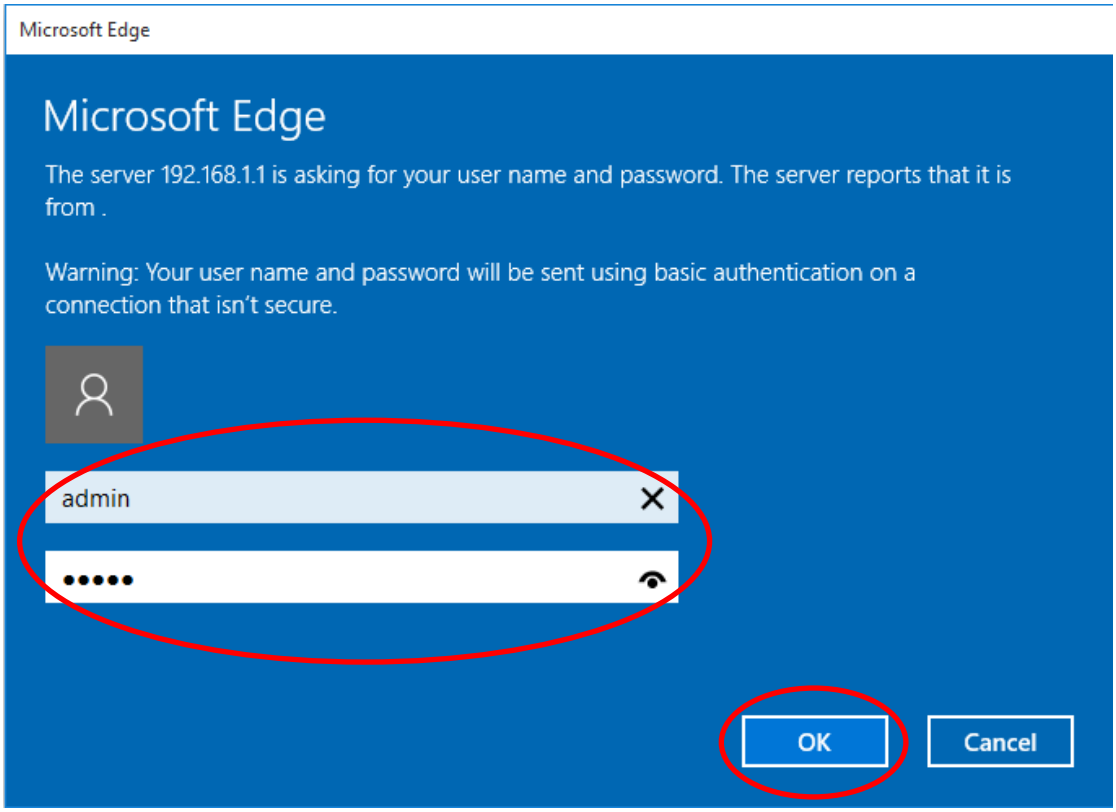
5 Advanced Configuration

Advanced Configuration

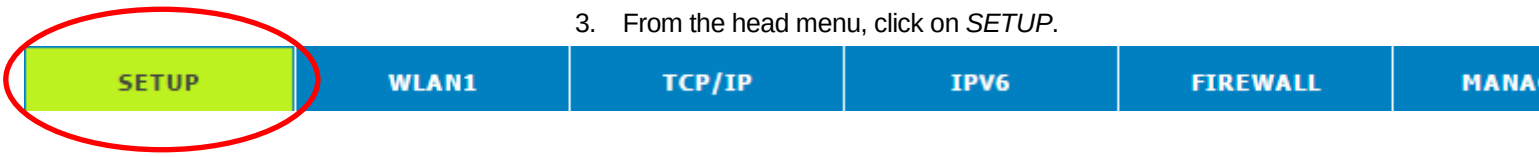
1. From any of the LAN computers, launch your web browser, type the following URL in the web address (or location) box, and press [Enter] on your keyboard:

   http://192.168.1.1

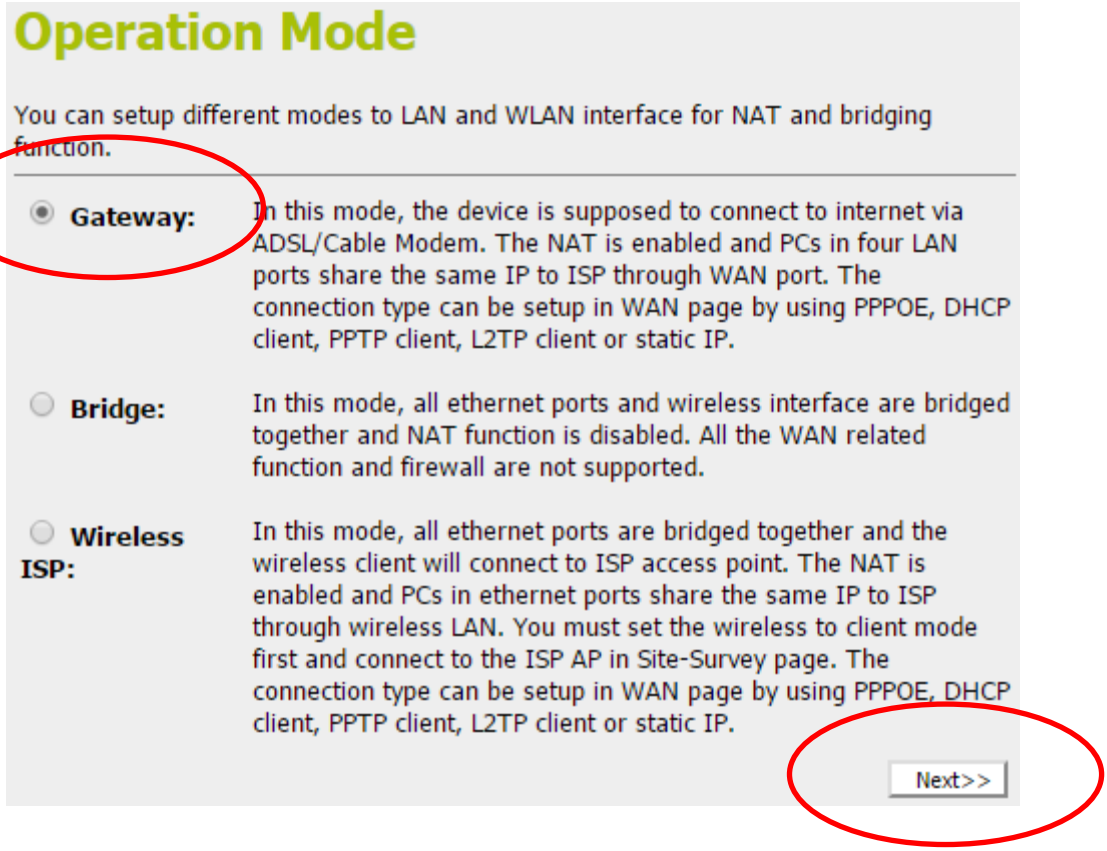
2. Please enter the User Name: **admin** and Password: **admin** and then click on **OK** button.



3. From the head menu, click on *SETUP*.



4. Check on *Gateway* ratio and then click on *Next*.

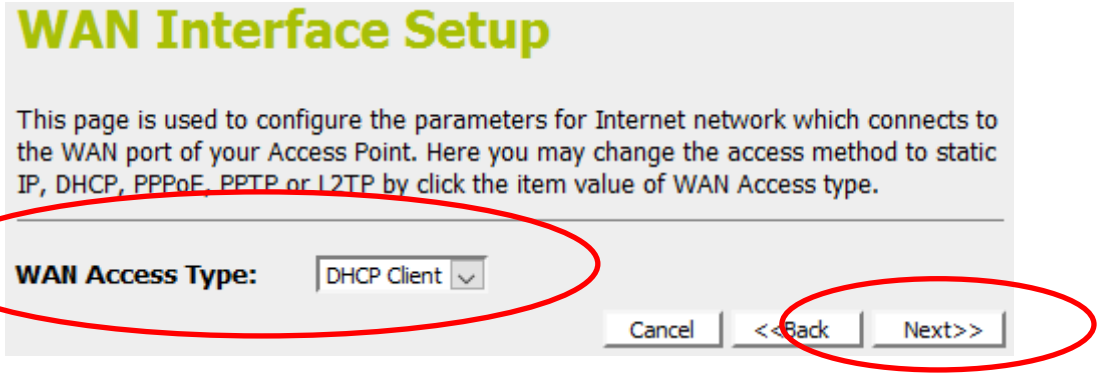


WAN Interface Setup

Examples

8-1. DHCP client

From the *WAN Access Type* drop-down list, select *DHCP Client*
If you are happy with your settings, click on*Next*

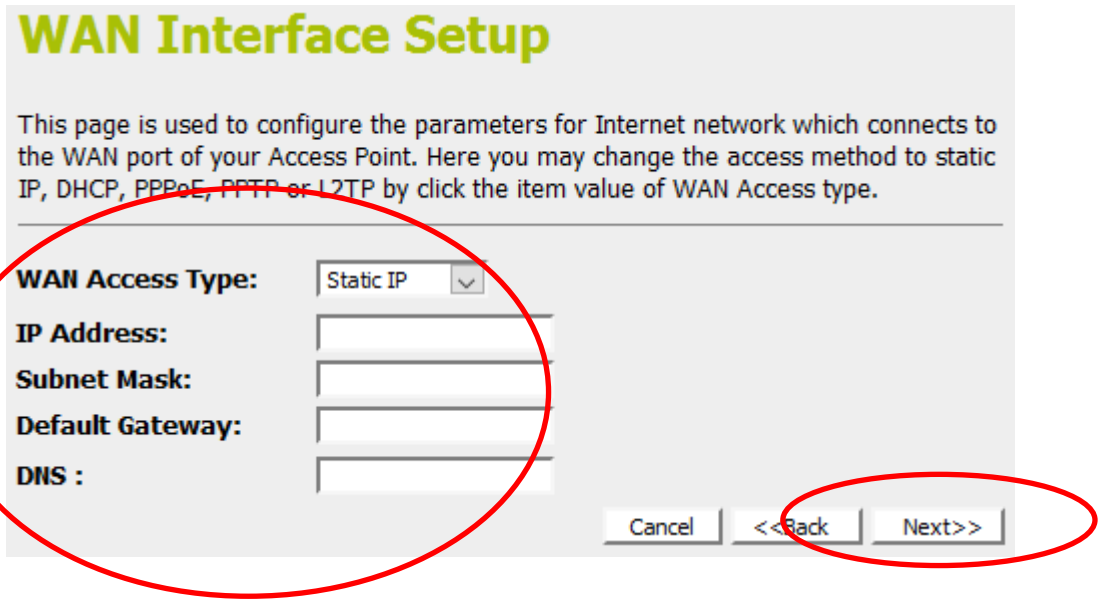


8-2. Static IP

From the *WAN Access Type* drop-down list, select *Static IP*setting.

Enter IP Address, Subnet Mask, Default Gatewayand DNS which was given by Telecom or by your Internet Service Provider (ISP).

If you are happy with your settings, click on*Next*

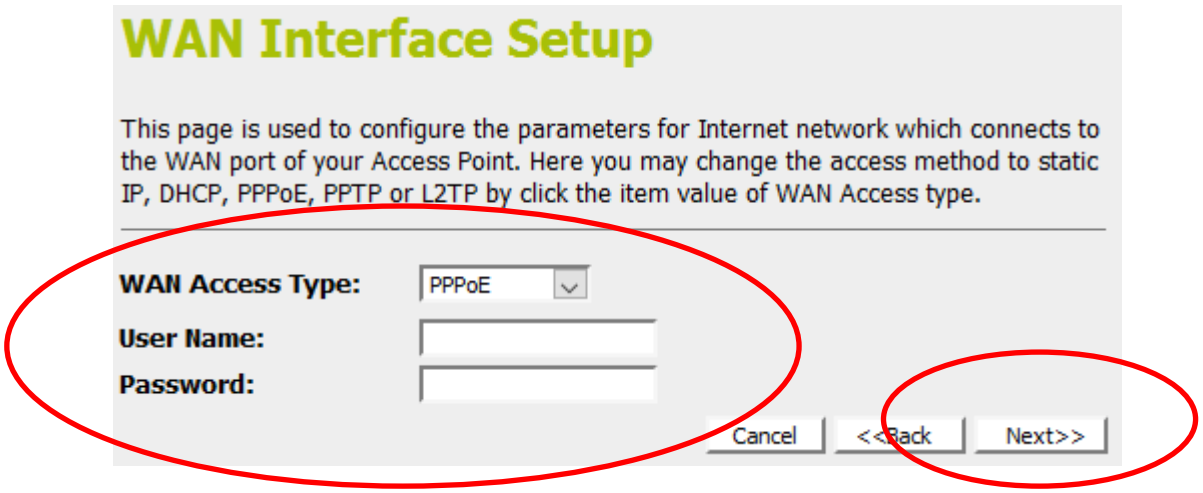


8-3. PPPoE

From the *WAN Access Type* drop-down list, select *PPPoE*setting.

Enter*User Name/Password* provided by your ISP. Type them in the relevant boxes.

If you are happy with your settings, click Next



8-4. PPTP

From the WAN Access Type drop-down list, select PPTP setting provided by your Network Administrator or ISP.

Click on the ratio of Dynamic IP (DHCP) or Static IP.

Enter IP Address for example 172.1.1.1 provided by your Network Administrator or ISP. (for Static IP only)

Enter Subnet Mask for example 255.255.0.0 provided by your Network Administrator or ISP. (for Static IP only)

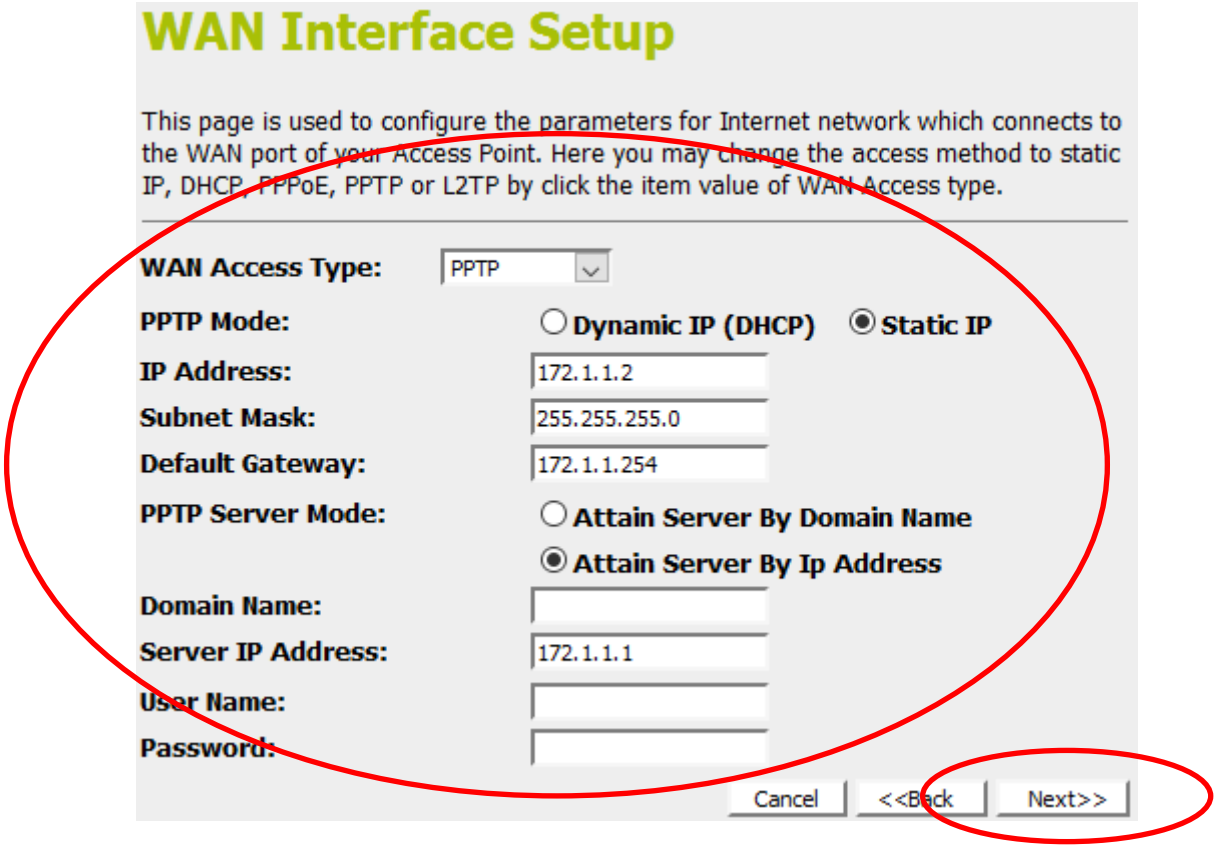
Enter Default Gateway for example 172.1.1.254 provided by your Network Administrator or ISP. (for Static IP only)

Enter Server Domain Address for example 222.222.222.222 or www.example.com provided by your Network Administrator or ISP.

Enter User Name for example 1234 provided by your Network Administrator or ISP.

Enter Password for example 1234 provided by your Network Administrator or ISP.

If you are happy with your settings, click Next



8-4. L2TP

From the WAN Access Type drop-down list, select L2TP setting provided by your Network Administrator or ISP.

Click on the ratio of Dynamic IP (DHCP) or Static IP.

Enter IP Address for example 172.1.1.1 provided by your Network Administrator or ISP. (for Static IP only)

Enter Subnet Mask for example 255.255.0.0 provided by your Network Administrator or ISP. (for Static IP only)

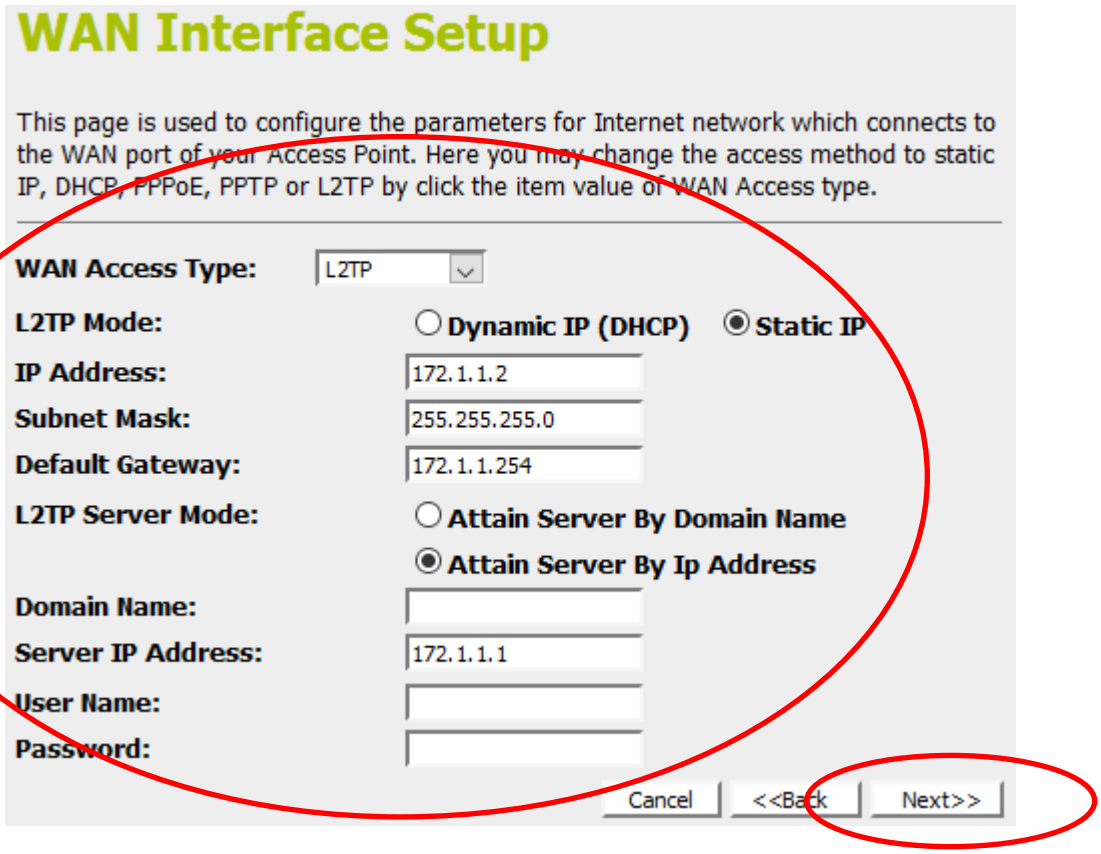
Enter Default Gateway for example 172.1.1.254 provided by your Network Administrator or ISP. (for Static IP only)

Enter Server Domain Address for example 222.222.222.222 or www.example.com provided by your Network Administrator or ISP.

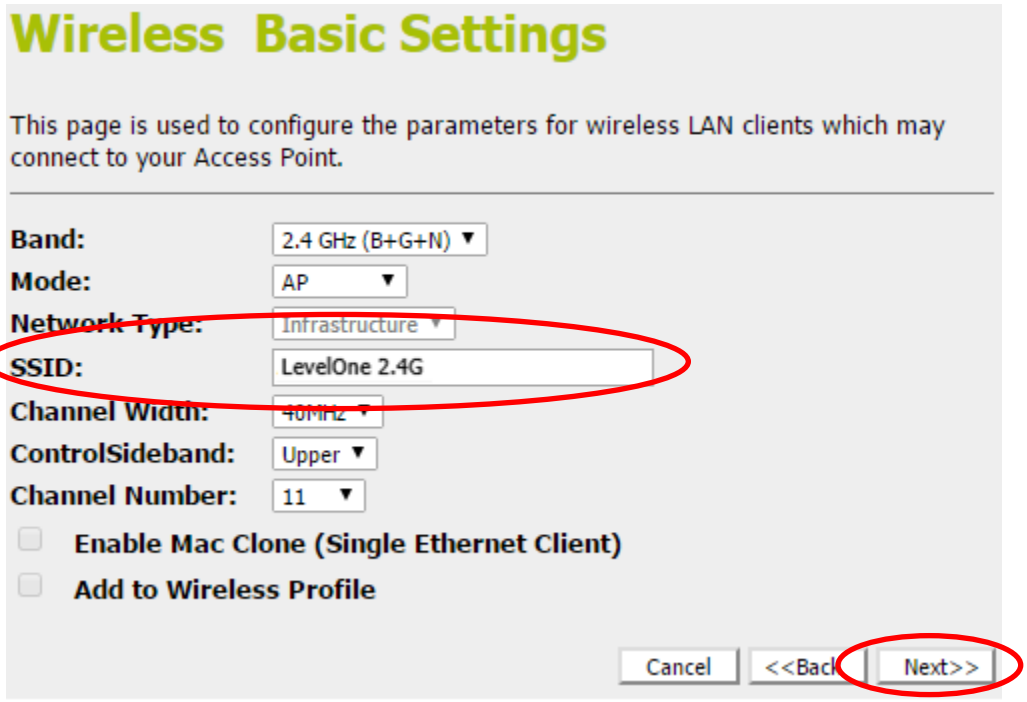
Enter User Name for example 1234 provided by your Network Administrator or ISP.

Enter Password for example 1234 provided by your Network Administrator or ISP.

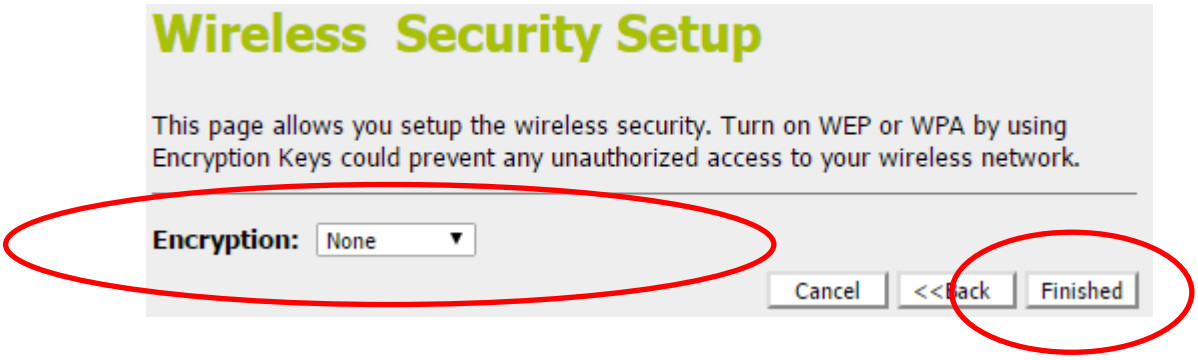
If you are happy with your settings, click Next



5. Enter SSID.
6. Click on *Next*.



7. From the *Encryption* list, choose the Encryption type and enter related parameters if necessary, as None / WEP / WPA2(AES) and WPA Mixed Mode (the default settings Security Mode = None). For example, the Encryption you choose is None.
8. Click on *Finished*.



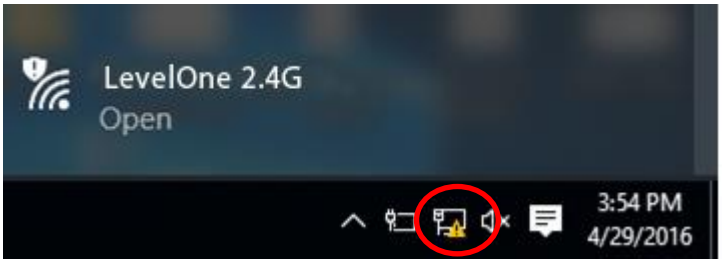
9. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

10. Now, the WBR-6013 has been configured completely, and suitable for Wireless and Internet Connections.

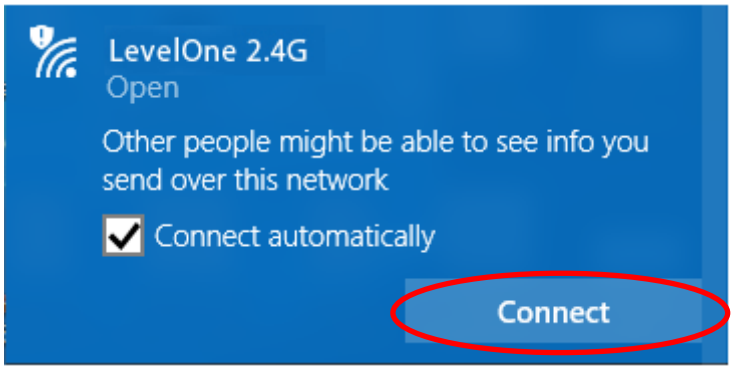
Wireless Connection

For easy installation it is saved to keep the settings. You can later change the wireless settings via the wireless configuration menu.

11. Double click on the wireless icon on your computer and search for the wireless network that you enter SSID name.
12. Click on the wireless network that you enter SSID name (the default settings, Wireless Network = Enable, Default Channel = Auto, SSID = LevelOne 2.4G which could be found on the bottom side of the device) to connect.



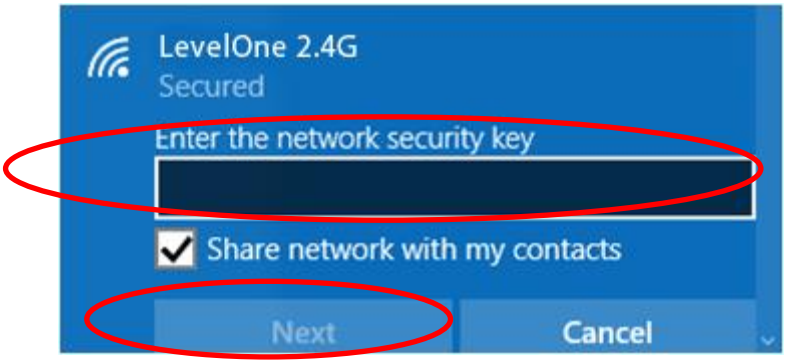
13. If the wireless network isn't encrypted, click on "Connect " to connect.



14. If the wireless network is encrypted, enter the network key that belongs to your authentication type and key.**(the default settings Security Mode = WPA Mixed mode**

which could be found on the bottom side of the device). You can later change this network key via the wireless configuration menu.

15. Click on "Next".



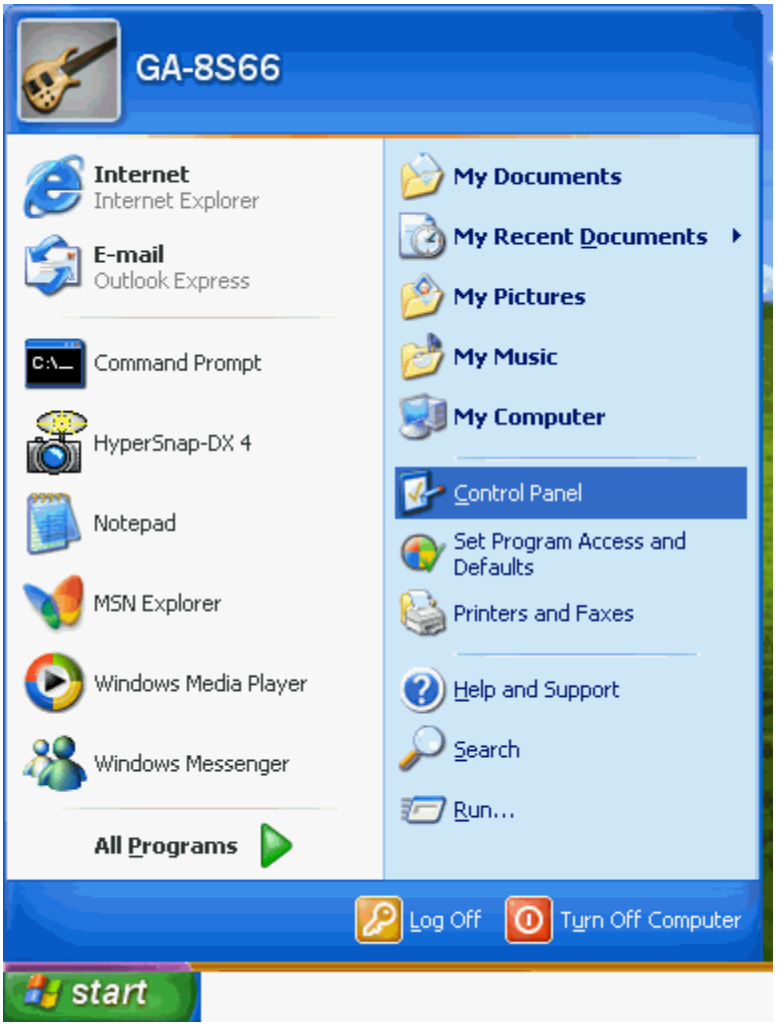
16. Now you are ready to use the Wireless Network to Internet or intranet.

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

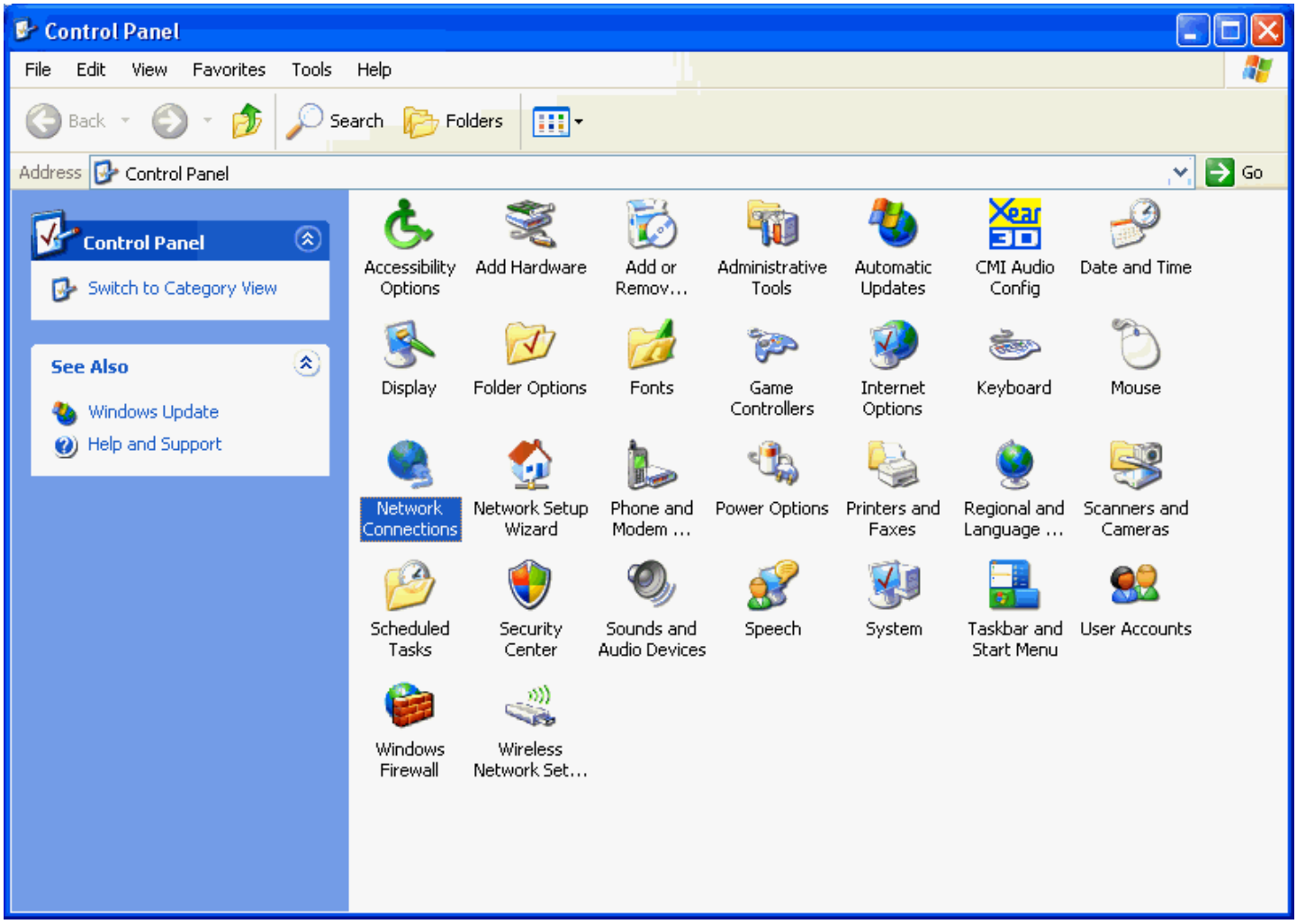
Now you could check what the Internet/WAN access of your network is to know how to configure the WAN port of WBR-6013.

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



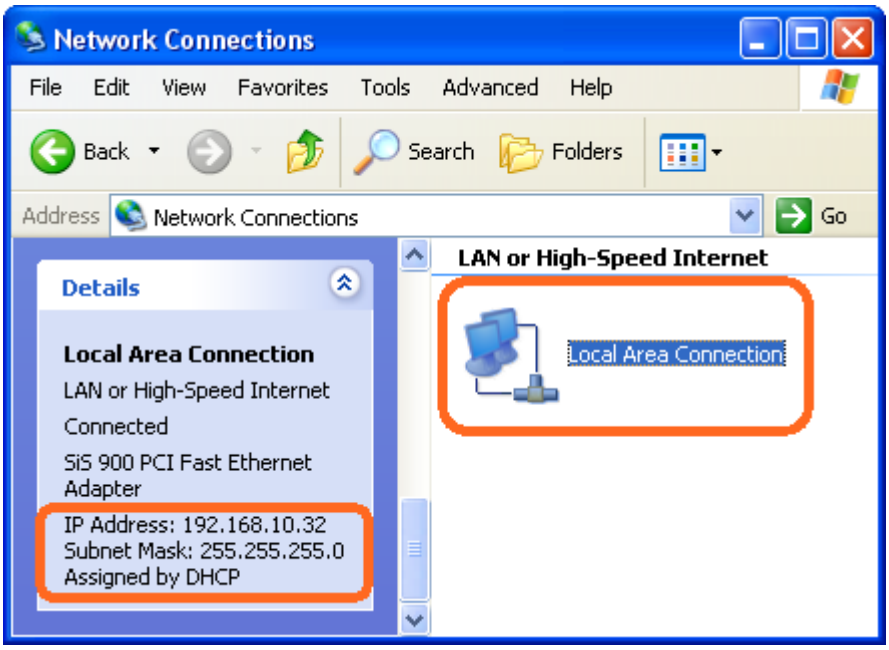
2. Double click *Network Connections*



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**.

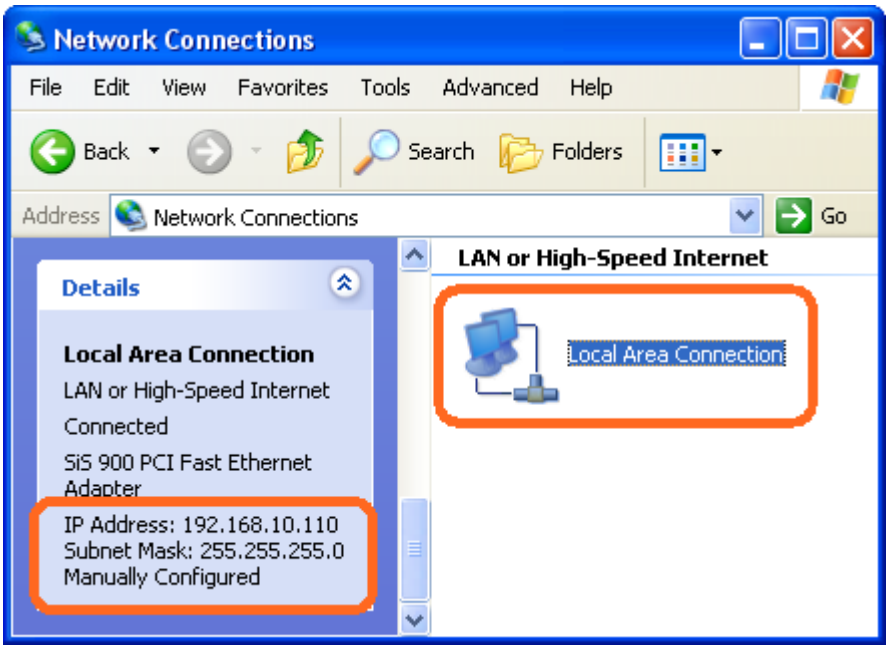
3. Click **Local Area Connection** in **LAN or High-Speed Internet** and you could see string **Assigned by DHCP** in Details.



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**.

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



5. 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:

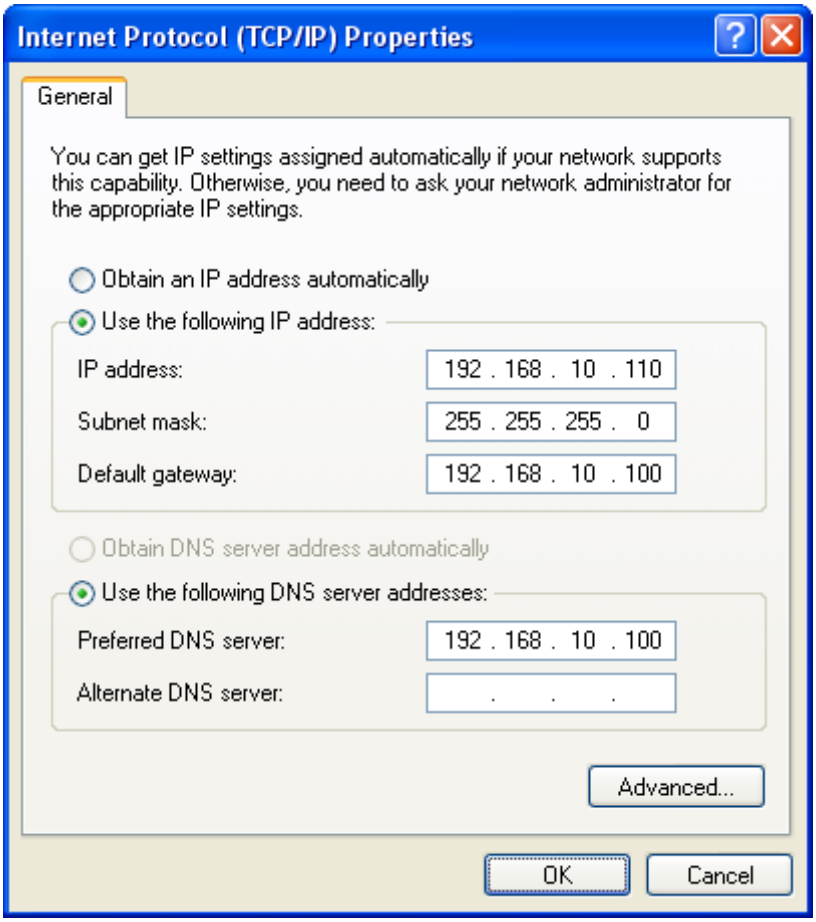
IP Address: 192.168.10.110

Subnet mask: 255.255.255.0

Default gateway: 192.168.10.100

Preferred DNS server: 192.168.10.100

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



Internet/WAN access is the PPPoE client

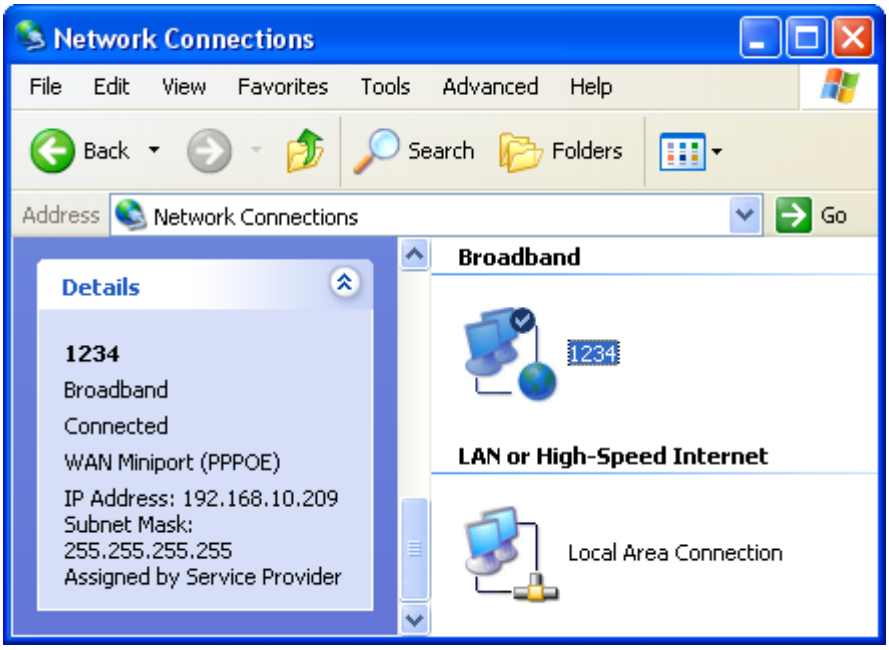
If you can see any **Broadband Adapter** in the **Network Connections**, your Internet/WAN access is **PPPoE Client**.

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

For PPPoE configuration on Wireless Gateway, 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



7 Getting Started with the Web pages

The WBR-6013 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 viathe 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://192.168.1.1

  The homepage for the web pages is displayed:

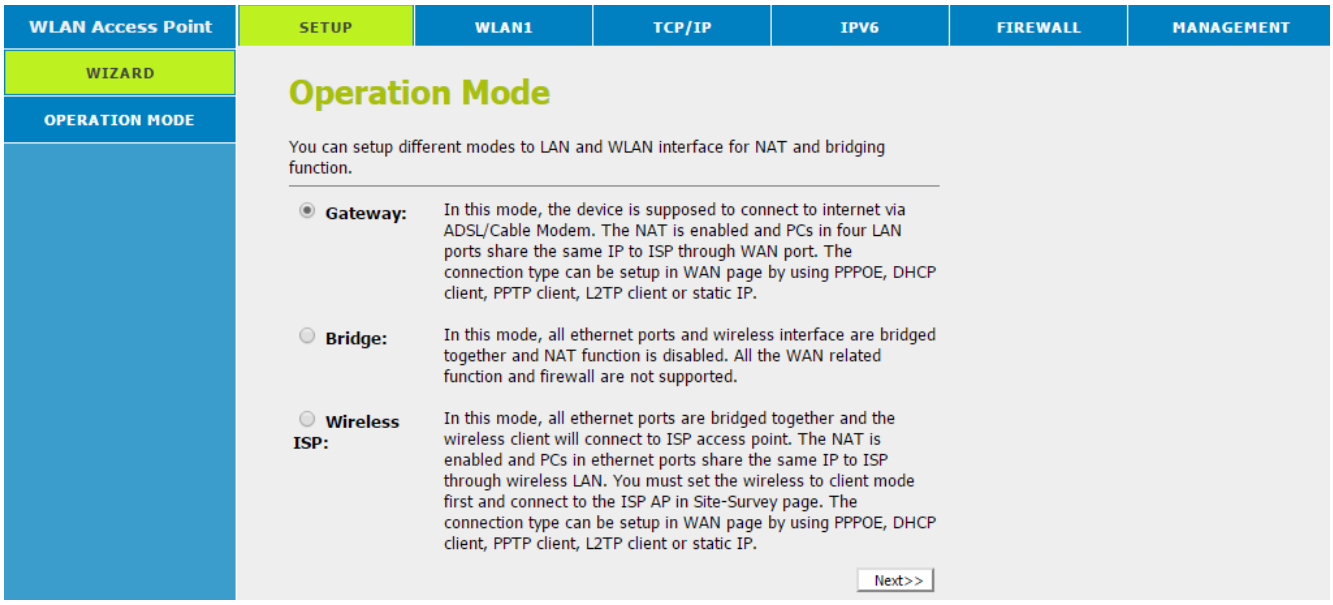


Figure 5: Homepage

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

A login screen is displayed:

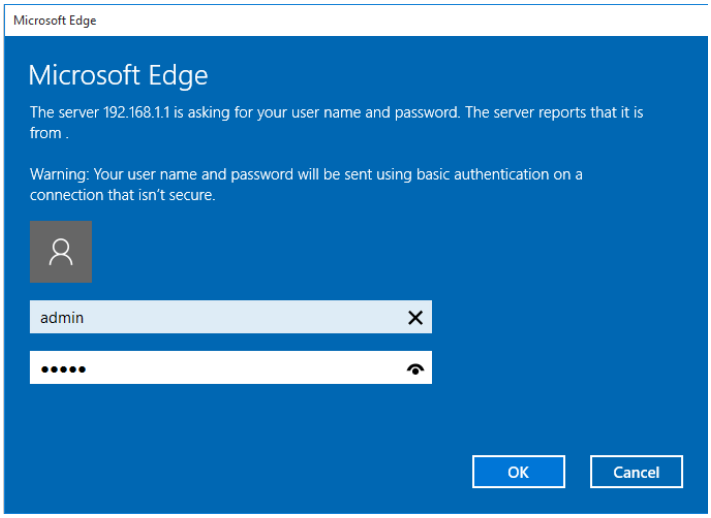


Figure 6: Login screen

1. 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.

2. Click on OK. You are now ready to configure your device.

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.

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 (2.4G)	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 WBR-6013 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*.

Option	Default Setting	Explanation/Instructions
LANPort IP Address	Assigned static IP address: 192.168.1.1 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: 192.168.1.100 through 192.168.1.200	The WBR-6013 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*.

8 Quick Setup

The *Quick Setup* page displays useful information about the setup of your device, including:

- details of the device's Internet access settings
- details of the device's Wireless settings

To display this page:

1. From the head menu, click on *SETUP*.

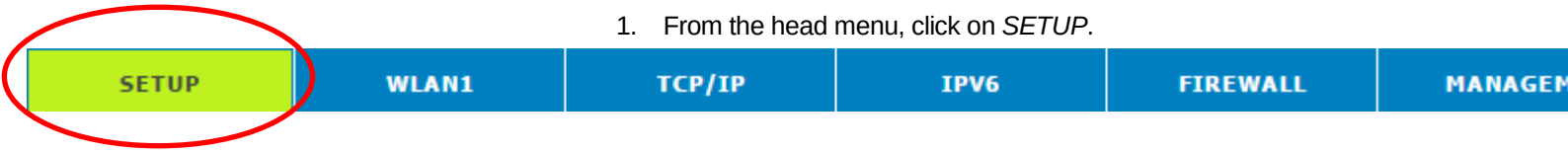


Figure 7: Quick Setup page

Operation Mode Setup

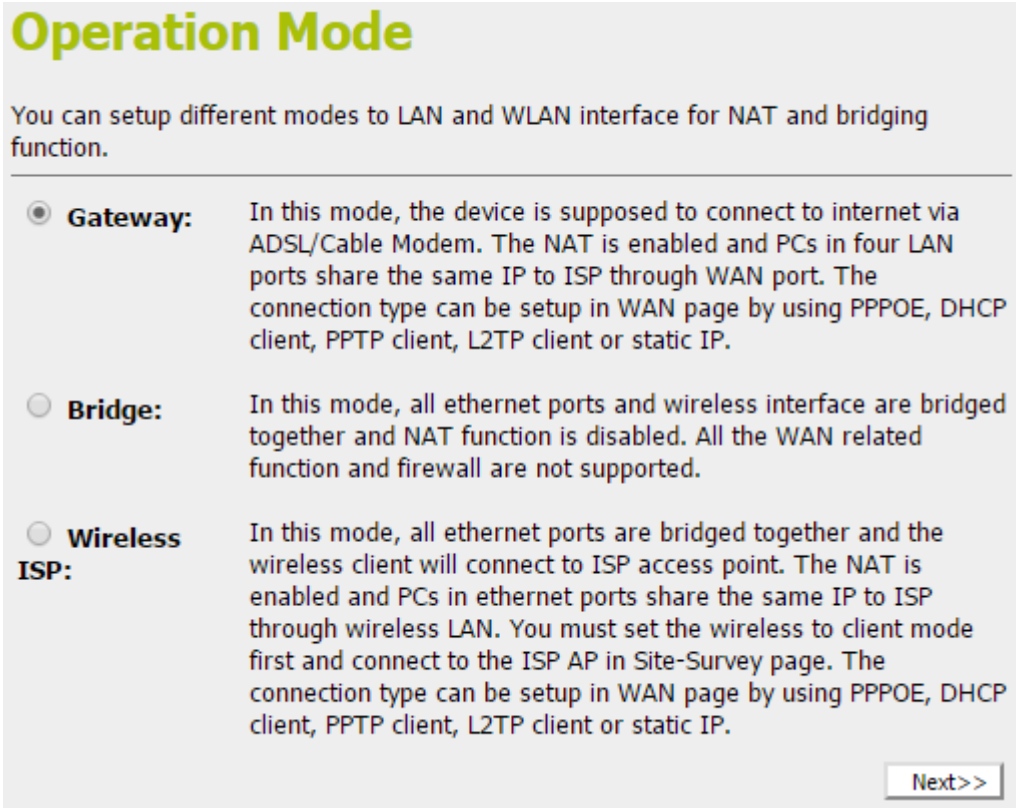
You can setup different modes to LAN and WLAN interface for NAT function.

Gateway

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

To change the Operation Mode:

1. From the left-hand menu, click on *Wizard*. The following page is displayed:
2. Click on the ratio of *Gateway* and then click on *Next>>*.

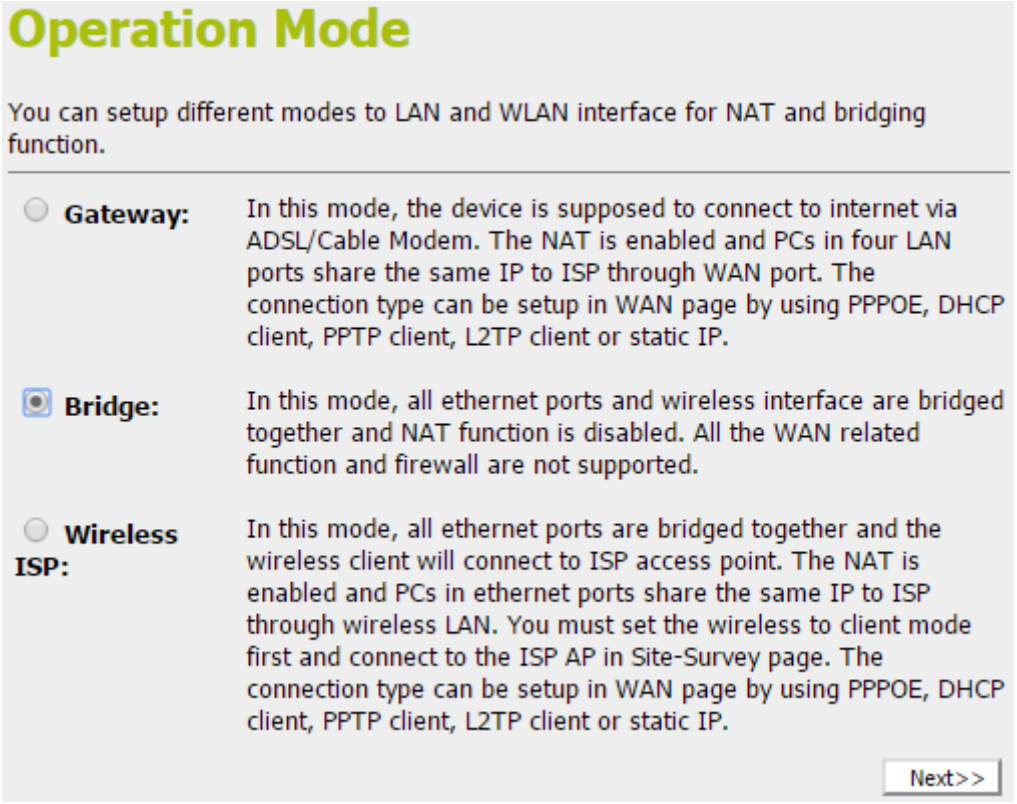


Bridge

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

To change the Operation Mode:

1. From the left-hand menu, click on *Wizard*. The following page is displayed:
2. Click on the ratio of *Bridge* and then click on *Next>>*.

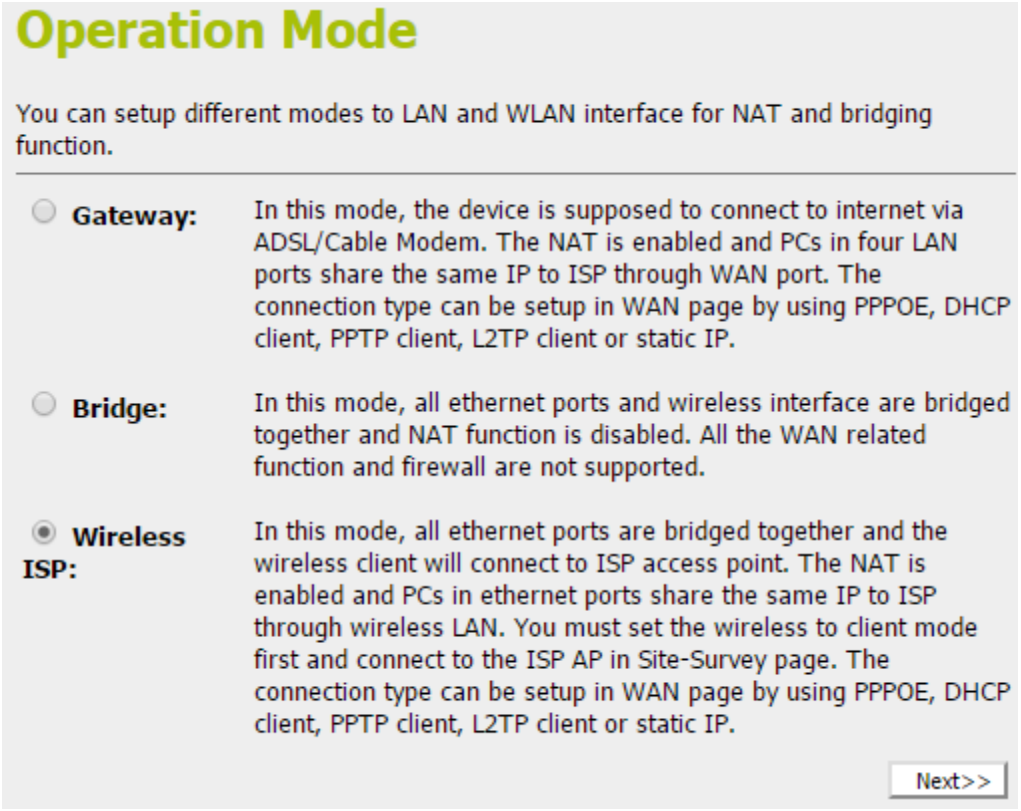


Wireless ISP

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

To change the Operation Mode:

3. From the left-hand menu, click on *Wizard*. The following page is displayed:
4. Click on the ratio of *Wireless ISP*.
5. Select WLAN1 for 5GHz or wlan2 for 2.4GHz from the WAN Interface drop-down list.
6. Click on *Next>>*.

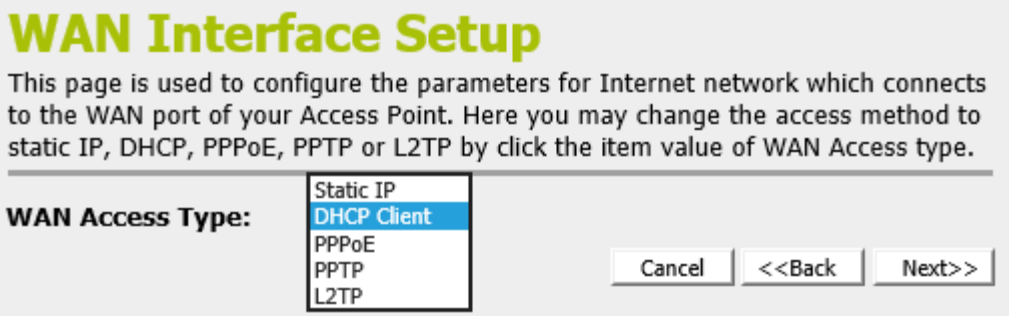


WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, *PPTP*or *L2TP* by click the item value of WAN Access type.

To change the WAN Access Type:

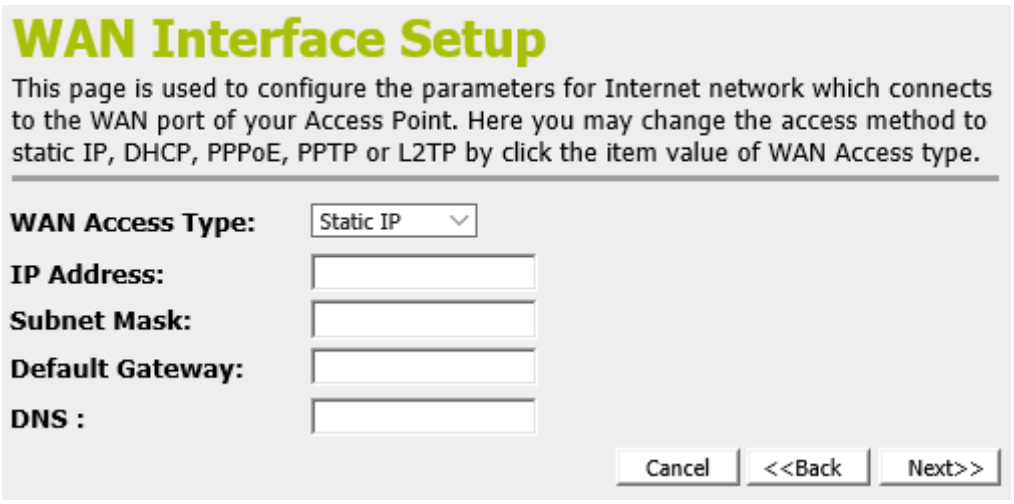
7. From the *WAN Access Type* drop-down list, select *Static IP, DHCP Client, PPPoE, PPTP, or L2TP*setting determined by your Network Administrator or ISP.
8. Click *Next>>*.



Static IP

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

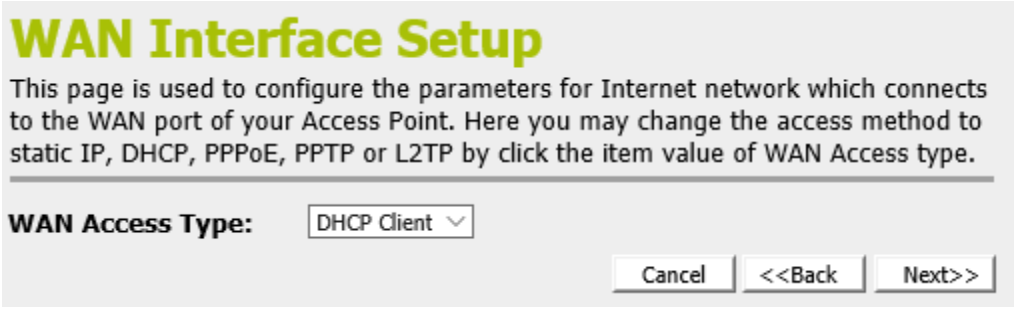
1. From the *WAN Access Type* drop-down list, select *Static IP* setting determined by your Network Administrator or ISP.
2. Enter *IP Address* for example 172.1.1.1.
3. Enter *Subnet Mask* for example 255.255.255.0.
4. Enter *Default Gateway* for example 172.1.1.254.
5. Enter *DNS* for example 172.1.1.254.
6. Click *Next>>*.



DHCP Client

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

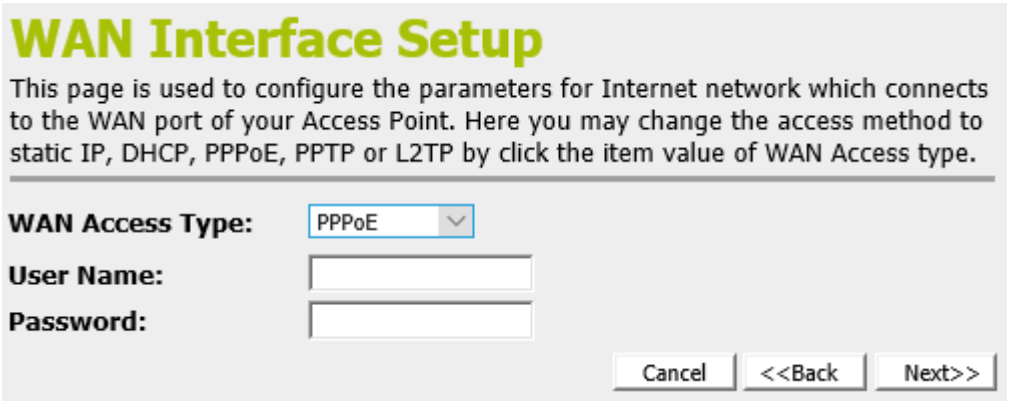
1. From the *WAN Access Type* drop-down list, select *DHCP Client* setting determined by your Network Administrator or ISP.
2. Click *Next>>*.



PPPoE

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

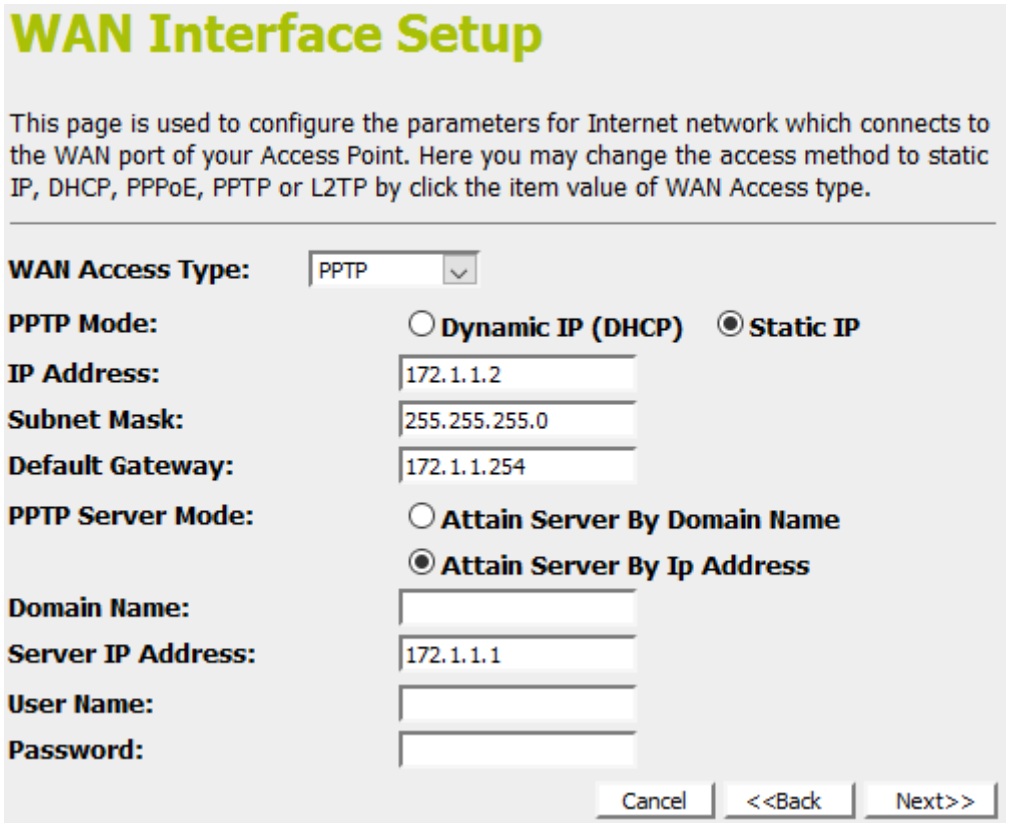
1. From the *WAN Access Type* drop-down list, select *PPPoE*setting determined by your Network Administrator or ISP.
2. Enter *User Name* for example 1234.
3. Enter *Password* for example 1234.
4. Click *Next>>*.



PPTP

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

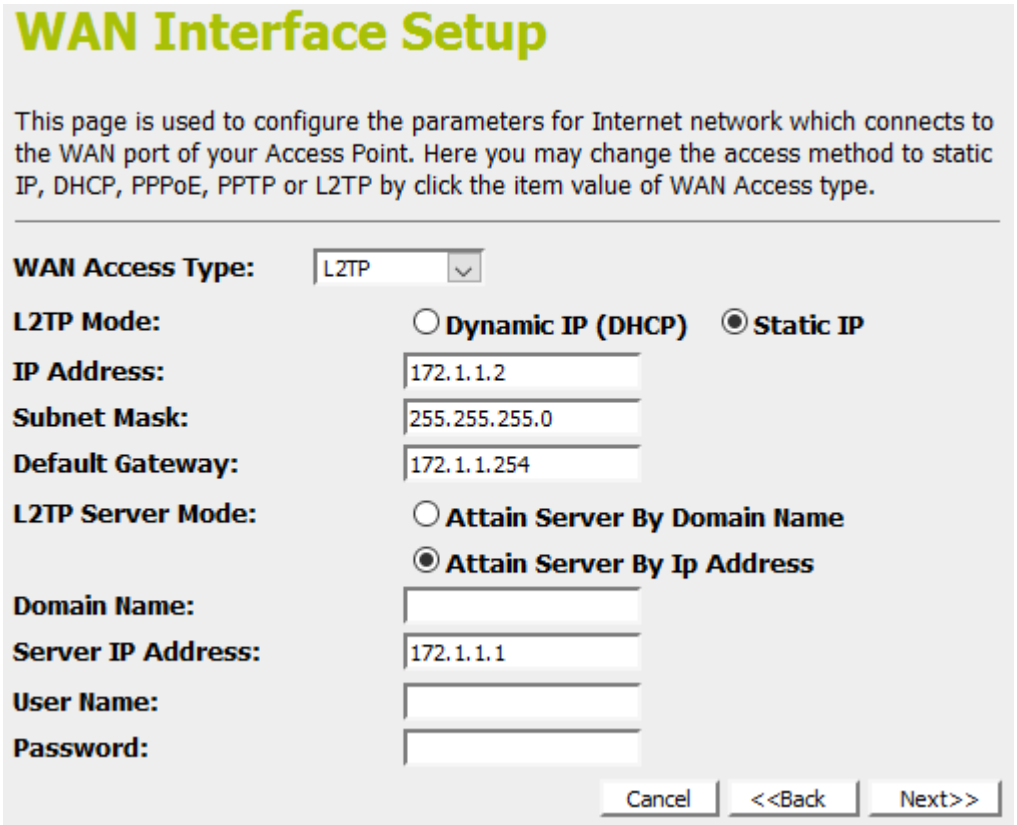
1. From the *WAN Access Type* drop-down list, select *PPTP* setting provided by your Network Administrator or ISP.
2. Click on the ratio of Dynamic IP (DHCP) or Static IP.
3. Enter *IP Address* for example 172.1.1.1 provided by your Network Administrator or ISP. (for Static IP only)
4. Enter *Subnet Mask* for example 255.255.0.0 provided by your Network Administrator or ISP. (for Static IP only)
5. Enter *Default Gateway* for example 172.1.1.254 provided by your Network Administrator or ISP. (for Static IP only)
6. Select PPTP Server Mode by Attain Server By Domain Name or Attain Server By Ip Address
7. Enter Server Domain Address for example 222.222.222.222 or www.example.com provided by your Network Administrator or ISP.
8. Enter *User Name* for example 1234 provided by your Network Administrator or ISP.
9. Enter *Password* for example 1234 provided by your Network Administrator or ISP.
10. Click *Next>>*.



L2TP

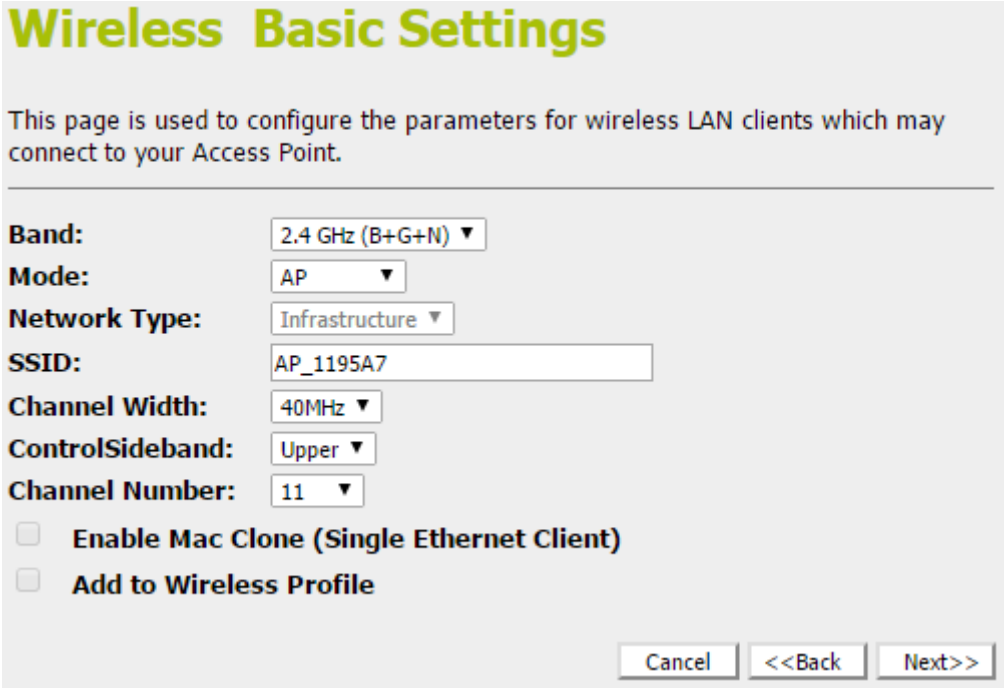
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using L2TP.

1. From the *WAN Access Type* drop-down list, select *L2TP* setting provided by your Network Administrator or ISP.
2. Click on the ratio of Dynamic IP (DHCP) or Static IP.
3. Enter *IP Address* for example 172.1.1.1 provided by your Network Administrator or ISP. (for Static IP only)
4. Enter *Subnet Mask* for example 255.255.0.0 provided by your Network Administrator or ISP. (for Static IP only)
5. Enter *Default Gateway* for example 172.1.1.254 provided by your Network Administrator or ISP. (for Static IP only)
6. Select L2TP Server Mode by Attain Server By Domain Name or Attain Server By Ip Address
7. Enter Server Domain Address for example 222.222.222.222 or www.example.com provided by your Network Administrator or ISP.
8. Enter *User Name* for example 1234 provided by your Network Administrator or ISP.
9. Enter *Password* for example 1234 provided by your Network Administrator or ISP.
10. Click *Next>>*.



Wireless Basic Settings

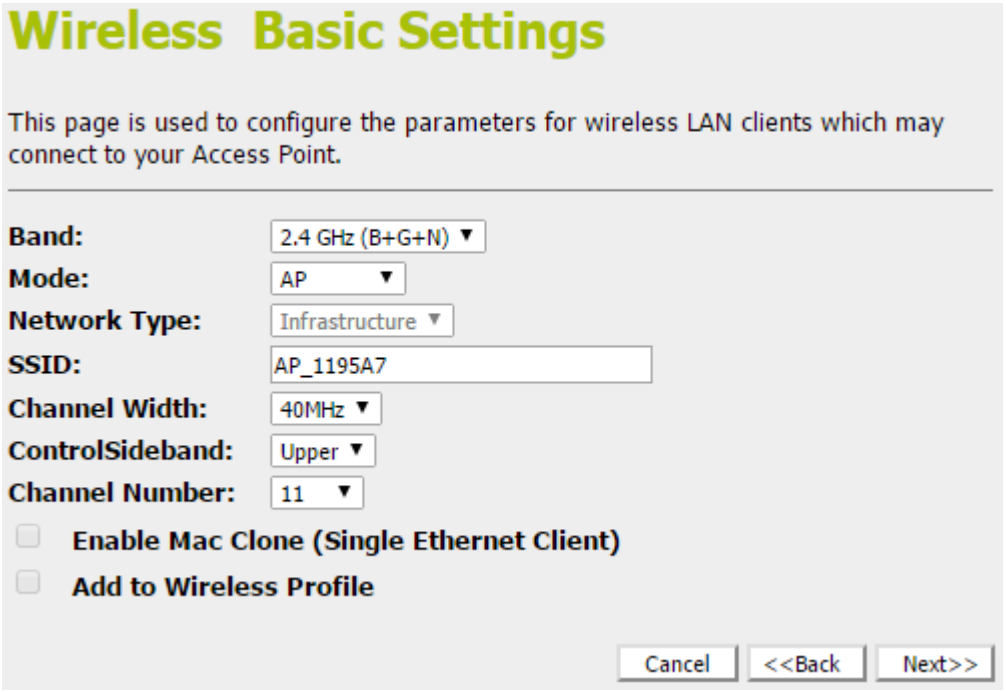
This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.



AP (Access Point)

Access Point is used to configure the parameters for wireless LAN clients who may connect to your Access Point.

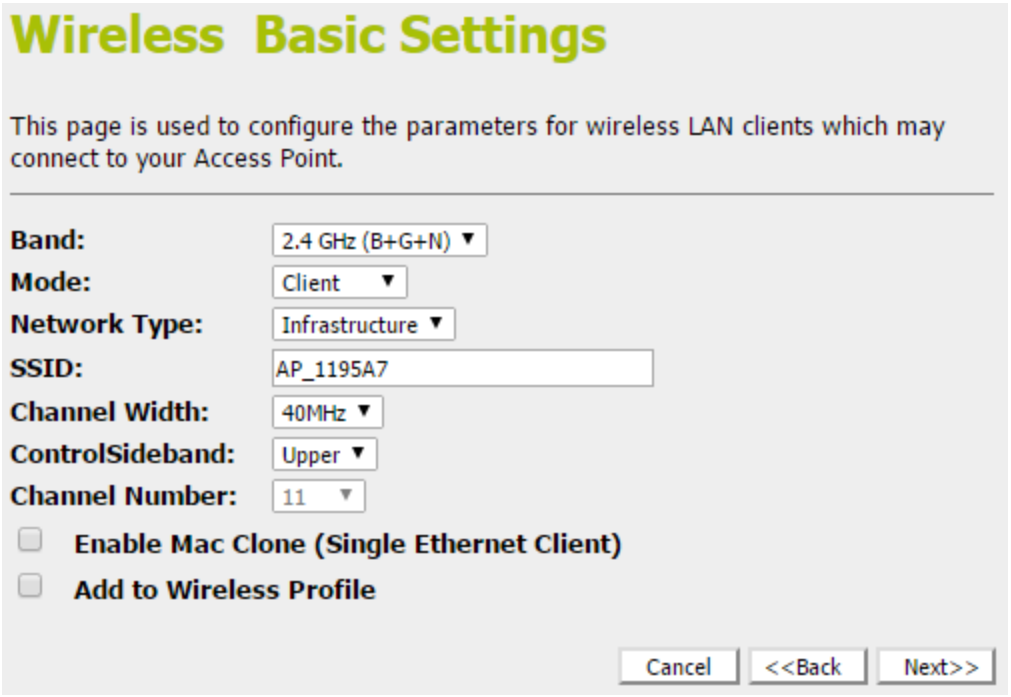
1. From the *Band* drop-down list, select a Band.
2. From the *Mode* drop-down list, select *AP* setting.
3. Enter *SSID* for example AP_1195A7.
4. From the *Channel Width* drop-down list, select a Channel Width.
5. From the *ControlSideband* drop-down list, select a ControlSideband.
6. From the *Channel Number* drop-down list, select a Channel Number.
7. Click *Next>>*.



Client

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

1. From the *Band* drop-down list, select a Band.
2. From the *Mode* drop-down list, select *Client* setting.
3. From the *Network Type* drop-down list, select a Type.
4. Enter *SSID* for example AP_1195A7.
5. Click *Next>>*.



WDS (Wireless Distribution System)

WDS stands for Wireless Distribution System. It enables the access points (APs) to be connected wirelessly. 802.11n WLAN AP Router can also provide you services of WDS.

Note

802.11n WLAN AP Router that supports WDS does not support security systems like WEP, WPA or WPA-Enterprise on a WDS network.

Sometimes you want to establish a multi-access point wireless network in your home or office, but you don't have Ethernet cabling running to the locations where you want to add the extra AP. After all, you may be using wireless because you don't have wires in place already.

One way to overcome this problem is to use a system built into Wireless Gateway that is known as Wireless Distribution System (WDS).

WDS basically creates a mesh network by providing a mechanism for access points to "talk" to each other as well as sending data to devices associated with them.

Note

WDS is based on some standardized 802.11 protocols, but there is no standardized way of implementing it that works across different AP and router vendors. So if you have a Wireless Gateway in one location and you want to create a WDS link to a other brand of router in another location (just to pick two brands at random), you probably won't be able to get it to work. You have your best luck when you use equipment from the same manufacturer.

Note

When you use WDS as a repeater system, as described below, it effectively halves the data rate for clients connected to Integrated Wireless Gateway. That's because every bit of data needs to be sent twice (data is received by the AP and then retransmitted).

To configure WDS, you need to modify some settings on each AP within thenetwork. Your exact steps (and the verbiage used) will vary from vendor tovendor. Generally, you'll see some settings like the following:

Main WDS station:

One of your WDS stations is the main base station forthe WDS network. This AP is connected directly to your Internet connection,or connected to your router via a wired connection. The main stationis the bridge to your Internet connection that all wireless trafficeventually flows through.

Repeater WDS stations:

In a simple, two-AP WDS network, the other“unwired” AP is a repeater. The repeater receives data from the mainbase station and relays the data to the wireless clients associated to therepeater station (and vice versa for data coming from the clients). If youhave more than two APs, remote APs may be repeaters, or they may berelays that provide an intermediate stopping point for data if therepeater is too far away from the main station to communicate.

When you configure your main or base WDS station, take note of the channelyou’re set to and the SSID or network name of your network. If your AP hasany kind of channel auto configuration function that changes channels basedon network conditions, be sure to disable this feature. If your main WDS stationis also your network’s router, make sure it’s set up to distribute IPaddresses in the network.

Note

Write down or otherwise take note of the MAC addresses of all of your WDS stations — many configuration software systems require you to know these addresses to make the configuration settings work. Write down the wireless MAC address (it’s often on a sticker) and not the Ethernet MAC address.

Turn on the WDS functionality in your main station (it’s often labeled WDS,or may say something like Enable This Base Station As a WDS Main BaseStation — that’s the wording Apple uses for their AirPort Extreme products).When you turn on this functionality, the configuration software may ask youto identify the remote repeater(s). Have the MAC addresses of thoserepeaters handy in case you need them.

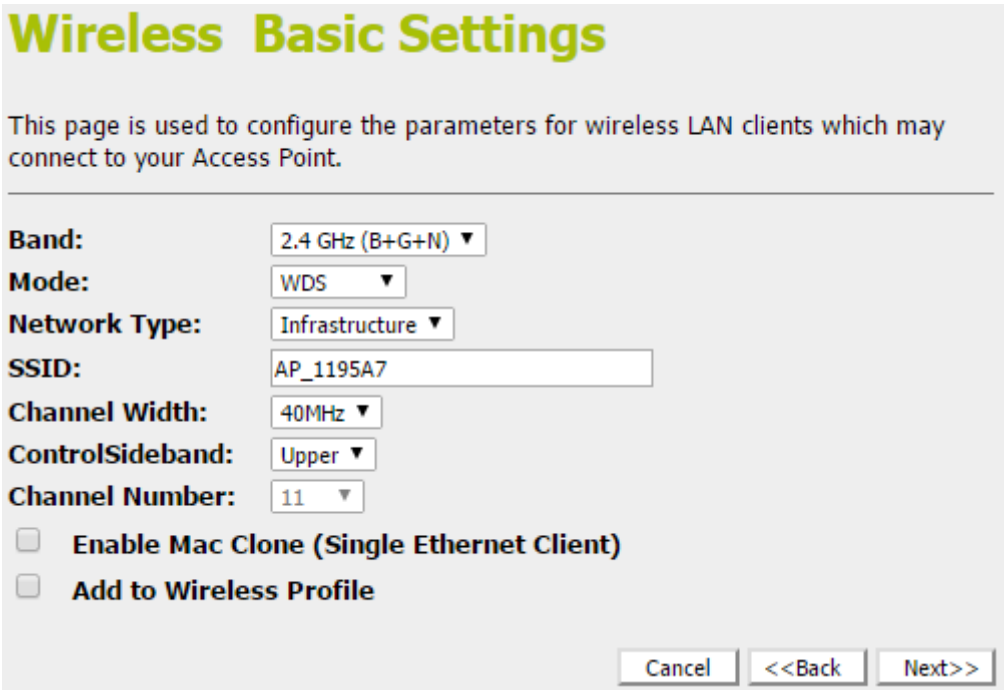
Depending upon how your software works, you may have to separatelyaccess the configuration software on the remote repeater APs to turn onWDS. Here are a few things to remember:

- You need to assign any other WDS stations to the same channel that yourmain base station is using. This is counterintuitive to many folks who havehad the 802.11b/g “use channels 1, 6, and 11 and keep your APs on differentchannels” mantra driven into their heads for a long time!

- You set the SSID of the remote location(s) using either a unique nameor by using the same SSID as you use for your main base station.(Whoa, our heads just exploded!) Using the same SSID (a “roaming” network)is pretty cool. You associate with one AP one time and then yourPC or Mac can associate with any AP on your WDS network without youhaving to do anything — it’s more seamless this way. But remember, youdon’t have to do this — you can give each AP a unique SSID and justconfigure your computer to associate with them according to yourpreference.
- Make sure you turn off any routing or DHCP functionality in the remoterepeater stations. All of this functionality should be performed in themain base station or the network’s main router.

WDS (Wireless Distribution System) only

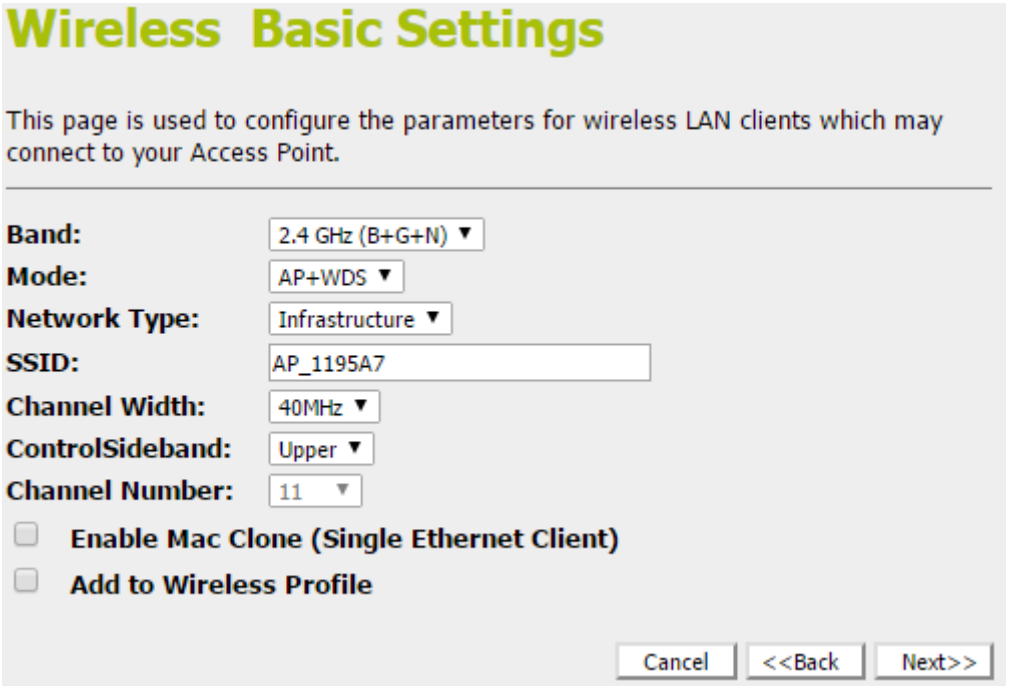
1. From the *Band* drop-down list, select a Band.
2. From the *Mode* drop-down list, select *WDS* setting.
3. From the *Channel Width* drop-down list, select a Channel Width.
4. From the *ControlSideband* drop-down list, select a ControlSideband.
5. From the *Channel Number* drop-down list, select a Channel Number.
6. Click *Next>>*.



AP (Access Point) + WDS (Wireless Distribution System)

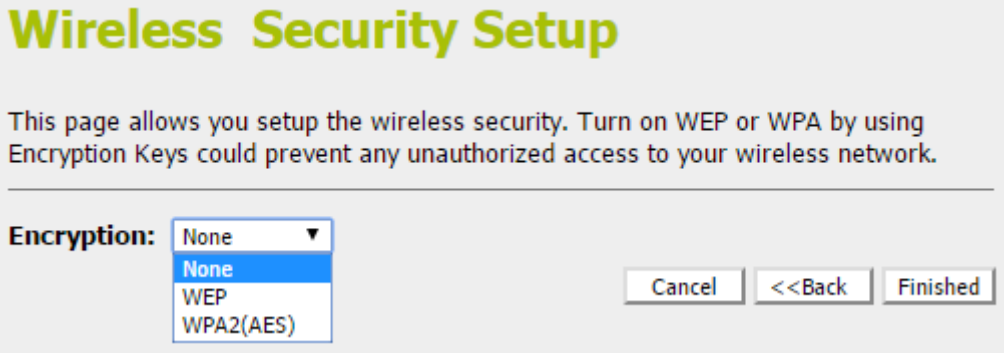
Access Point is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

1. From the *Band* drop-down list, select a Band.
2. From the *Mode* drop-down list, select *AP+WDS* setting.
3. Enter *SSID* for example AP_5G.
4. From the *Channel Width* drop-down list, select a Channel Width.
5. From the *ControlSideband* drop-down list, select a ControlSideband.
6. From the *Channel Number* drop-down list, select a Channel Number.
7. Click *Next>>*.



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.



You can protect your wireless data from potential *eavesdroppers* by encrypting wireless data transmissions. An eavesdropper might set up a compatible wireless adapter within range of your device and attempt to access your network. Data encryption is the translation of data into a form that cannot be easily understood by unauthorized users.

There are two methods of wireless security to choose from:

- *Wired Equivalent Privacy (WEP)*; data is encrypted into blocks of either 64 bits length or 128 bits length. The encrypted data can only be sent and received by users with access to a private network key. Each PC on your wireless network must be manually configured with the same key as your device in order to allow wireless encrypted data transmissions. Eavesdroppers cannot access your network if they do not know your private key. WEP is considered to be a low security option.
- *Wi-Fi Protected Access (WPA)*; provides a stronger data encryption method (called Temporal Key Integrity Protocol (TKIP)). It runs in a special, easy-to-set-up home mode called Pre-Shared Key (PSK) that allows you to manually enter a pass phrase on all the devices in your wireless network. WPA data encryption is based on a WPA master key. The master key is derived from the pass phrase and the network name (SSID) of the device.

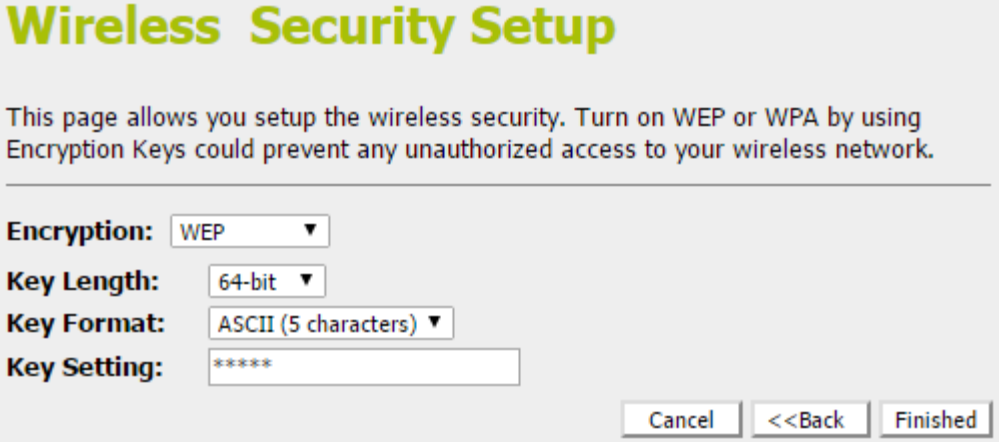
To configure security, choose one of the following options:

- If you do not want to use Wireless Network security, From the *Encryption* drop-down list, select *None* setting and then click *Finished.None* is the default setting, but you are **strongly recommended** to use wireless network security on your device.
- If you want to use WEP 64bit ASCII (5 characters) data encryption, follow the instructions in *Configuring 64bit ASCII (5 characters) encryption*.
- If you want to use WEP 64bit Hex (10 characters) data encryption, follow the instructions in *Configuring WEP64bit Hex (10 characters)security*.
- If you want to use WEP 128bit ASCII (5 characters) data encryption, follow the instructions in *Configuring WEP 128bit ASCII (5 characters)security*.
- If you want to use WEP 128bit Hex (10 characters) data encryption, follow the instructions in *Configuring WEP 128bit Hex (10 characters)security*.
- If you want to use WPA2(AES) - *Wi-Fi Protected Access 2(AES) Passphrase encryption*, follow the instructions in *Configuring WPA2 (AES) Passphrase security*.
- If you want to use WPA2 (AES) - *Wi-Fi Protected Access 2(AES) HEX (64 characters) encryption*, follow the instructions in *Configuring WPA2 (AES) HEX (64 characters) security*.
- If you want to use WPA Mixed- *Wi-Fi Protected Access 2(Mixed) Passphrase encryption*, follow the instructions in *Configuring WPA2 (Mixed) Passphrase security*.
- If you want to use WPA Mixed- *Wi-Fi Protected Access 2(Mixed) HEX (64 characters) encryption*, follow the instructions in *Configuring WPA2 (Mixed) HEX (64 characters) security*.

Configuring WEP64bit ASCII (5 characters) security

The example set in this section is for 64bit encryption.

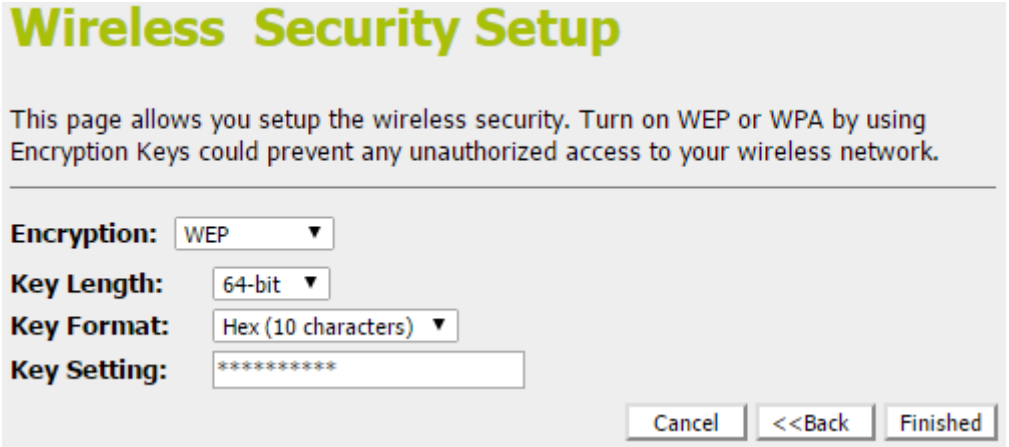
1. From the *Encryption* drop-down list, select *WEP* setting.
2. From the *Key Length* drop-down list, select *64-bit* setting.
3. From the *Key Format* drop-down list, select *ASCII (5 characters)* setting.
4. Type the *Key Setting*.
5. Click *Next>>*.



Configuring WEP64bit Hex (10 characters)security

The example set in this section is for 64bit encryption.

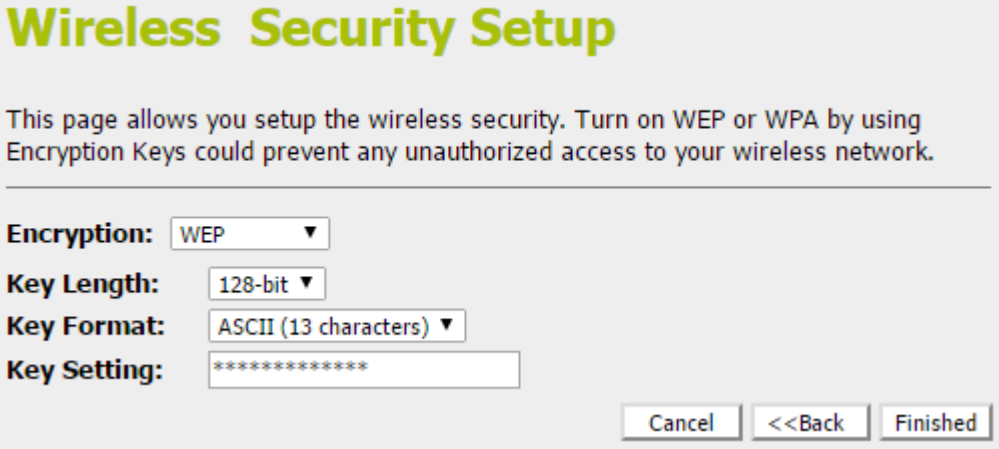
6. From the *Encryption* drop-down list, select *WEP* setting.
7. From the *Key Length* drop-down list, select *64-bit* setting.
8. From the *Key Format* drop-down list, select *Hex (10 characters)*setting.
9. Type the *Key Setting*.
10. Click *Next>>*.



Configuring WEP 128bit ASCII (13 characters) security

The example set in this section is for 128bit encryption.

1. From the *Encryption* drop-down list, select *WEP* setting.
2. From the *Key Length* drop-down list, select *128-bit* setting.
3. From the *Key Format* drop-down list, select *ASCII (13 characters)* setting.
4. Type the *Key Setting*.
5. Click *Next>>*.



Configuring WEP 128bit Hex (26 characters)security

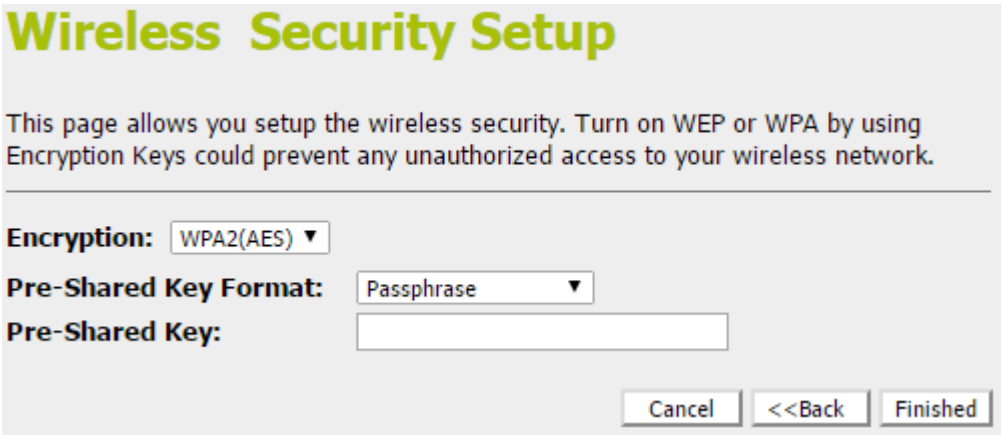
The example set in this section is for 128bit encryption.

6. From the *Encryption* drop-down list, select *WEP* setting.
7. From the *Key Length* drop-down list, select *128-bit* setting.
8. From the *Key Format* drop-down list, select *Hex (26 characters)*setting.
9. Type the *Key Setting*.
10. Click *Next>>*.

Configuring WPA2 (AES) Passphrase security

The example set in this section is for WPA2 (AES) Passphrase encryption.

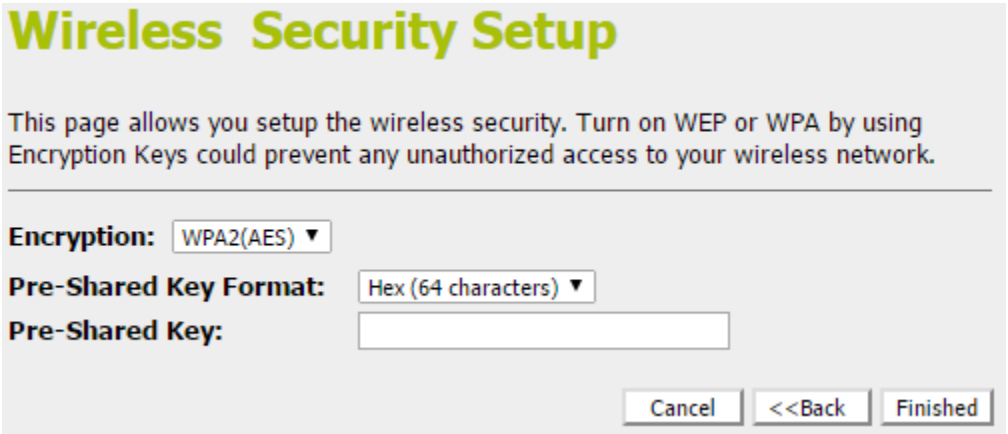
1. From the *Encryption* drop-down list, select *WPA2 (AES)* setting.
2. From the *Pre-Shared Key Format* drop-down list, select *Passphrase* setting.
3. Type the *Pre-Shared Key*.
4. Click *Next>>*.



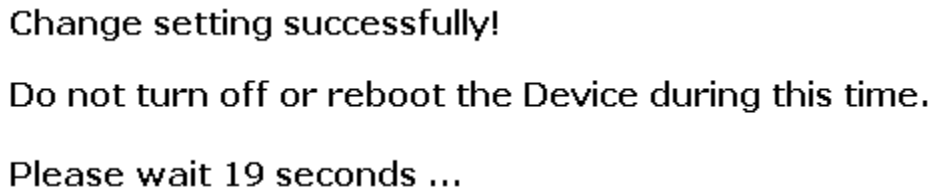
Configuring WPA2 (AES) HEX (64 characters)security

The example set in this section is for WPA2 (AES) HEX (64 characters) encryption.

5. From the *Encryption* drop-down list, select *WPA2 (AES)* setting.
6. From the *Pre-Shared Key Format* drop-down list, select *HEX (64 characters)*setting.
7. Type the *Pre-Shared Key*.
8. Click *Finished*.



9. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...



9 Operation Mode

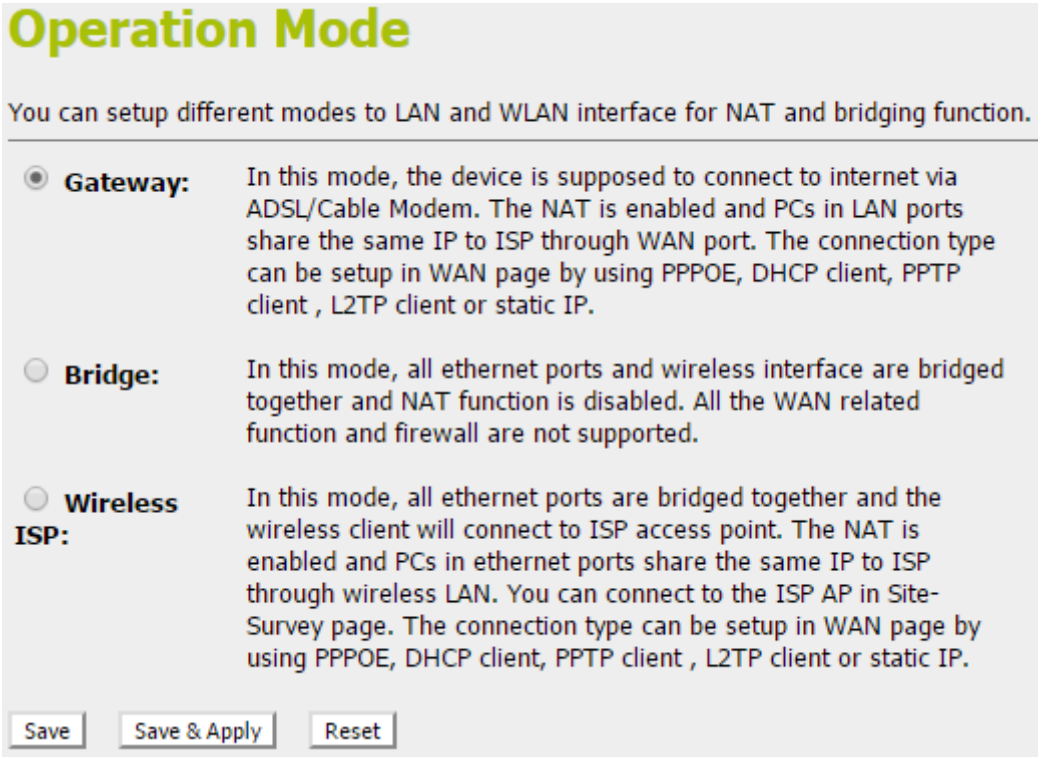
This chapter describes how to configure the way that your device connects to the Internet. There are Three options of Operation Mode: Gateway, Bridgeand Wireless ISP.

Setting Operation Mode

To change the Operation Mode:

1. From the head menu, click on *SETUP*.

2. From the left-hand *Operation Mode* menu. The following page is displayed:
3. Click on the ratio of *Gateway*, *Bridge*or *Wireless ISP* and then click on *Save & Apply* to active it.



10 Wireless Network - WLAN1

This chapter assumes that you have already set up your Wireless PCs and installed a compatible Wireless card on your device. See *Configuring Wireless PCs*.

Basic Settings

The *Wireless Network* page allows you to configure the Wireless features of your device. To access the *Wireless NetworkBasic Settings* page:

1. From the head menu, click on *WLAN1*.

2. From the left-hand *Wireless*menu, click on*Basic Settings*.
   The following page is displayed:

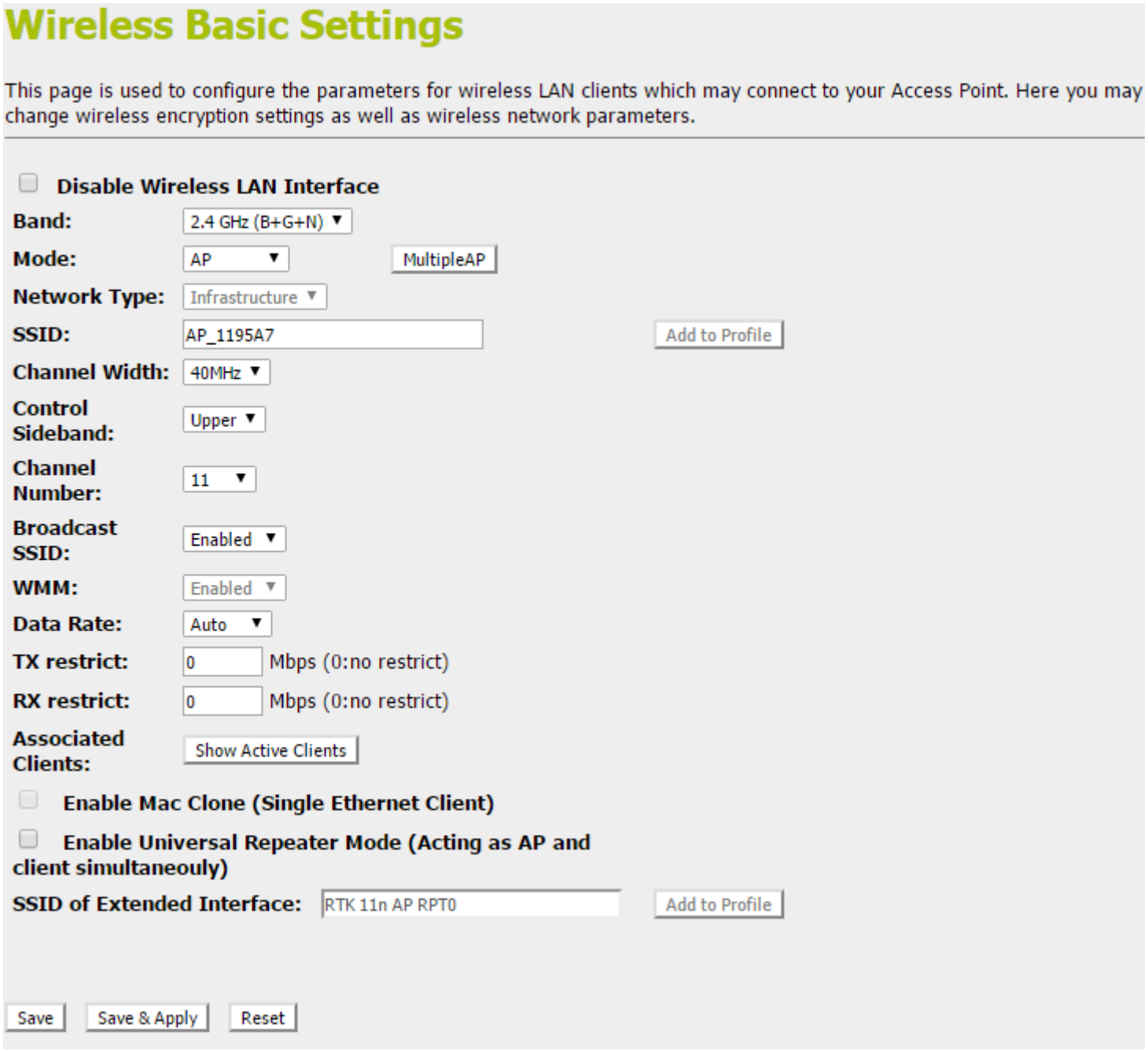


Figure 8: Wireless Network page

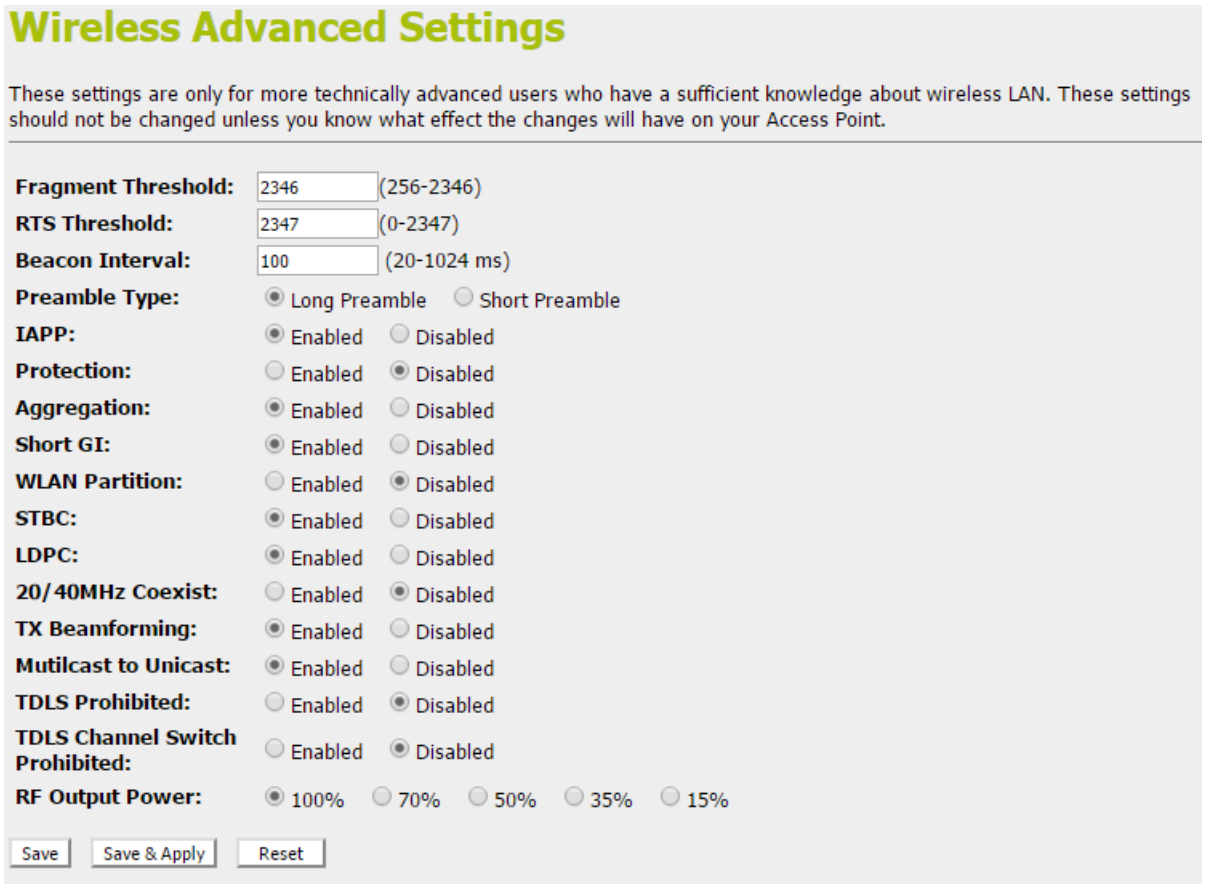
Field	Description
Disable Wireless LAN Interface	**Enable/Disable the Wireless LAN Interface.** **Default: Disable**
Band	**Specify the WLAN Mode**
Mode	**Configure the Wireless LAN Interface to AP, Client, WDS orAP + WDS mode**
Network Type	**Configure the Network Type to Infrastructure or Ad hoc.**
SSID	**Specify the network name.** **Each Wireless LAN network uses a unique Network Name to identify the network. This name is called the Service Set Identifier (SSID). When you set up your wireless adapter, you specify the SSID. If you want to connect to an existing network, you must use the name for that network. If you are setting up your own network you can make up your own name and use it on each computer. The name can be up to 20 characters long and contain letters and numbers.**
Channel Width	**Choose a Channel Width from the pull-down menu.**
Control Sideband	**Choose a Control Sideband from the pull-down menu.**
Channel Number	**Choose a Channel Number from the pull-down menu.**
Broadcast SSID	**Broadcast or Hide SSID to your Network.** **Default: Enabled**
WMM	**Enable/disable the Wi-Fi Multimedia (WMM) support.**
Data Rate	**Select the Data Rate from the drop-down list**
Associated Clients	**Show Active Wireless Client Table** **This table shows the MAC address, transmission, receiption packet counters and encrypted status for each associated wireless client.**
Enable Mac Clone (Single Ethernet Client)	**Enable Mac Clone (Single Ethernet Client)**
Enable Universal Repeater Mode	**Acting as AP and client simultaneously**
SSID of Extended Interface	**When mode is set to "AP" and URM (Universal Repeater Mode) is enabled, user should input SSID of another AP in the field of "SSID of Extended Interface". Please note, the channel number should be set to the one, used by another AP because 8186 will share the same channel between AP and URM interface (called as extended interface hereafter).**

Advanced Settings

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

1. From the head menu, click on *WLAN1*.

2. From the left-hand menu, click on *Advanced Settings*. The following page is displayed:



Field	Description
Fragment Threshold	**When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium.** **The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages.**
RTS Threshold	**RTS stands for "Request to Send". This parameter controls what size data packet the low level RF protocol issues to an RTS packet. The default is 2347.**
Beacon Interval	**Choosing beacon period for improved response time for wireless http clients.**

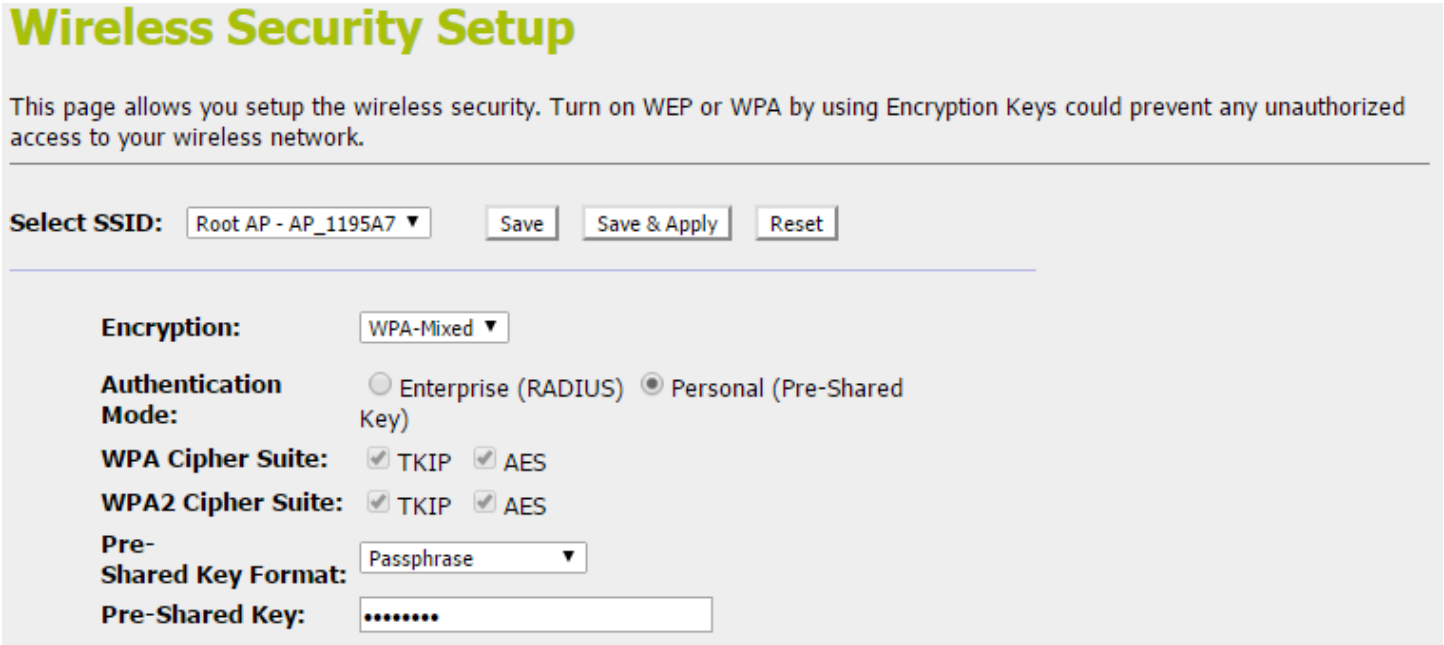
IAPP	**Disable or Enable IAPP**
Protection	**A protection mechanism prevents collisions among 802.11g nodes.**
Aggregation	**Disable or Enable Aggregation**
Short GI	**Disable or Enable Short GI**
WLAN Partition	**Disable or Enable WLAN Partition**
STBC	**Disable or Enable STBC**
LDPC	**Disable or Enable LDPC**
TX Beamforming	**Disable or Enable TX Beamforming**
RF Output Power	**TX Power measurement.**

Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network. To access the *Wireless NetworkSecurity*page:

1. From the head menu, click on *WLAN1*.

2. From the left-hand menu, click on *Security*. The following page is displayed:



Field	Description
Select SSID	**Select the SSID**
Encryption	**Configure the Encryption to Disable, WEP, WPA , WPA2 or WPA-Mixed**
Use 802.1x Authentication	**Use 802.1x Authentication by WEP 64bits or WEP 128bits**
Authentication	**Configure the Authentication Mode to Open System, Shared Key or Auto**
Key Length	**Select the Key Length 64-bit or 128-bit**
Key Format	**Select the Key Format ASCII (5 characters), Hex (10 characters), ASCII (13 characters) or Hex (26 characters)**
Encryption Key	**Enter the Encryption Key**
WPA Authentication Mode	**Configure the WPA Authentication Mode to Enterprise (RADIUS) or Personal (Pre-Shared Key)**
WPA Cipher Suite	**Configure the WPA Cipher Suite to AES**

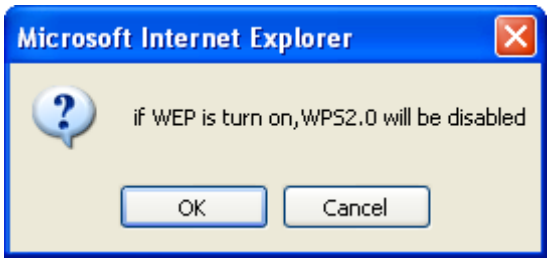
Field	Description
WPA2 Cipher Suite	**Configure the WPA2 Cipher Suite to AES**
Pre-Shared Key Format	**Configure the Pre-Shared Key Format to Passphrase or HEX (64 characters)**
Pre-Shared Key	**Type the Pre-Shared Key**
Enable Pre-Authentication	**According to some of the preferred embodiments, a method for proactively establishing a security association between a mobile node in a visiting network and an authentication agent in another network to which the mobile node can move includes: negotiating pre-authentication using a flag in a message header that indicates whether the communication is for establishing a pre-authentication security association; and one of the mobile node and the authentication agent initiating pre-authentication by transmitting a message with the flag set in its message header, and the other of the mobile node and the authentication agent responding with the flag set in its message header only if it supports the pre-authentication. Enable/disable pre-authentication support. Default: disable.**
Authentication RADIUS Server	**Port: Type the port number of RADIUS Server** **IP address: Type the IP address of RADIUS Server** **Password: Type the Password of RADIUS Server**

WEP + Encryption Key

WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed.

3. From the *Encryption* drop-down list, select *WEP* setting.
4. From the *Key Length*drop-down list, select *64-bit* or *128-bit* setting.
5. From the *Key Format* drop-down list, select *ASCII (5 characters),Hex (10 characters), ASCII (13 characters)* or *Hex (26 characters)*setting.
6. Enter the *Encryption Key* value depending on selected ASCII or Hexadecimal.
7. Click *Save & Apply* button.

8. Click *OK* button.

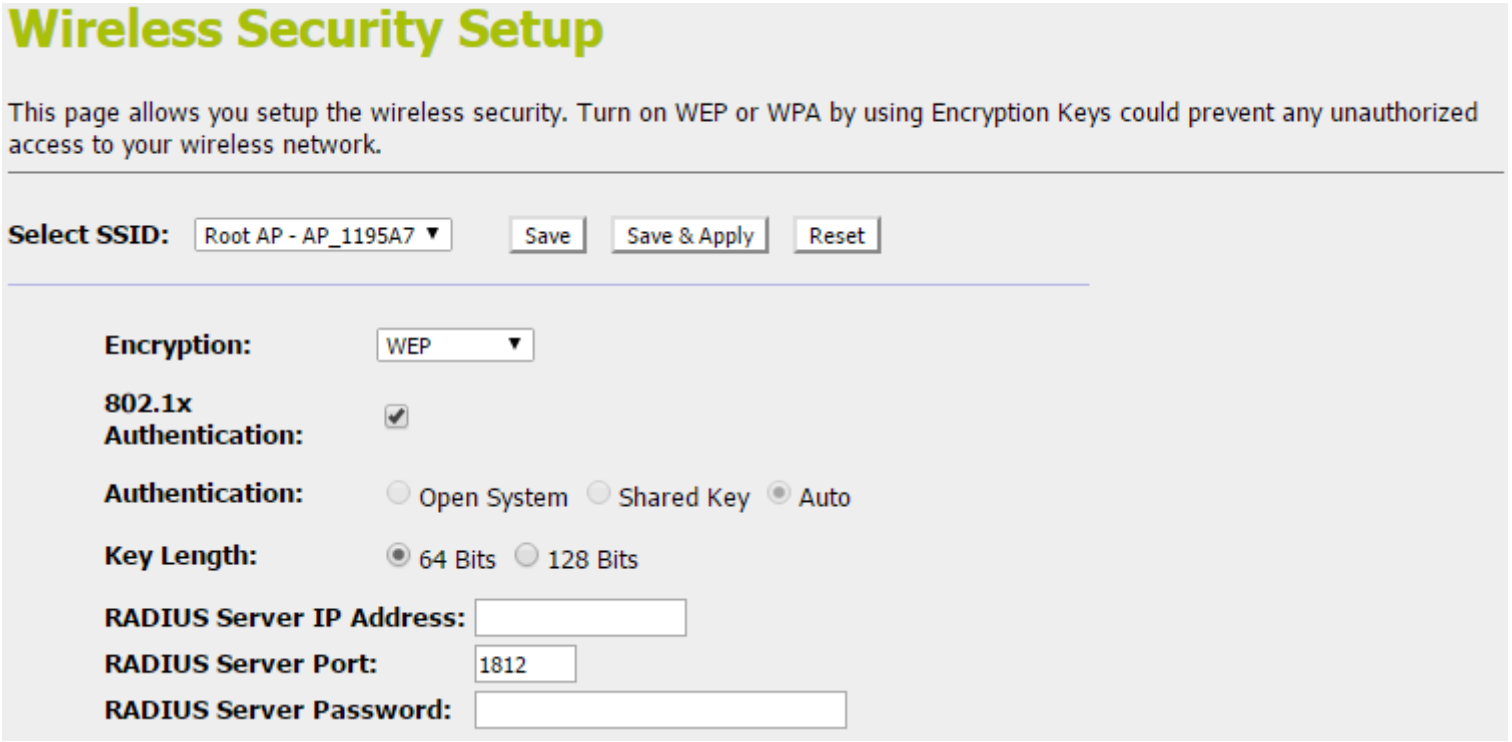


9. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

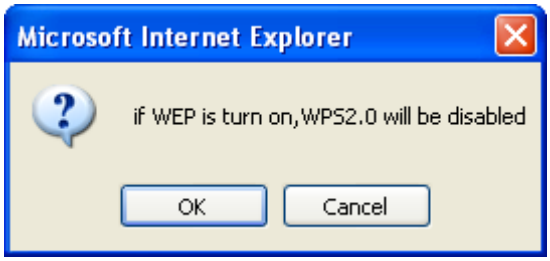
WEP + Use 802.1x Authentication

WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed.

1. From the *Encryption* drop-down list, select *WEP* setting.
2. Check the option of *Use 802.1x Authentication.*
3. Click on the ratio of *WEP 64bits* or *WEP 128bits*.
4. Enter the *Port*, *IP Address* and*Password* of RADIUS Server:
5. Click *Save & Apply* button.



6. Click *OK* button.



7. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

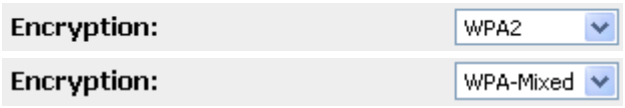
WPA2/WPA Mixed + Personal (Pre-Shared Key)

Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless (Wi-Fi)

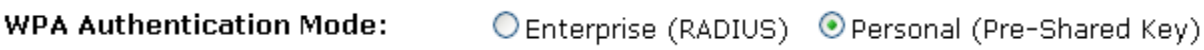
computer networks. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues:

- Either WPA or WPA2 must be enabled and chosen in preference to WEP. WEP is usually presented as the first security choice in most installation instructions.
- In the "Personal" mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.

1. From the *Encryption* drop-down list, select *WPA2* or *WPA Mixed*setting.

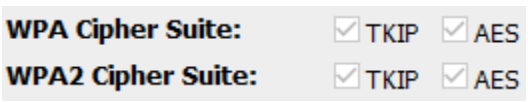


2. Click on the ratio of *Personal (Pre-Shared Key)*.



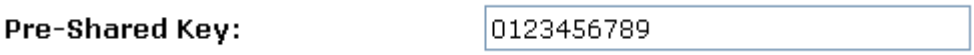
3. Check the option of *TKIP* and/or *AES* in *WPA2 Cipher Suite* if your Encryption is *WPA2*:

4. Check the option of *TKIP* and/or *AES* in *WPA2 Cipher Suite* if your Encryption is *WPA Mixed*:

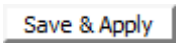


5. From the *Pre-Shared Key Format* drop-down list, select *Passphrase* or *Hex (64 characters)* setting.

6. Enter the *Pre-Shared Key* depending on selected *Passphrase* or *Hex (64 characters)*.



7. Click on *Save & Apply* button to confirm and return.



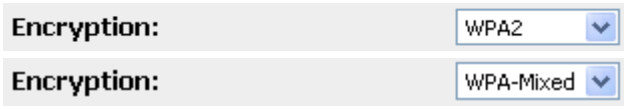
8. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

WPA2/WPA Mixed + Enterprise (RADIUS)

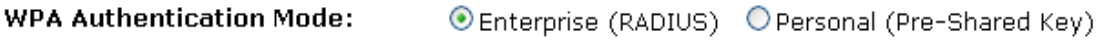
Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless (Wi-Fi) computer networks. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues:

- Either WPA or WPA2 must be enabled and chosen in preference to WEP. WEP is usually presented as the first security choice in most installation instructions.
- In the "Personal" mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.

1. From the *Encryption* drop-down list, select *WPA2* or *WPA Mixed* setting.

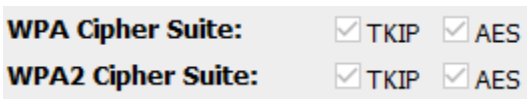


2. Click on the ratio of *Enterprise (RADIUS)*.

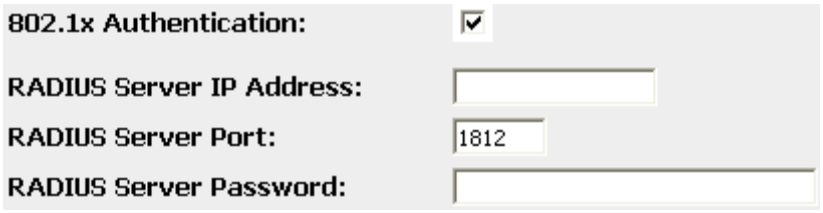


3. Check the option of *TKIP* and/or *AES* in *WPA2 Cipher Suite* if your Encryption is *WPA2*:

4. Check the option of *TKIP* and/or *AES* in *WPA/WPA2 Cipher Suite* if your Encryption is *WPA Mixed*:



5. Enter the *Port*, *IP Address* and*Password* of RADIUS Server:



6. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

Access Control

For security reason, using MAC ACL's (MAC Address Access List) creates another level of difficulty to hacking a network. A MAC ACL is created and distributed to AP so that only authorized NIC's can connect to the network. While MAC address spoofing is a proven means to hacking a network this can be used in conjunction with additional security measures to increase the level of complexity of the network security decreasing the chance of a breach.

MAC addresses can be add/delete/edit from the ACL list depending on the MAC Access Policy.

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point. To access the *Wireless NetworkAccess Control*page:

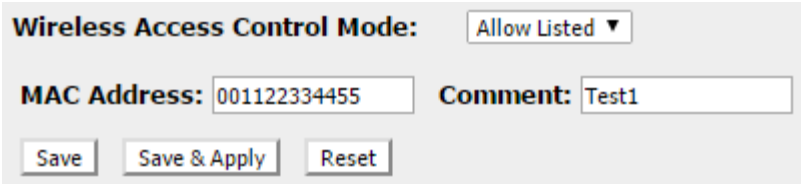
1. From the head menu, click on *WLAN1*.

2. From the left-hand menu, click on *Access Control*. The following page is displayed:

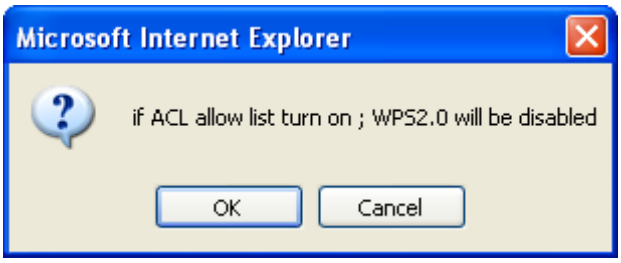
Allow Listed

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point.

1. From the Wireless Access Control Mode drop-down list, select Allowed Listedsetting.
2. Enter the *MAC Address*.
3. Enter the *Comment*.
4. Click *Save & Apply* button.

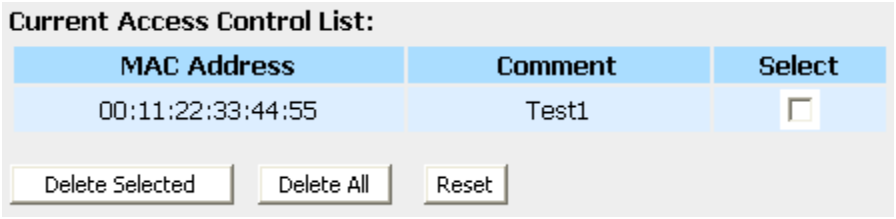


5. Click *OK* button.



6. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

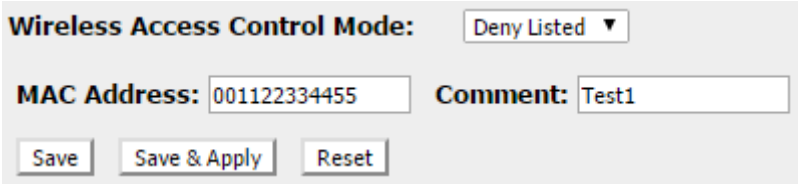
7. The MAC Address that you created has been added in the *Current Access Control List*.



Deny Listed

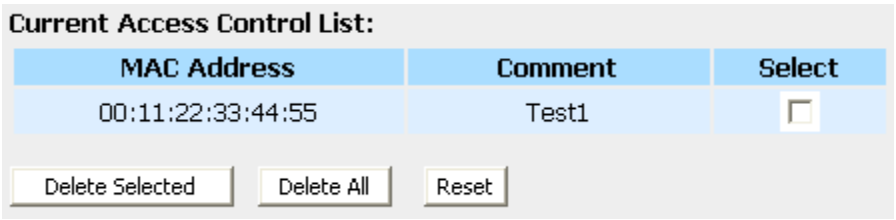
When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

1. From the Wireless Access Control Mode drop-down list, select *Deny Listed*setting.
2. Enter the *MAC Address*.
3. Enter the *Comment*.
4. Click *Save & Apply* button.



5. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

6. The MAC Address that you created has been added in the *Current Access Control List*.

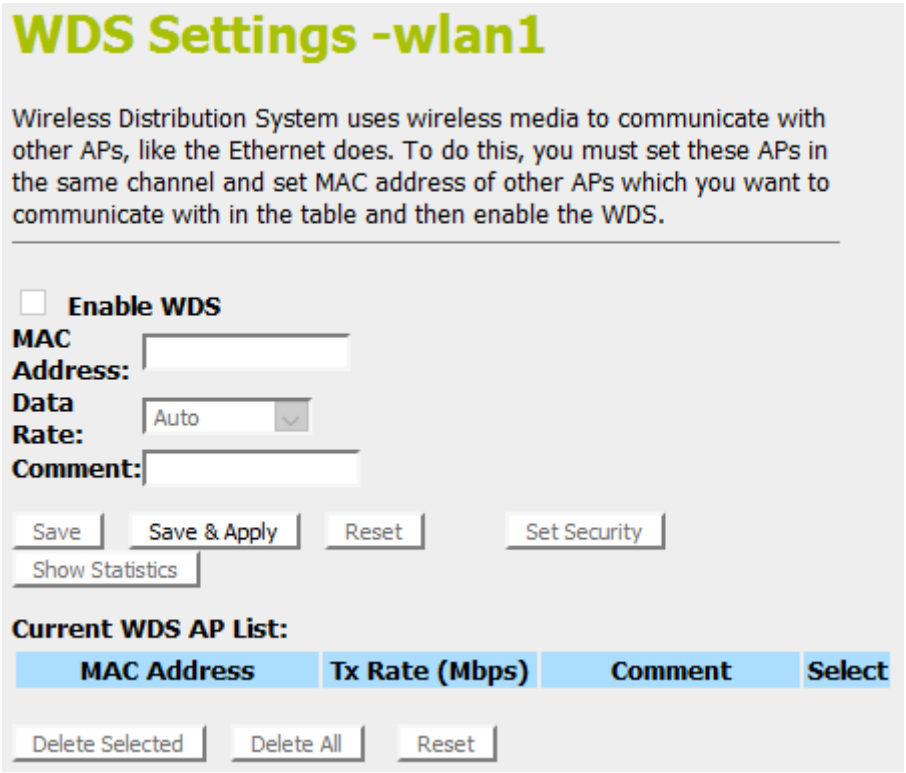


WDS settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS. To access the *Wireless NetworkWDS settings*page:

1. From the head menu, click on *WLAN1*.

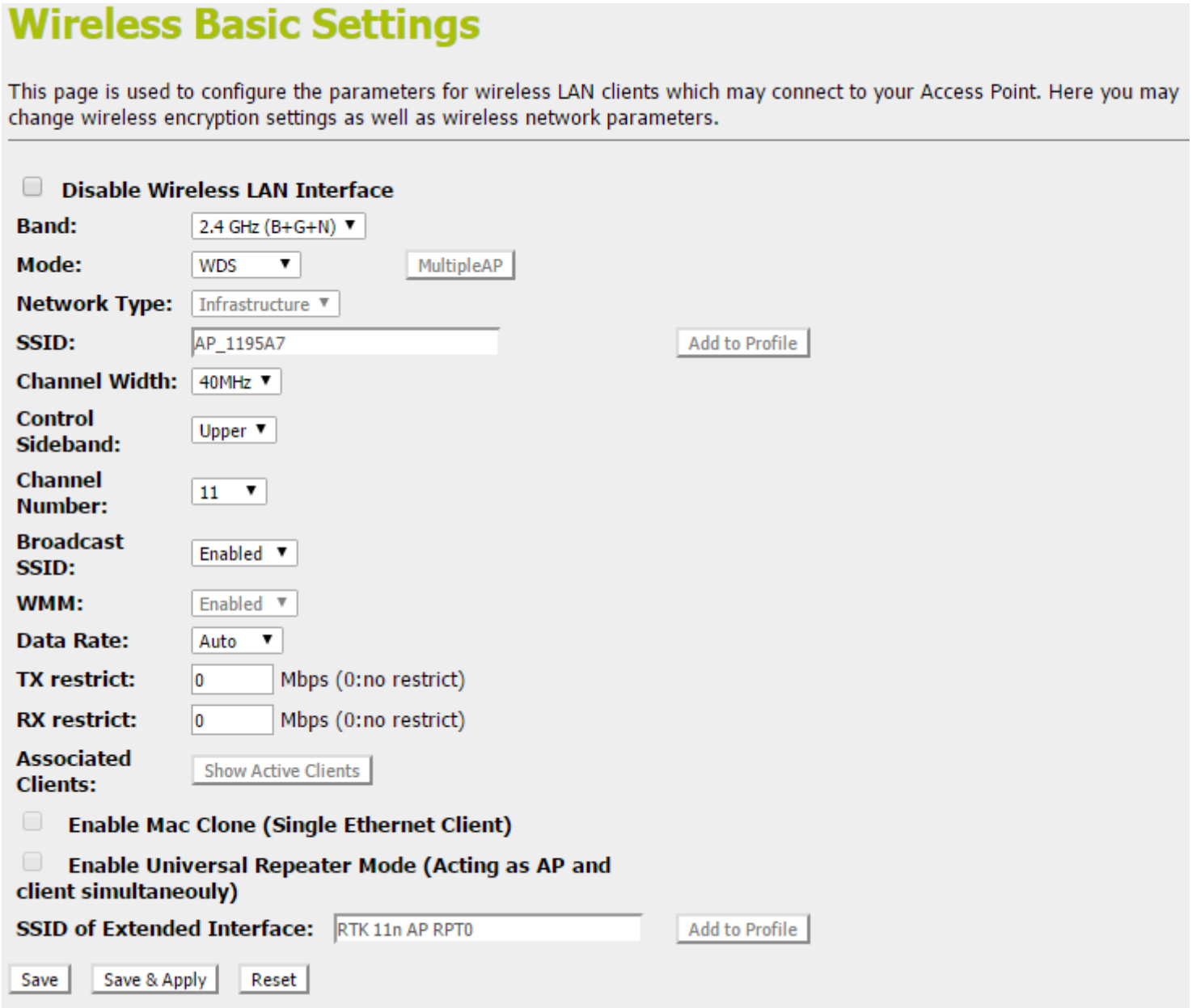
2. From the left-hand menu, click on *WDS settings*. The following page is displayed:



ConfigureWDS (Wireless Distribution System) only

1. From the head menu, click on *WLAN1*.

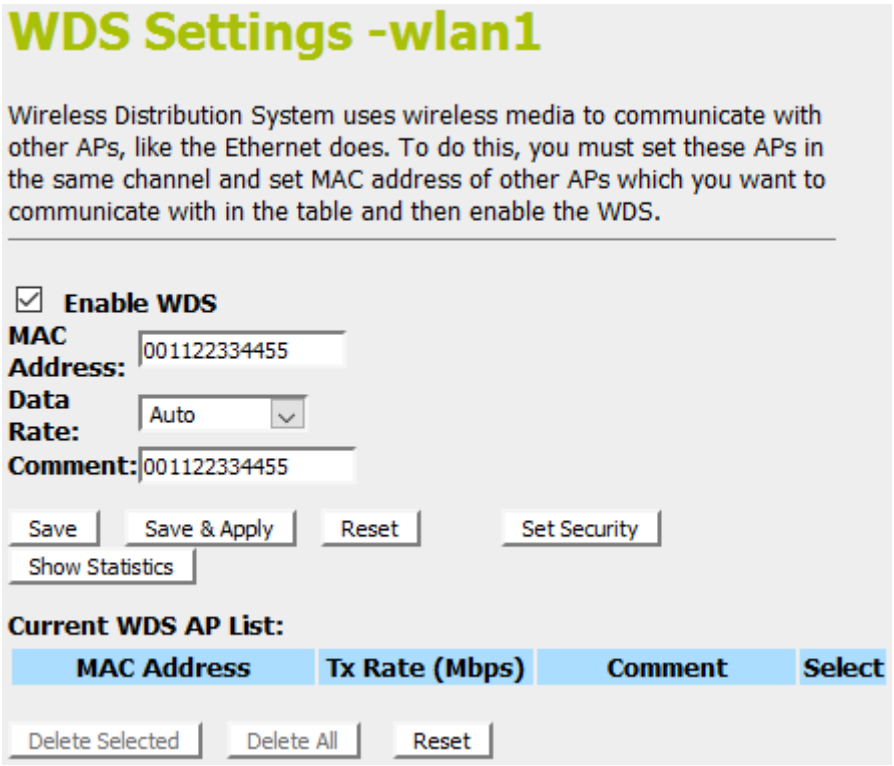
2. From the left-hand menu, click on *Basic Settings*.
3. From the *Mode* drop-down list, select *WDS.*
4. From the *Channel Number* drop-down list, select a Channel.
5. Click *Save & Apply* button.



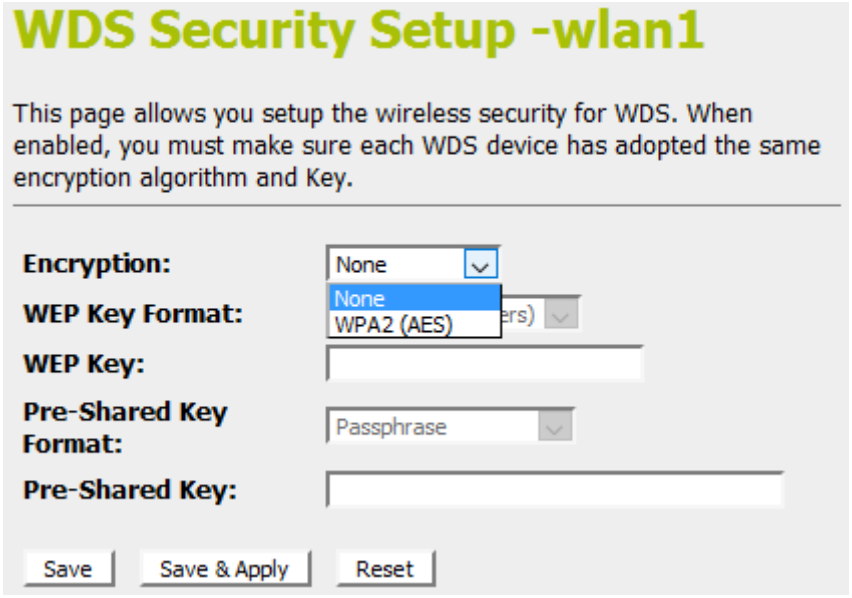
6. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

7. From the head menu, click on *WLAN1*.

8. From the left-hand menu, click on *WDS settings*.
9. Check on the option*Enable WDS*.
10. Click the *Set Security*.



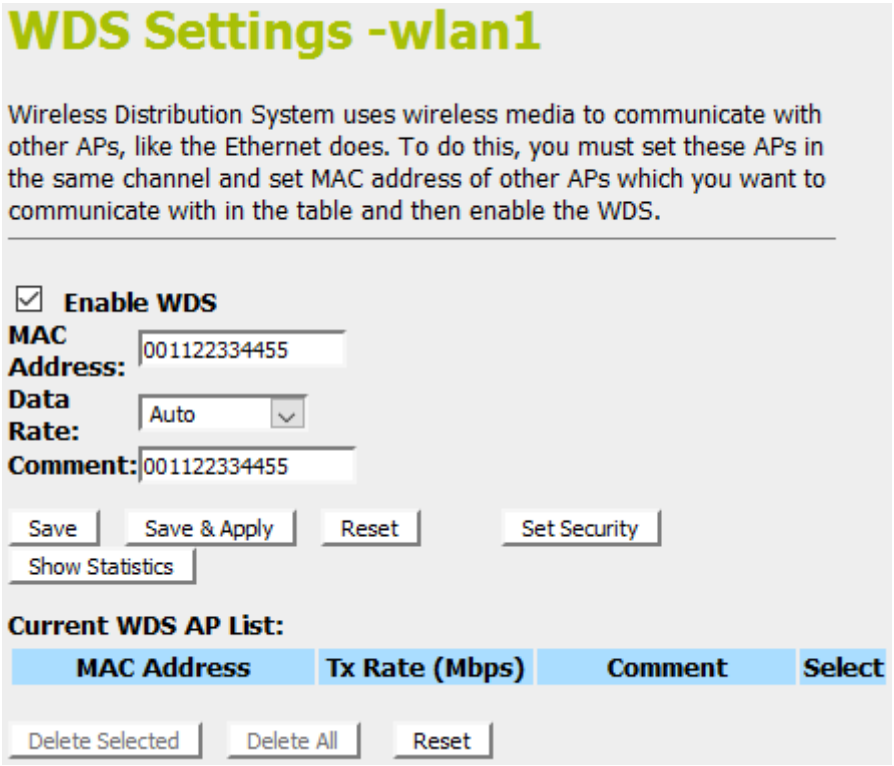
11. This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.
12. Configure each field with the *Encryption* that you selected.
13. Click *Save & Apply* button.



14. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

15. From the head menu, click on *WLAN1*.

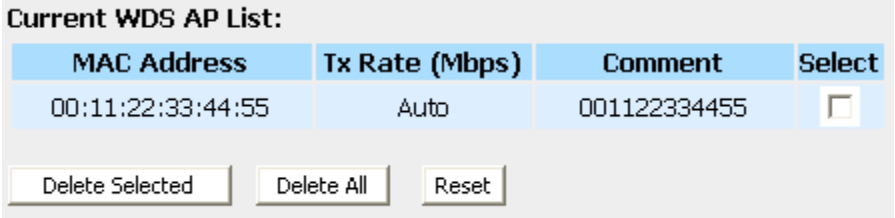
16. From the left-hand menu, click on *WDS settings*.
17. Check on the option*Enable WDS*.
18. Enter the *MAC Address*.
19. Enter the *Comment*.
20. Click the *Save & Apply*.



21. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

22. From the head menu, click on *WLAN1*.

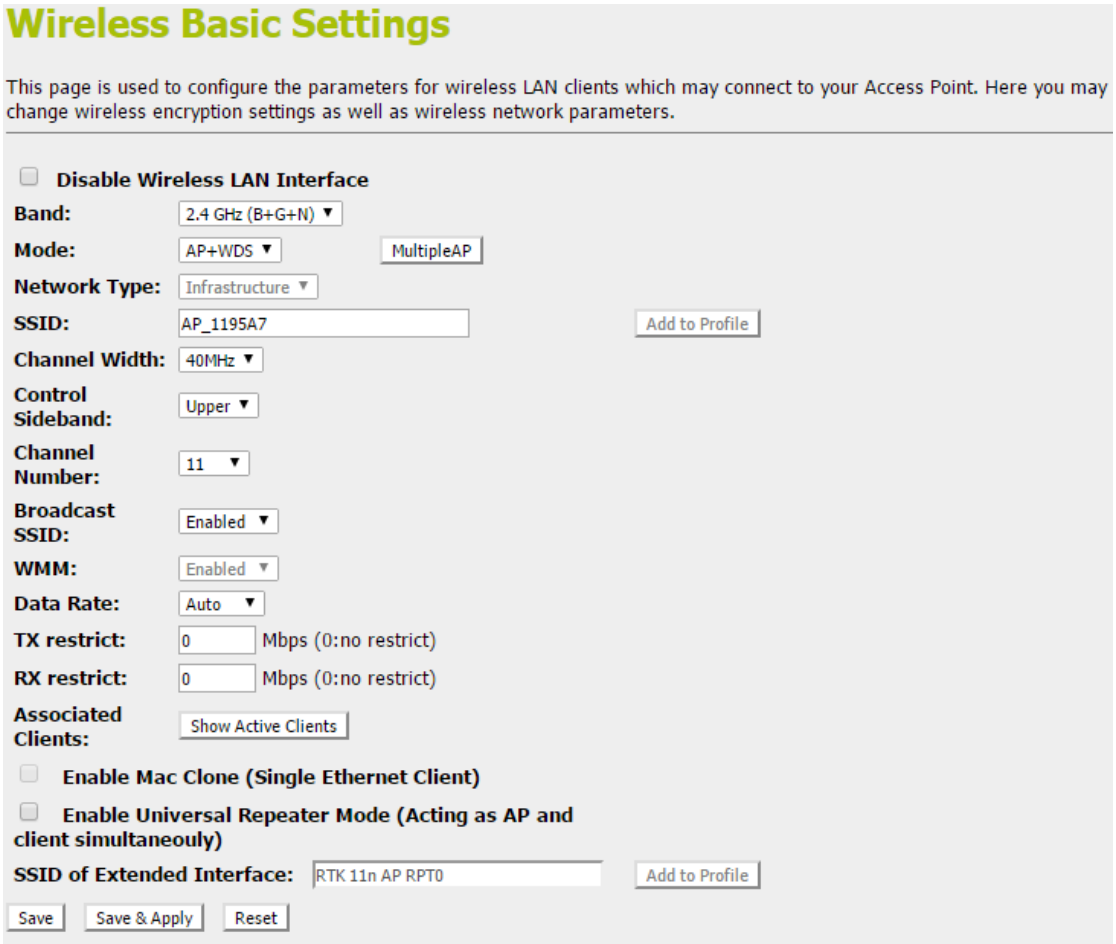
23. From the left-hand menu, click on *WDS settings*.
24. The MAC Address that you created has been added in the *Current Access Control List*.



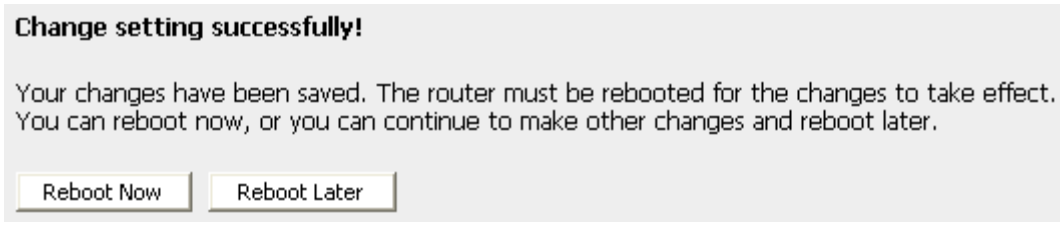
ConfigureAP (Access Point) + WDS (Wireless Distribution System)

1. From the head menu, click on *WLAN1*.

2. From the left-hand menu, click on *Basic Settings*.
3. From the *Mode* drop-down list, select *AP+WDS.*
4. Enter *SSID* for example AP_5G_A81261.
5. From the *Channel Number* drop-down list, select a Channel.
6. Click *Save & Apply* button.

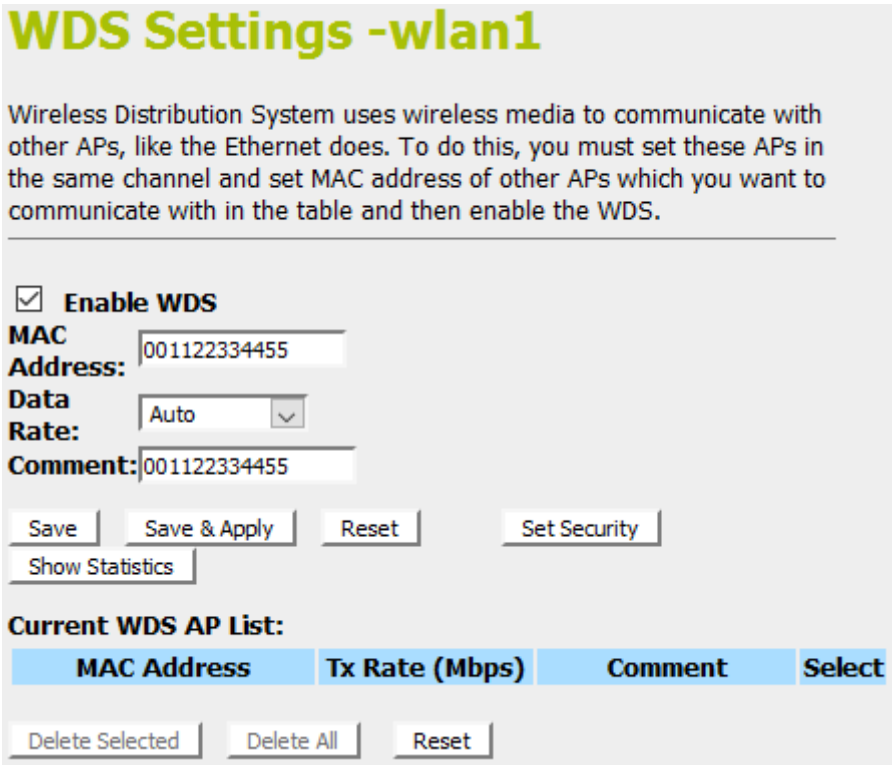


7. Change setting successfully! Click on *Reboot Now* button to confirm.

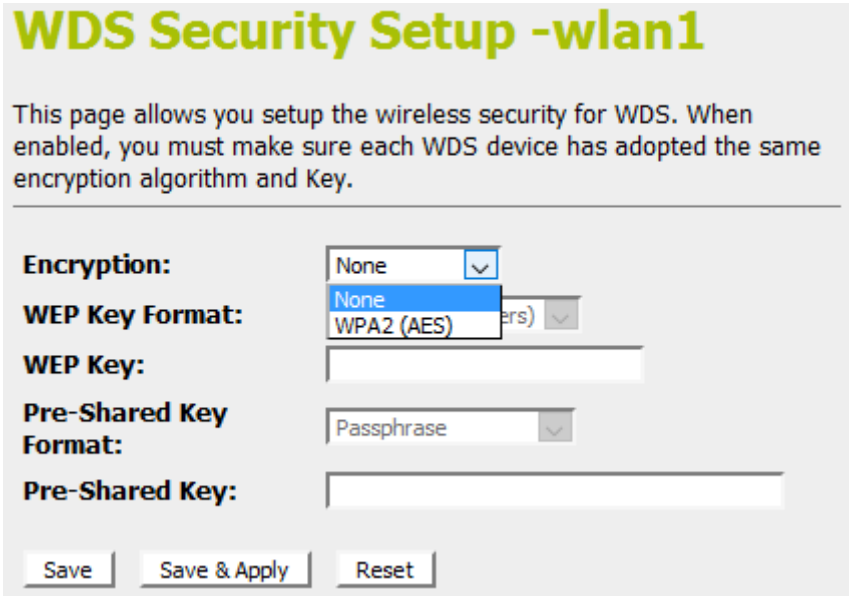


8. From the head menu, click on *WLAN1*.

9. From the left-hand menu, click on *WDS settings*.
10. Check on the option*Enable WDS*.
11. Click the *Set Security*.



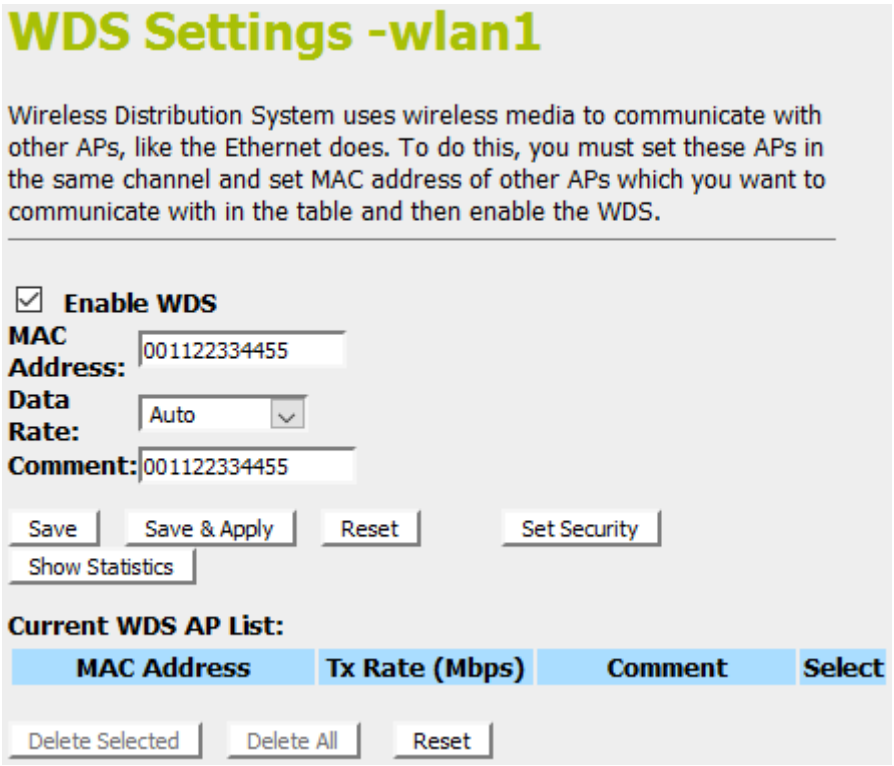
12. This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.
13. Configure each field with the *Encryption* that you selected.
14. Click *Save & Apply* button.



15. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

16. From the head menu, click on *WLAN1*.

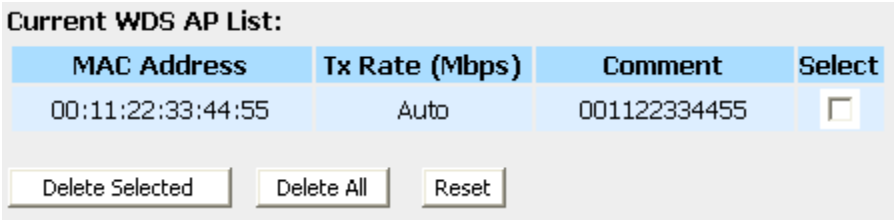
17. From the left-hand menu, click on *WDS settings*.
18. Check on the option*Enable WDS*.
19. Enter the *MAC Address*.
20. Enter the *Comment*.
21. Click the *Save & Apply*.



22. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

23. From the head menu, click on *WLAN1*.

24. From the left-hand menu, click on *WDS settings*.
25. The MAC Address that you created has been added in the *Current Access Control List*.

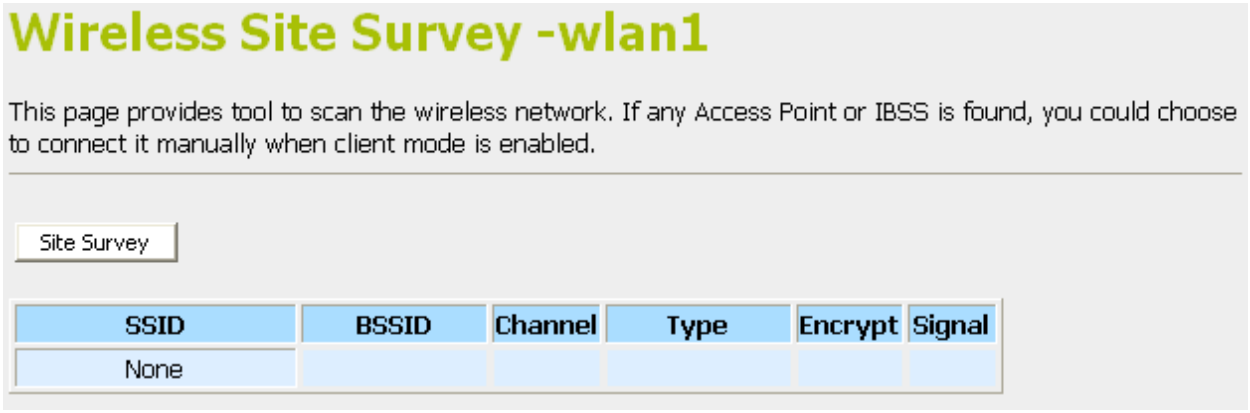


Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled. To access the *Wireless NetworkWDS settings*page:

1. From the head menu, click on *WLAN1*.

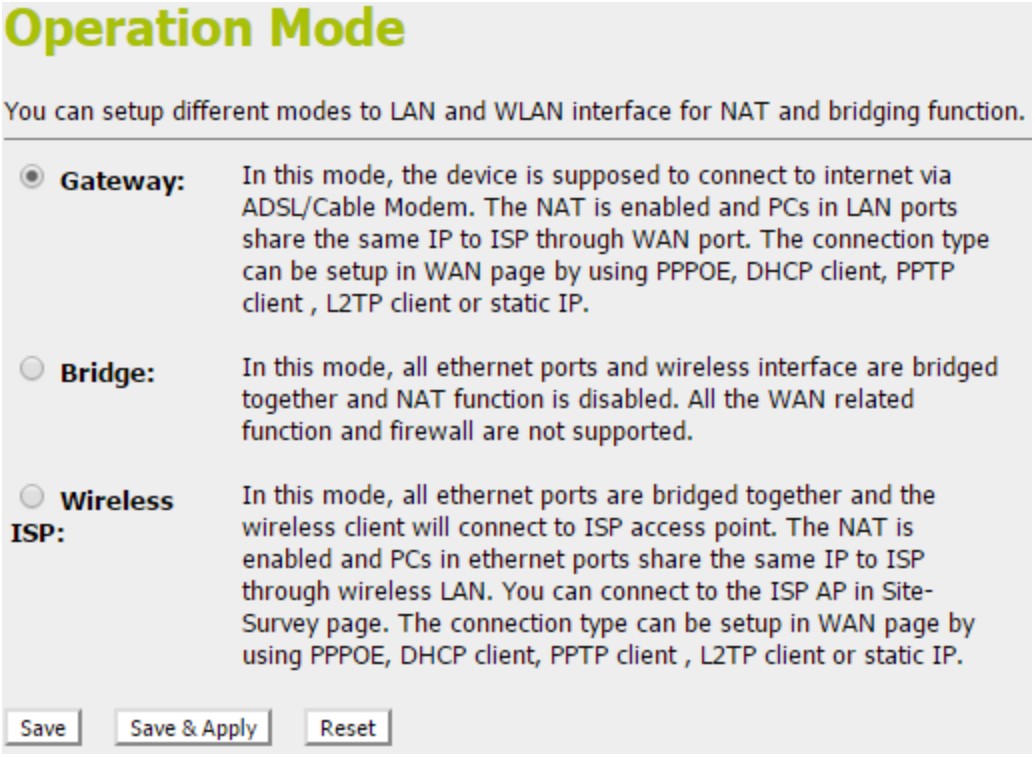
From the left-hand menu, click on *Site Survey*. The following page is displayed:



ConfigureWireless ISP + Wireless client +Site Survey

2. From the head menu, click on *SETUP*.

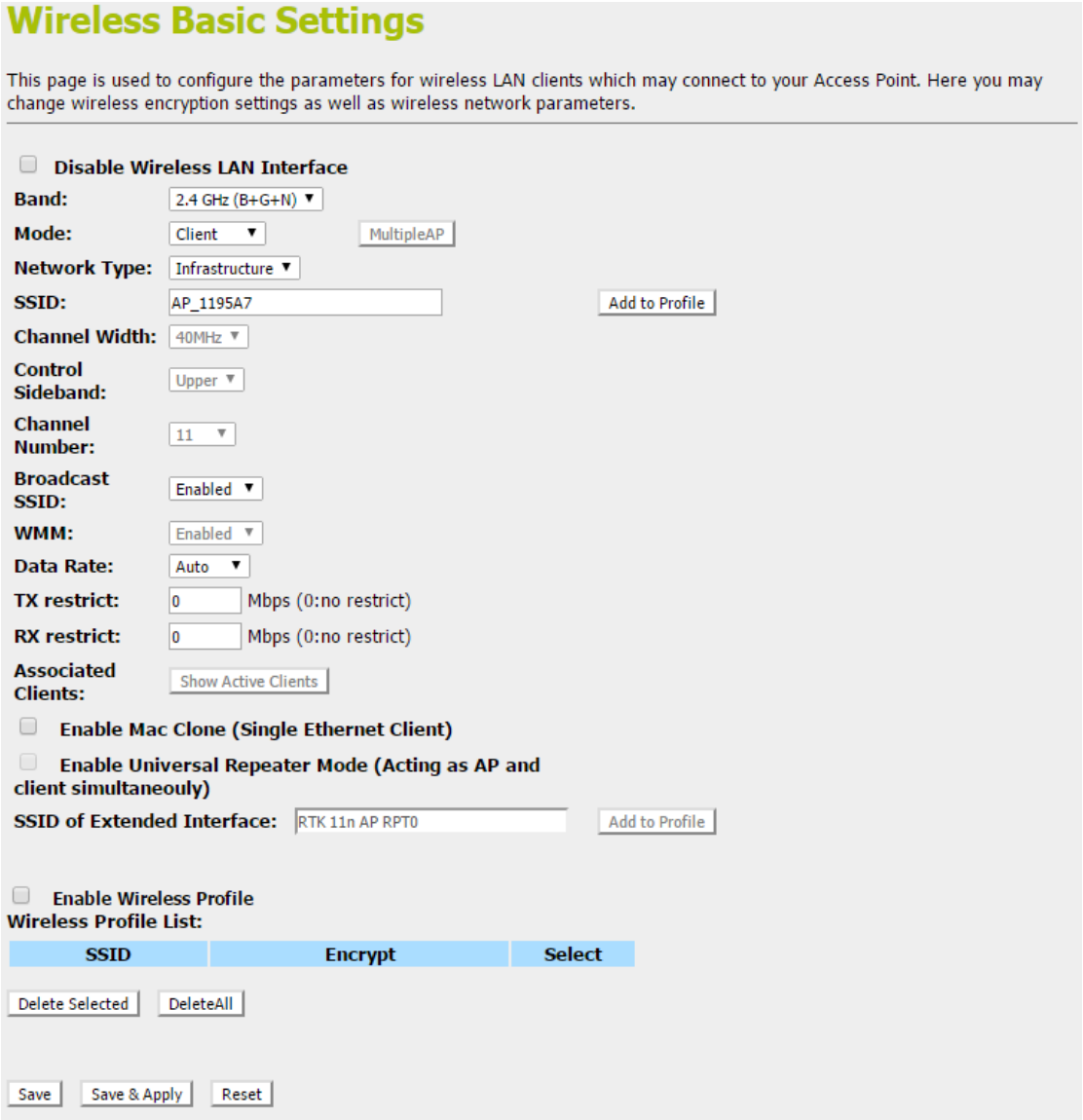
3. From the left-hand *Operation Mode*menu, click on *Wireless ISP Settings*.
4. Config WAN Interface.
5. Click *Save & Apply* button.



6. Change setting successfully! Do not turn off or reboot the Device during this time. Please wait 20 seconds ...

7. From the head menu, click on *WAN1*.

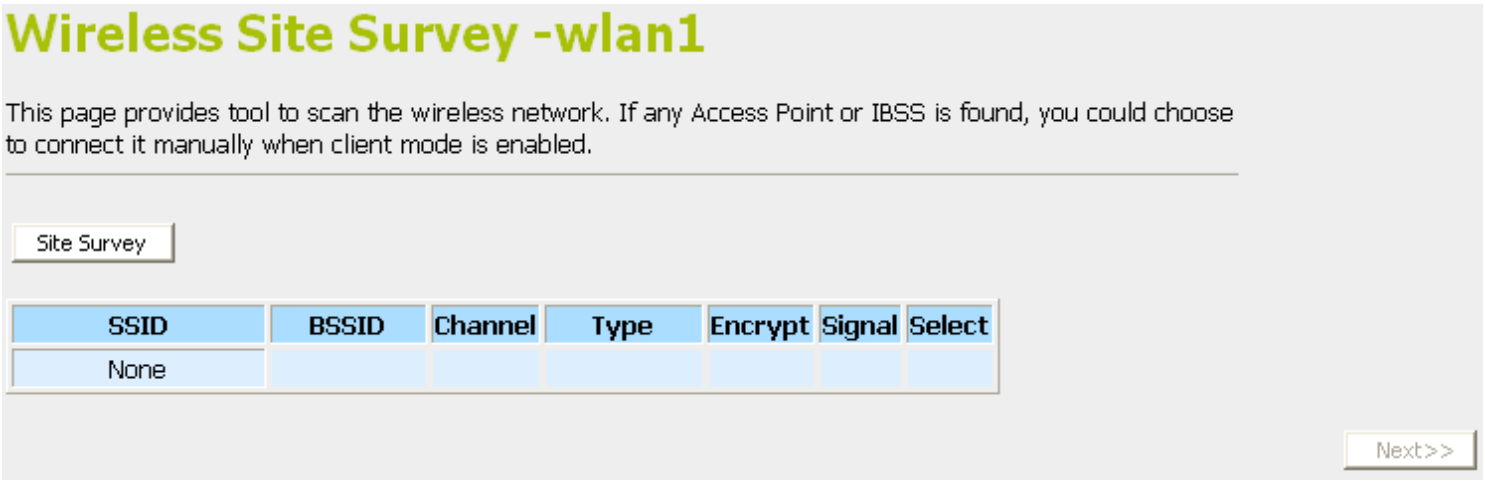
8. From the left-hand menu, click on *Basic Settings*.
9. From the *Mode* drop-down list, select *Client.*
10. Enter *SSID*of the AP that you want to connect to for example AP_5G_A81261. If you don't know what the SSID of the AP that you want to connect to, please skip this step.
11. Click *Save & Apply* button.



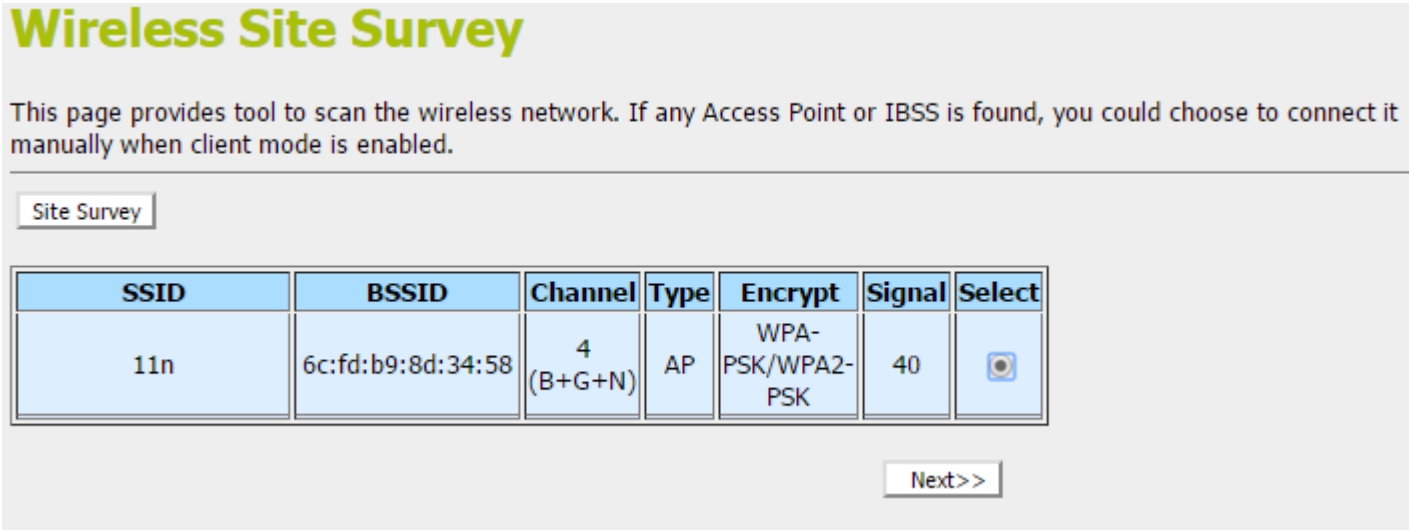
12. Please wait 20 seconds ...

13. From the head menu, click on *WAN1*.

14. From the left-hand menu, click on *Site Survey*.
15. Click *Site Survey* button.

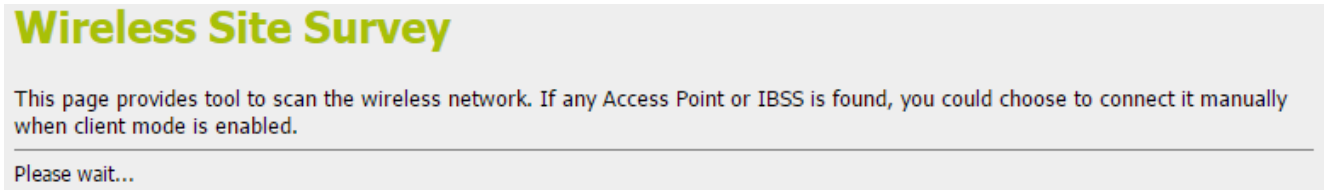


16. Now you could see the APs that scanned by the Wireless Gateway were listed below.
17. Click on the ratio of AP's SSID under the item *Select* that you want the Wireless Gateway to connect to.
18. Click *Next* button.

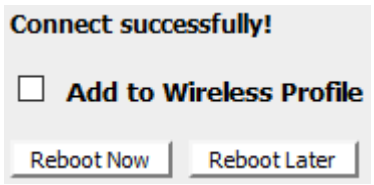


19. Click *Connect* button.

20. Please wait...



21. Check on *Add to Wireless Profile*.
22. Click *Reboot Now* button.



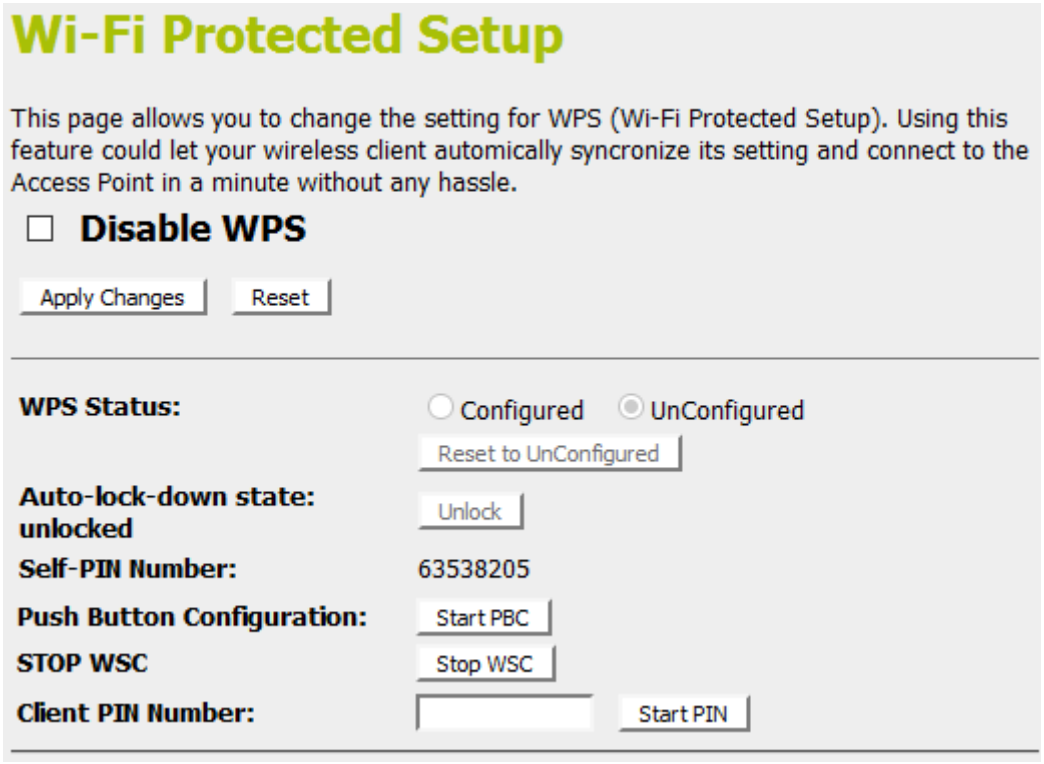
23. Change setting successfully! Please wait 20 seconds….

WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle. To access the *Wireless NetworkWPS*page:

1. From the head menu, click on *WAN1*.

2. From the left-hand menu, click on *WPS*. The following page is displayed:



Field	Description
Disable WPS	**Checking this box and clicking "Save & Apply" will disable Wi-Fi Protected Setup. WPS is turned on by default.**
WPS Status	**When AP's settings are factory default (out of box), it is set to open security and un-configured state. It will be displayed by "WPS Status". If it already shows "Configured", some registrars such as Vista WCN will not configure AP. Users will need to go to the "Save/Reload Settings" page and click "Reset" to reload factory default settings.**
Self-PIN Number	**"Self-PIN Number" is AP's PIN. Whenever users want to change AP's PIN, they could click "Regenerate PIN" and then click " Save & Apply". Moreover, if users want to make their own PIN, they could enter four digit PIN without checksum and then click " Save & Apply". However, this would not be recommended since the registrar side needs to be supported with four digit PIN.**

Field	Description
Push Button Configuration	**Clicking this button will invoke the PBC method of WPS. It is only used when AP acts as a registrar.**
Save & Apply	**Whenever users want to enable/disable WPS or change AP's PIN, they need to apply this button to commit changes.**
Reset	**It restores the original values of "Self-PIN Number" and "Client PIN Number".**
Client PIN Number	**It is only used when users want their station to join AP's network. The length of PIN is limited to four or eight numeric digits. If users enter eight digit PIN with checksum error, there will be a warning message popping up.** **If users insist on this PIN, AP will take it.**

Introduction of WPS

Although home Wi-Fi networks have become more and more popular, users still have trouble with the initial set up of network. This obstacle forces users to use the open security and increases the risk of eavesdropping. Therefore, WPS is designed to ease set up of security-enabled Wi-Fi networks and subsequently network management (Wi-Fi Protected Setup Specification 1.0h.pdf, p. 8).

The largest difference between WPS-enabled devices and legacy devices is that users do not need the knowledge about SSID, channel and security settings, but they could still surf in a security-enabled Wi-Fi network. For examples, in the initial network set up, if users want to use the PIN configuration, the only thing they need to do is entering the device PIN into registrar, starting the PIN method on that device and simply wait until the device joins the network. After the PIN method is started on both sides, a registration protocol will be initiated between the registrar and the enrollee. Typically, a registrar could be an access point or other device that is capable of managing the network. An enrollee could be an access point or a station that will join the network. After the registration protocol has been done, the enrollee will receive SSID and security settings from the registrar and then join the network. In other words; if a station attempts to join a network managed by an access point with built-in internal registrar, users will need to enter station's PIN into the web page of that access point. If the device PIN is correct and valid and users start PIN on station, the access point and the station will automatically exchange the encrypted information of the network settings under the management of AP's internal registrar. The station then uses this information to perform authentication algorithm, join the secure network, and transmit data with the encryption algorithm. More details will be demonstrated in the following sections.

Supported WPS features

Currently, Wireless Gateway supports WPS features for ***AP mode***, ***AP+WDS mode***, ***Infrastructure-Client mode***, and the ***wireless root interface of Universal Repeater mode***.

Other modes such as ***WDS mode***, ***Infrastructure-Adhoc mode***, and the ***wireless virtual interface of Universal Repeater mode*** are not implemented with WPS features.

If those unsupported modes are enforced by users, WPS will be disabled. Under the configuration of every WPS-supported mode, Wireless Gateway has *Push Button method* and *PIN method*. For each method, Wireless Gateway offers different security levels included in network credential, such as open security, WEP 64 bits, WEP 128 bits, WPA-Personal TKIP, WPA-Personal AES, WPA2-Personal TKIP, and WPA2-Personal AES. Users could choose either one of the methods at their convenience.

AP mode

For AP mode, Wireless Gateway supports three roles, registrar, proxy, and enrollee in registration protocol. At different scenarios, Wireless Gateway will automatically switch to an appropriate role depending on the other device's role or a specific configuration.

AP as Enrollee

If users know AP's PIN and enter it into external registrar, the external registrar will configure AP with a new wireless profile such as new SSID and new security settings. The external registrar does this job either utilizing the in-band EAP (wireless) or out-of-band UPnP (Ethernet). During the WPS handshake, a wireless profile is encrypted and transmitted to AP. If the handshake is successfully done, AP will be re-initialized with the new wireless profile and wait for legacy stations or WPS stations to join its network.

AP as Registrar

Wireless Gateway also has a built-in internal registrar. Whenever users enter station's PIN into AP's webpage, click "Start PBC", or push the physical button, AP will switch to registrar automatically. If users apply the same method on station side and the WPS handshake is successfully done, SSID and security settings will be transmitted to that station without the risk of eavesdropping. And then the station will associate with AP in a security-enabled network.

AP as Proxy

At this state, AP is transparent to users. If users want to configure a station or any device that is capable of being an enrollee, they have to enter device's PIN into an external registrar and choose an appropriate wireless profile. After the PIN is entered, the external registrar will inform AP this event. AP then conveys the encrypted wireless profile between the device and the external registrar. Finally, the device will use the wireless profile and associate with AP. However, the device may connect to other APs if the wireless profile does not belong to the proxy AP. Users must carefully choose the wireless profile or create a wireless profile on an external registrar.

Infrastructure-Client mode

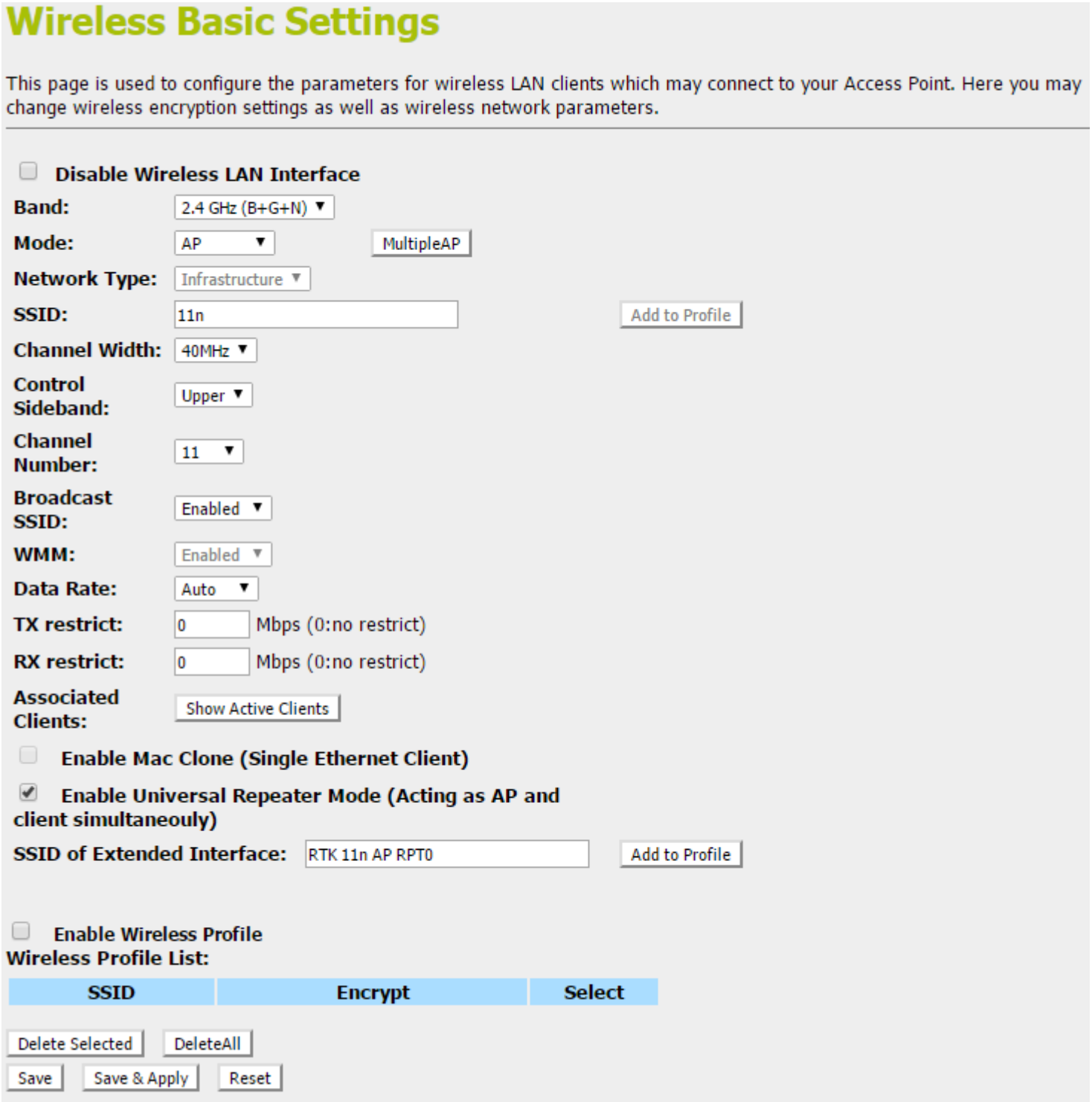
In Infrastructure-Client mode, Wireless Gateway only supports enrollee's role. If users click "Start PIN", click "Start PBC", or press the physical button on Wireless Gateway, it will start to seek WPS AP. Once users apply the same method on registrar side, Wireless Gateway will receive the wireless profile upon successfully doing the registration protocol. Then Wireless Gateway will associate with an AP.

Instructions of AP's and Client's operations

At this state, AP is transparent to users. If users want to configure a station or any device that is capable of being an enrollee, they have to enter device's PIN into an external registrar and choose an appropriate wireless profile. After the PIN is entered, the external registrar will inform AP this event. AP then conveys the encrypted wireless profile between the device and the external registrar. Finally, the device will use the wireless profile and associate with AP. However, the device may connect to other APs if the wireless profile does not belong to the proxy AP. Users must carefully choose the wireless profile or create a wireless profile on an external registrar.

Wireless Basic Settings - WLAN1page

Users need to make sure the “Broadcast SSID” file is set to “Enabled”. Otherwise, it might prevent WPS from working properly.

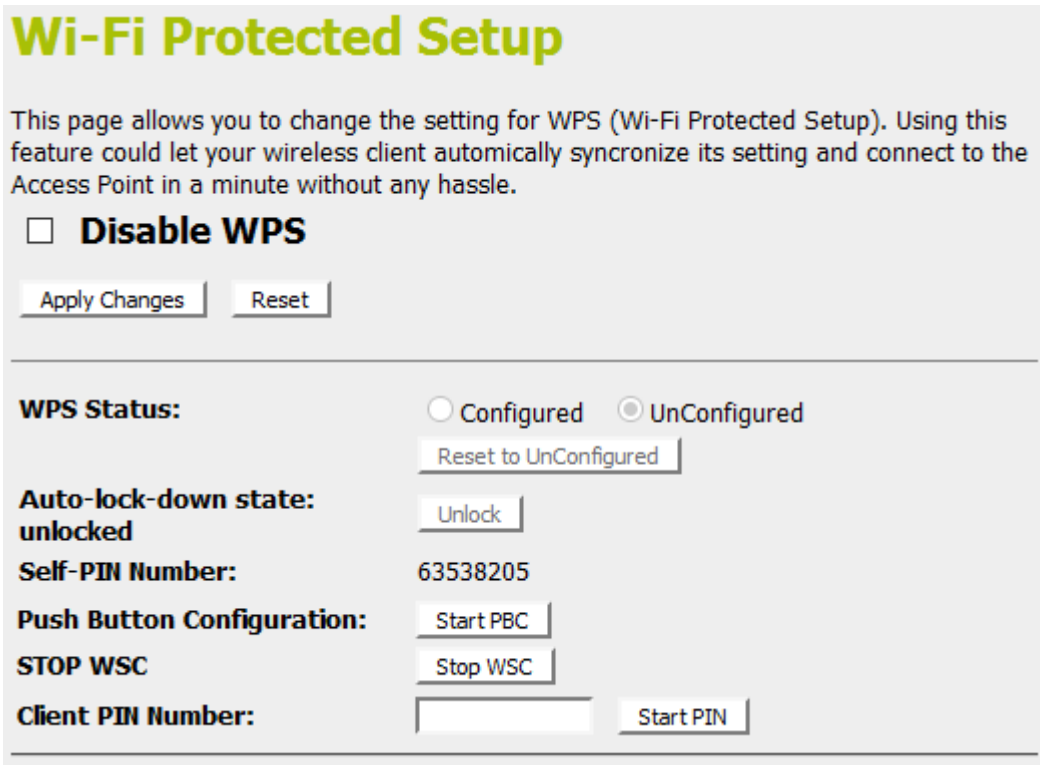


Operations of AP - AP being an enrollee

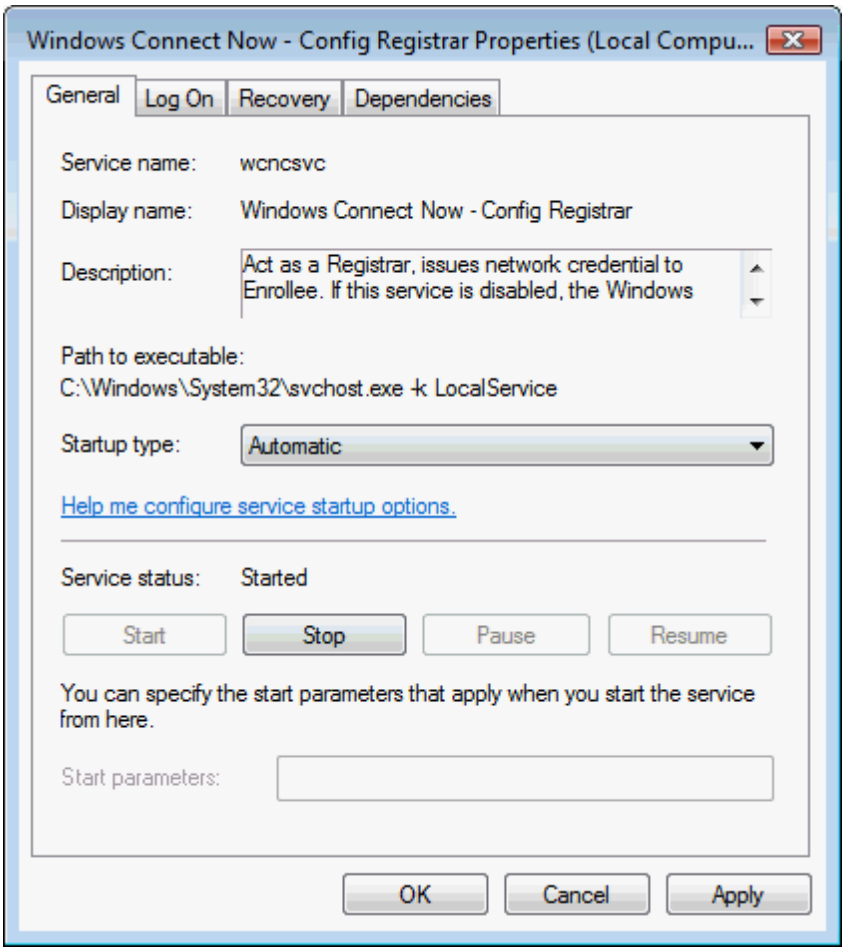
In this case, AP will be configured by any registrar either through in-band EAP or UPnP. Here, users do not need to do any action on AP side. They just need AP's device PIN and enter it into registrar. An example from Vista WCN will be given.

1. From the head menu, click on *WAN1*.

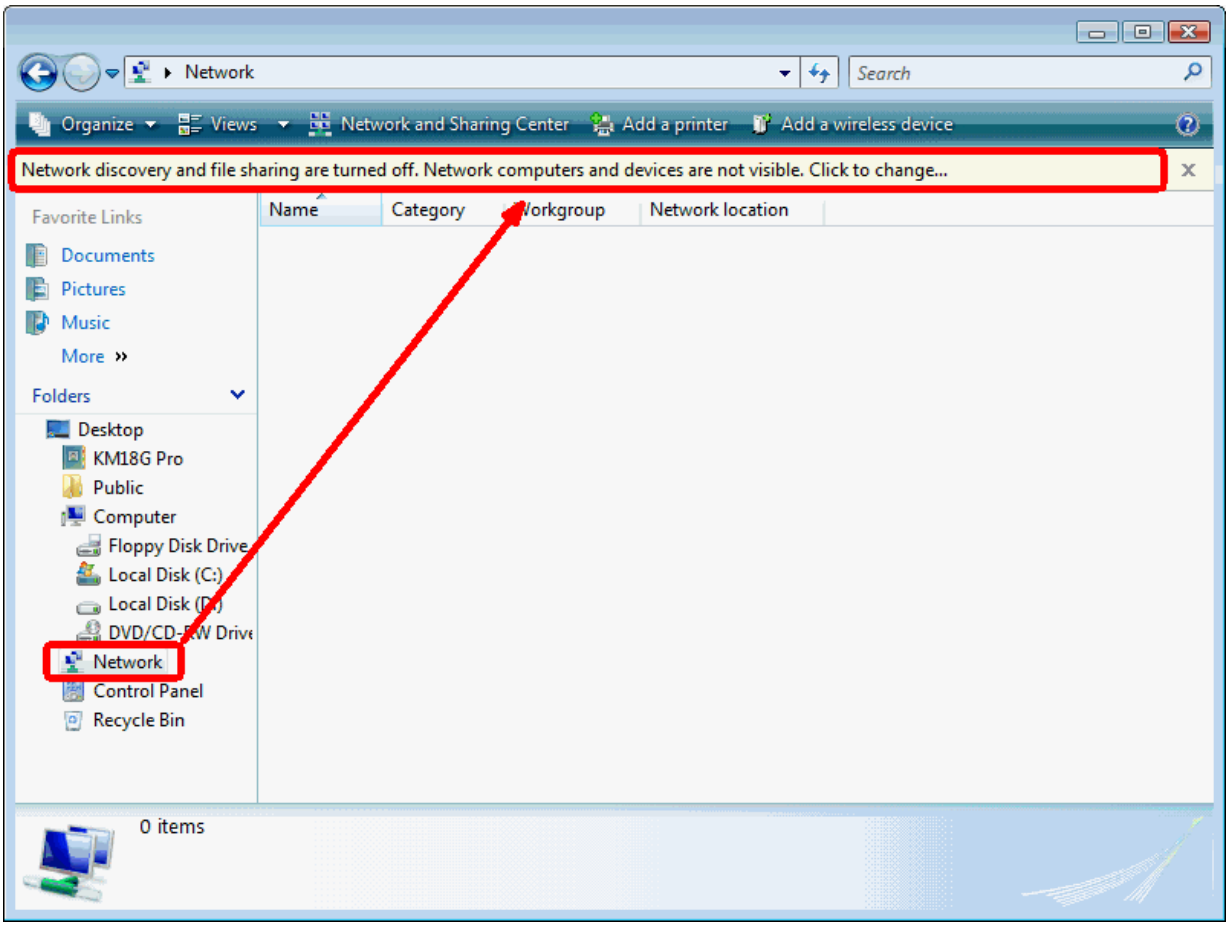
2. From the left-hand menu, click on *WPS*. The following page is displayed:
3. Make sure AP is in un-configured state.



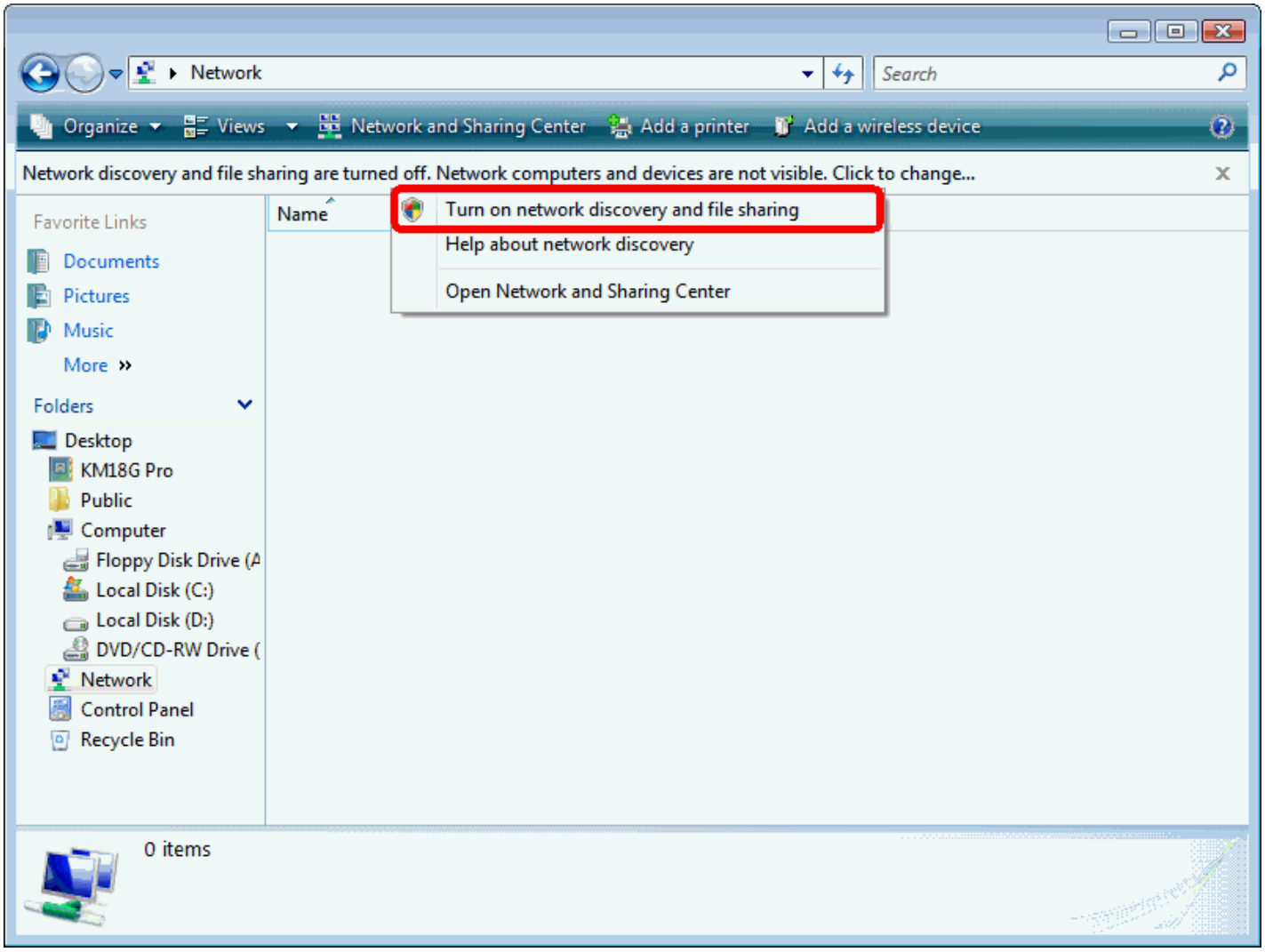
4. Plug the Ethernet cable into AP's LAN port and make sure the IP connection is valid with Vista.
5. Make sure WCN is enabled. Users may need to enable it at the first time. They could open the "Control Panel", click "Classic View", open "Administrative Tools", double click "Services", ", a User Account Control pop up and click "Continue", edit properties of "Windows Connect Now", choose the "Startup type" with "Automatic" and click "Start".



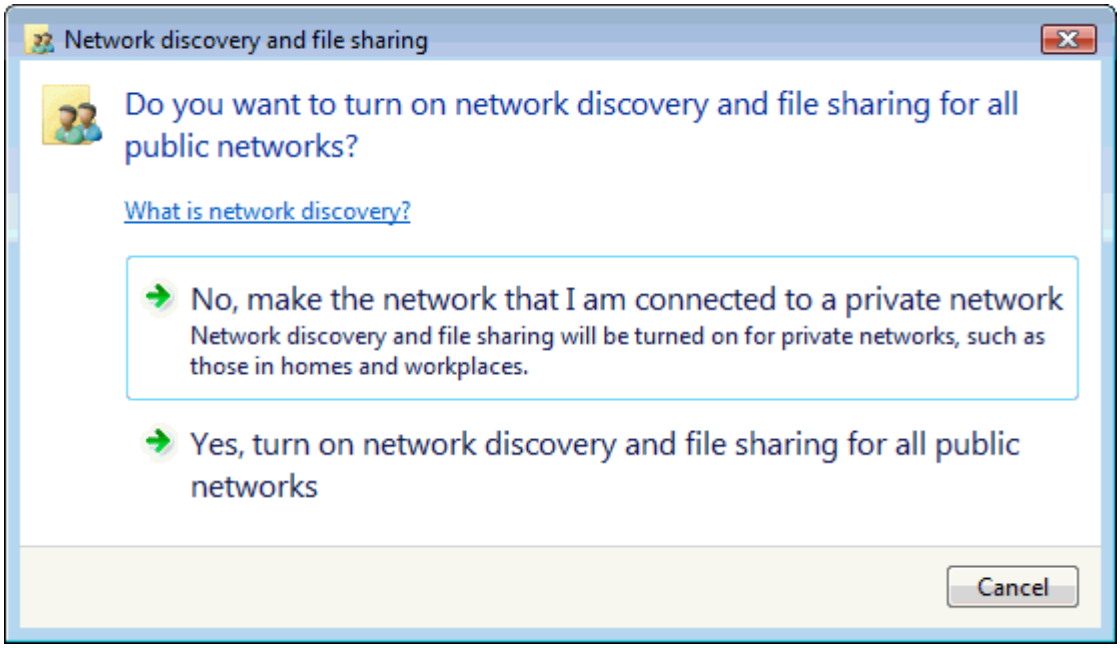
6. If the previous steps are done, open Windows Explorer. Go to the Network section.
7. Click on “Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to Change…“



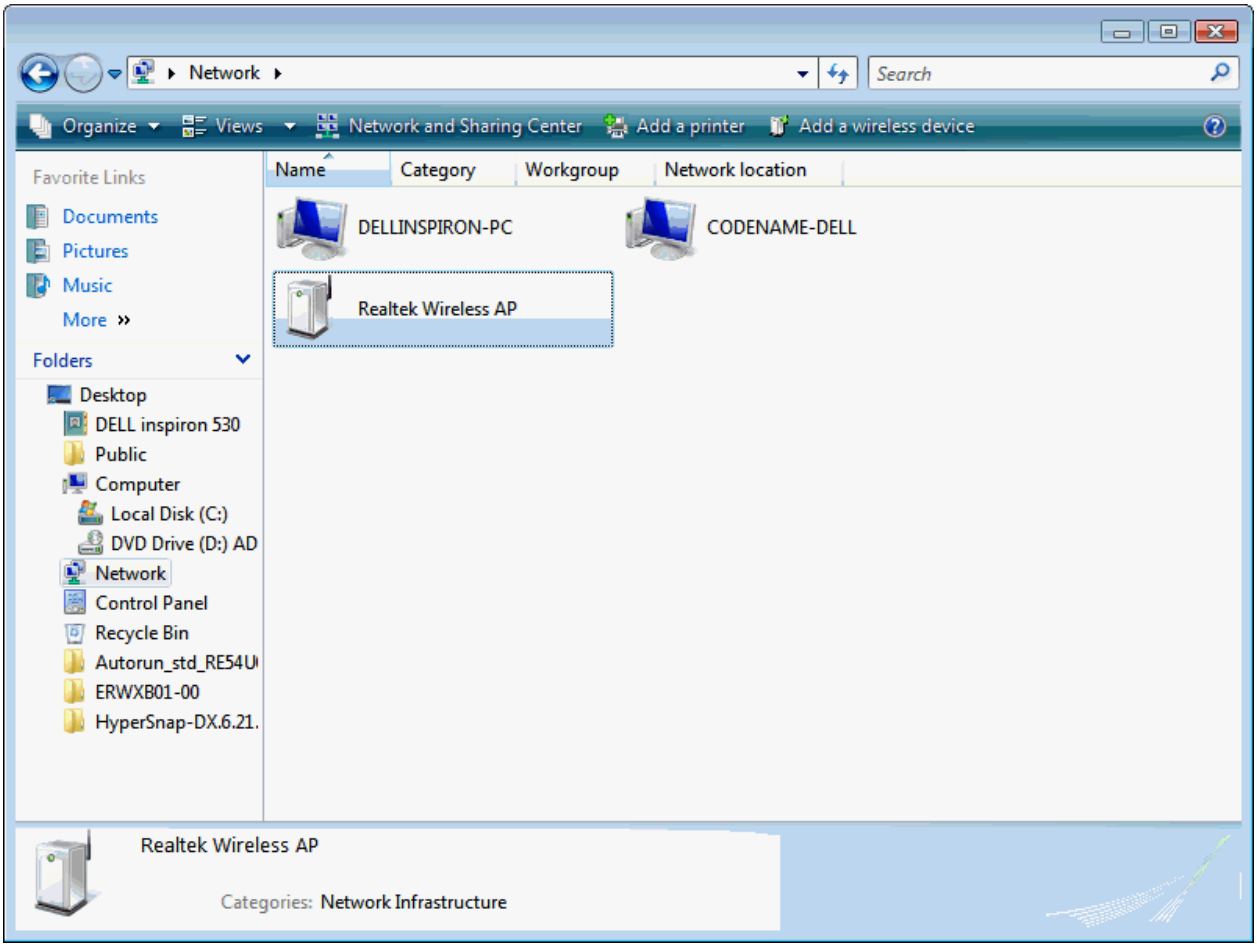
8. Click on “Turn on network discovery and file sharing“



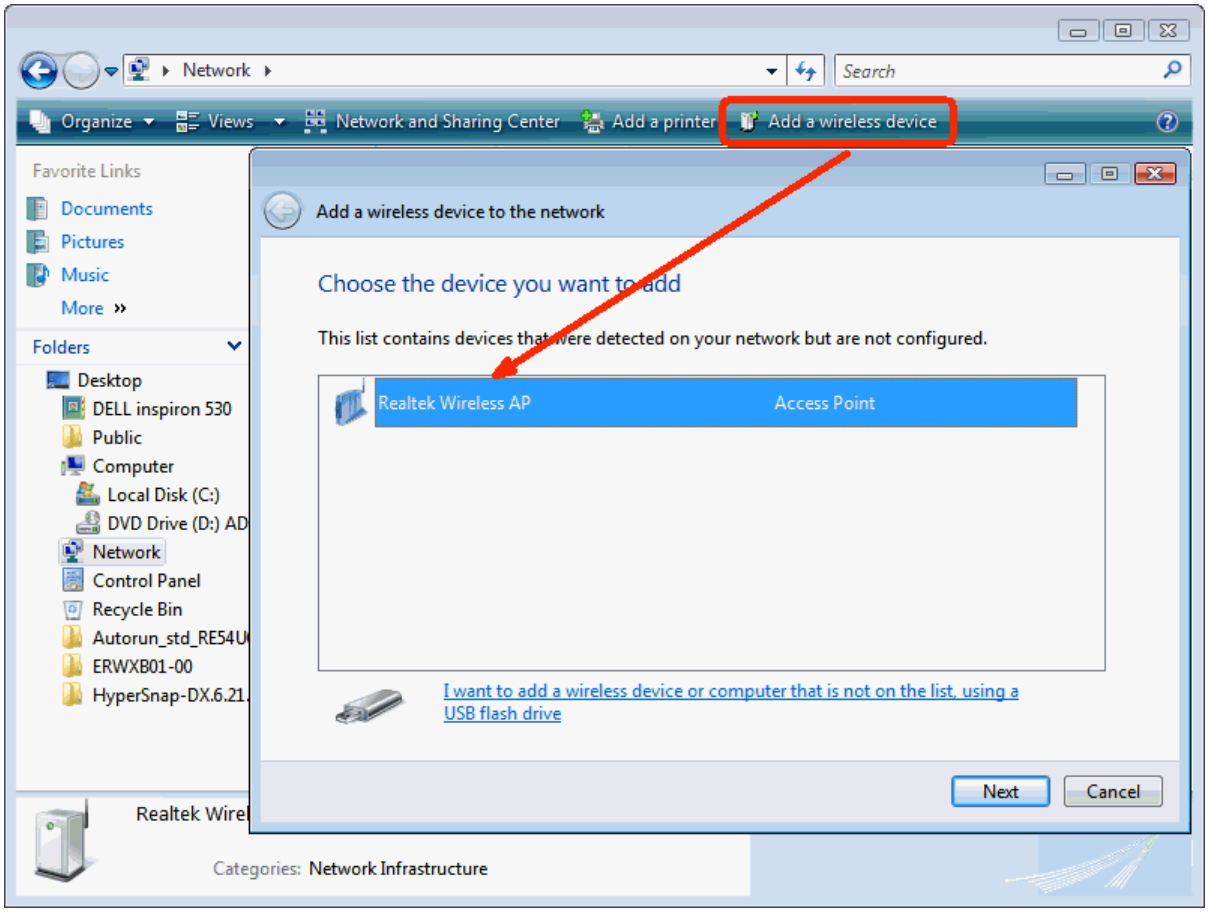
9. Click on “No, make the network that I am connected to a private network“



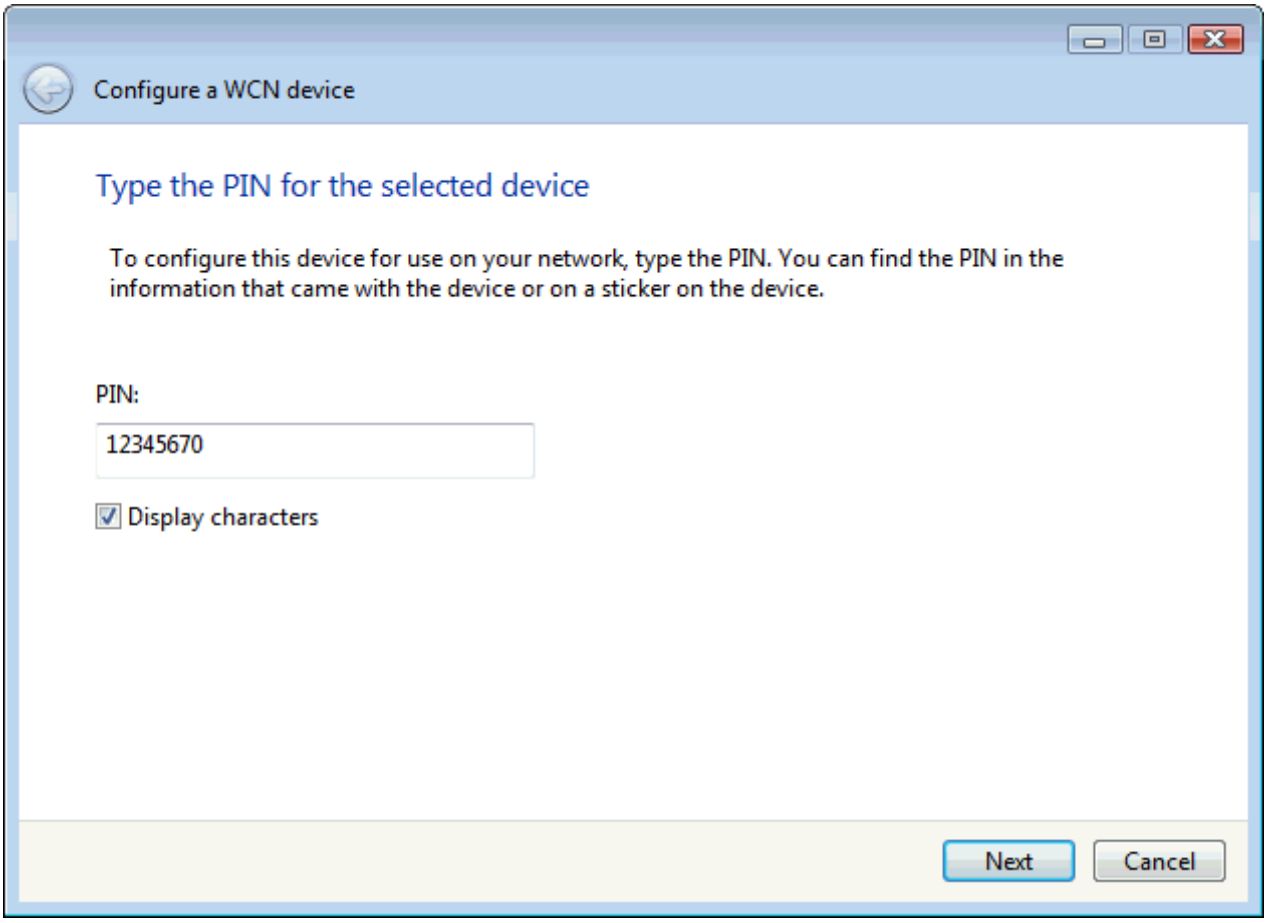
10. AP's icon will show up. Double click on it.



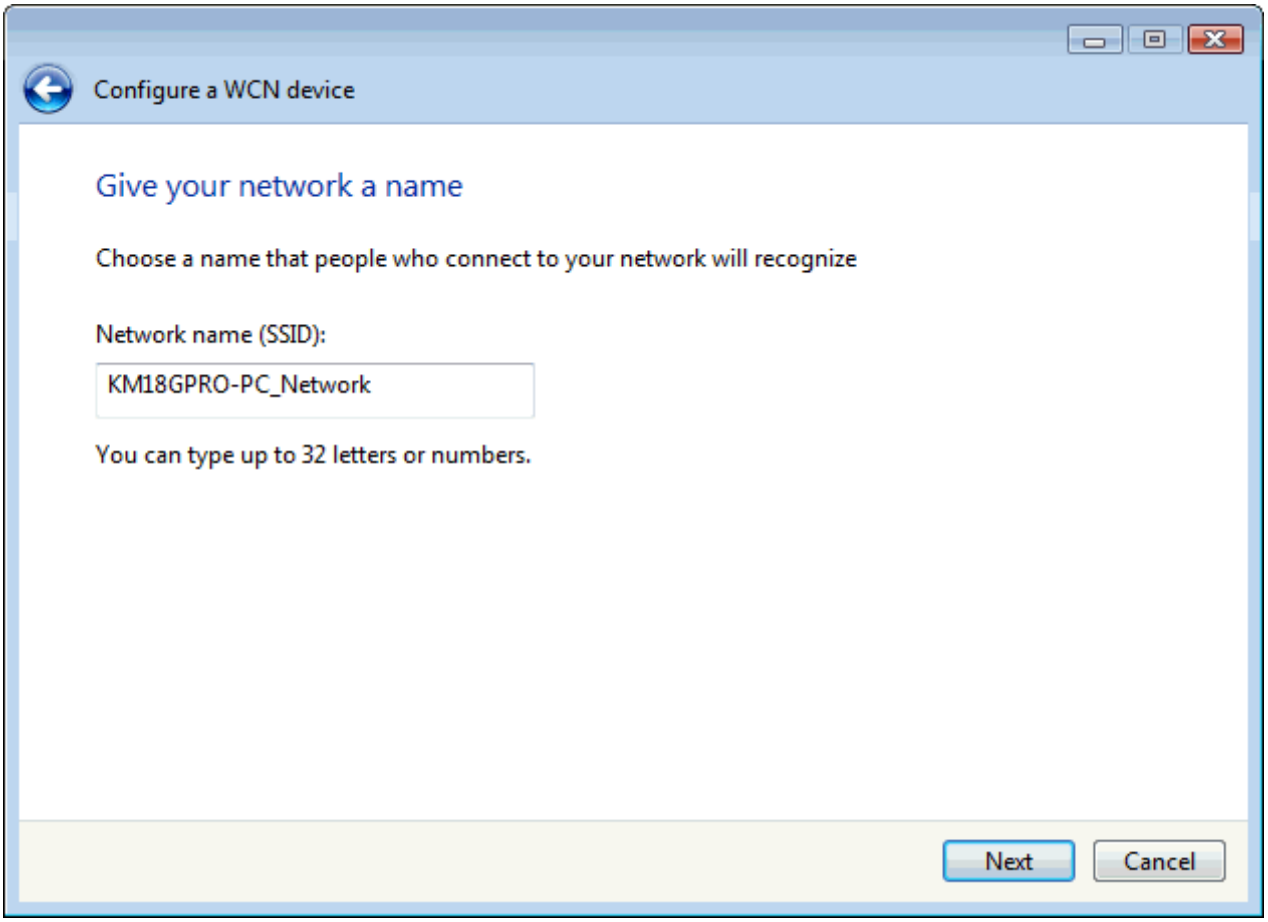
11. Users could also Click “Add a wireless device” if the icon is not there. Click “next”.



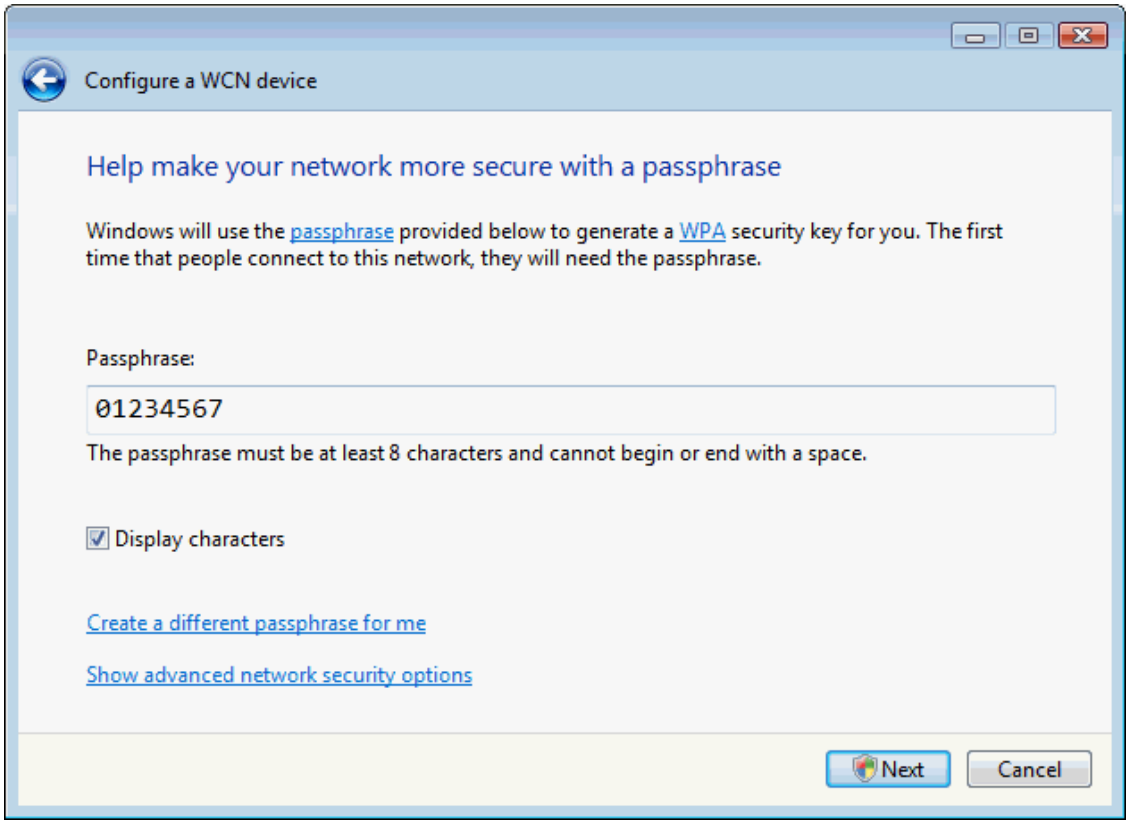
12. Enter AP's Self-PIN Numberand click "next".



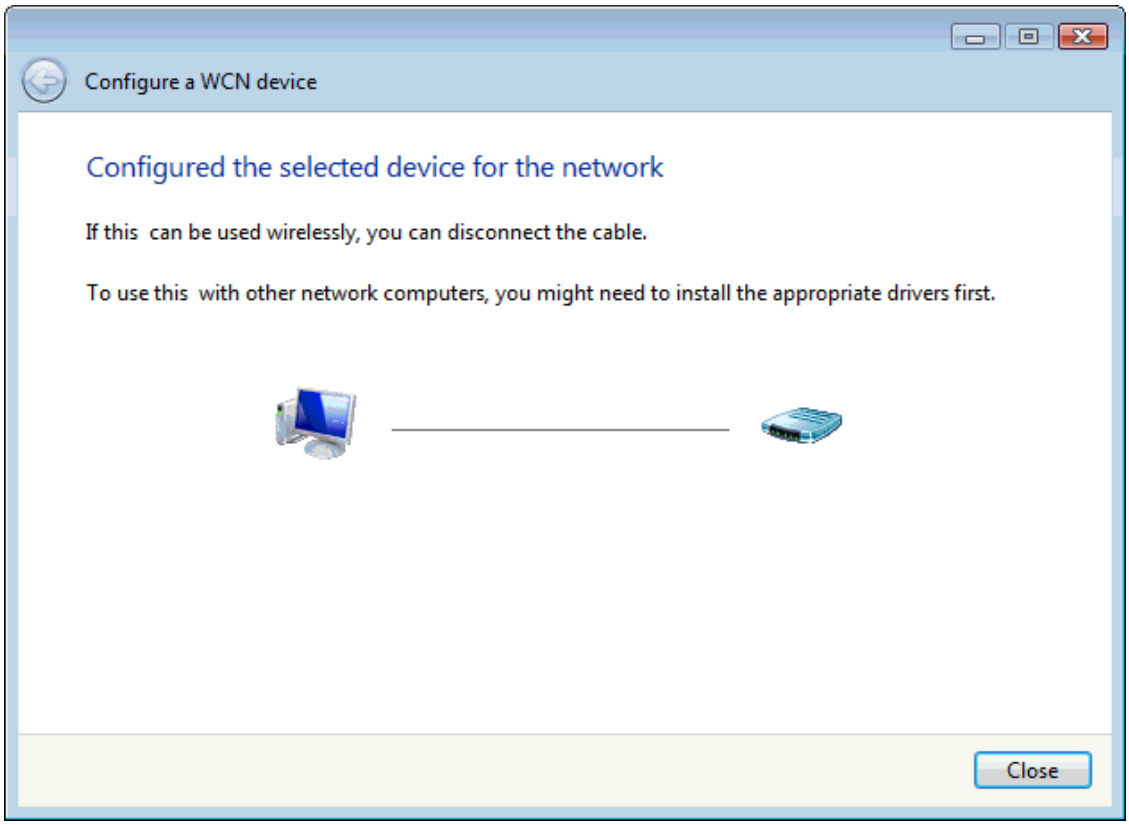
13. Choose a name that people who connect to your network will recognize.



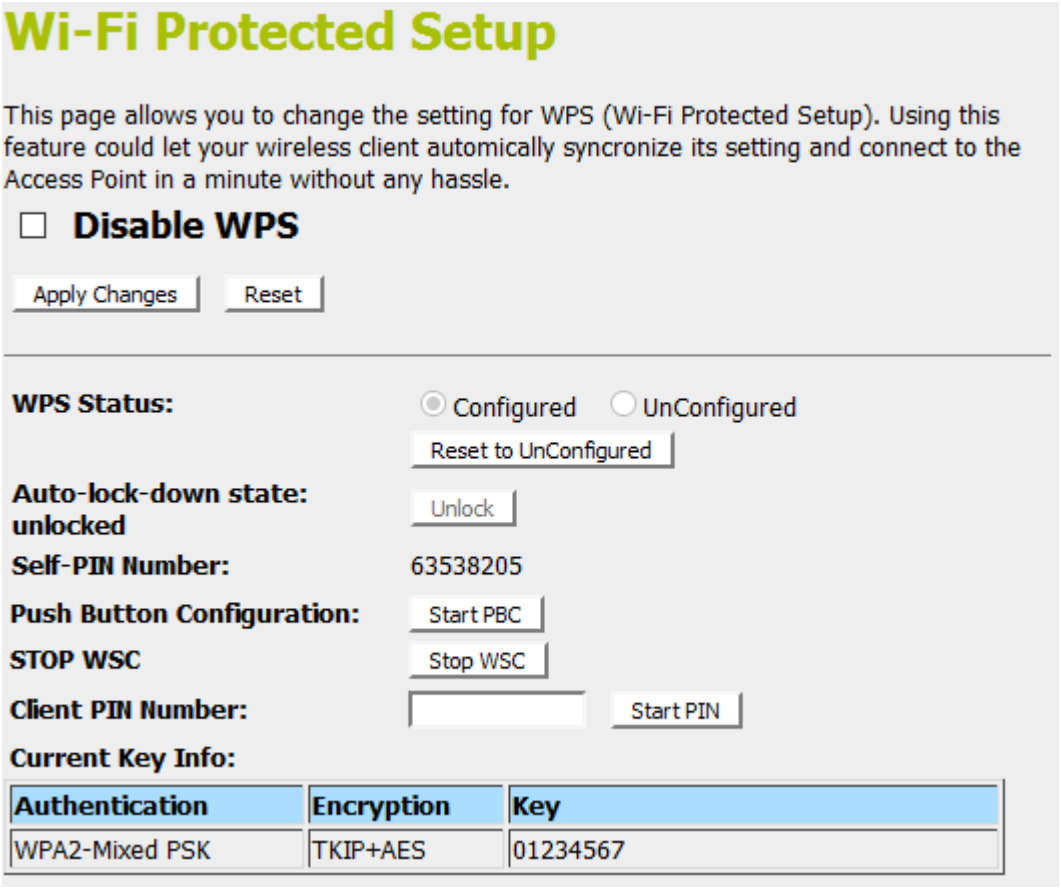
14. Enter the Passphrase and then click Next.



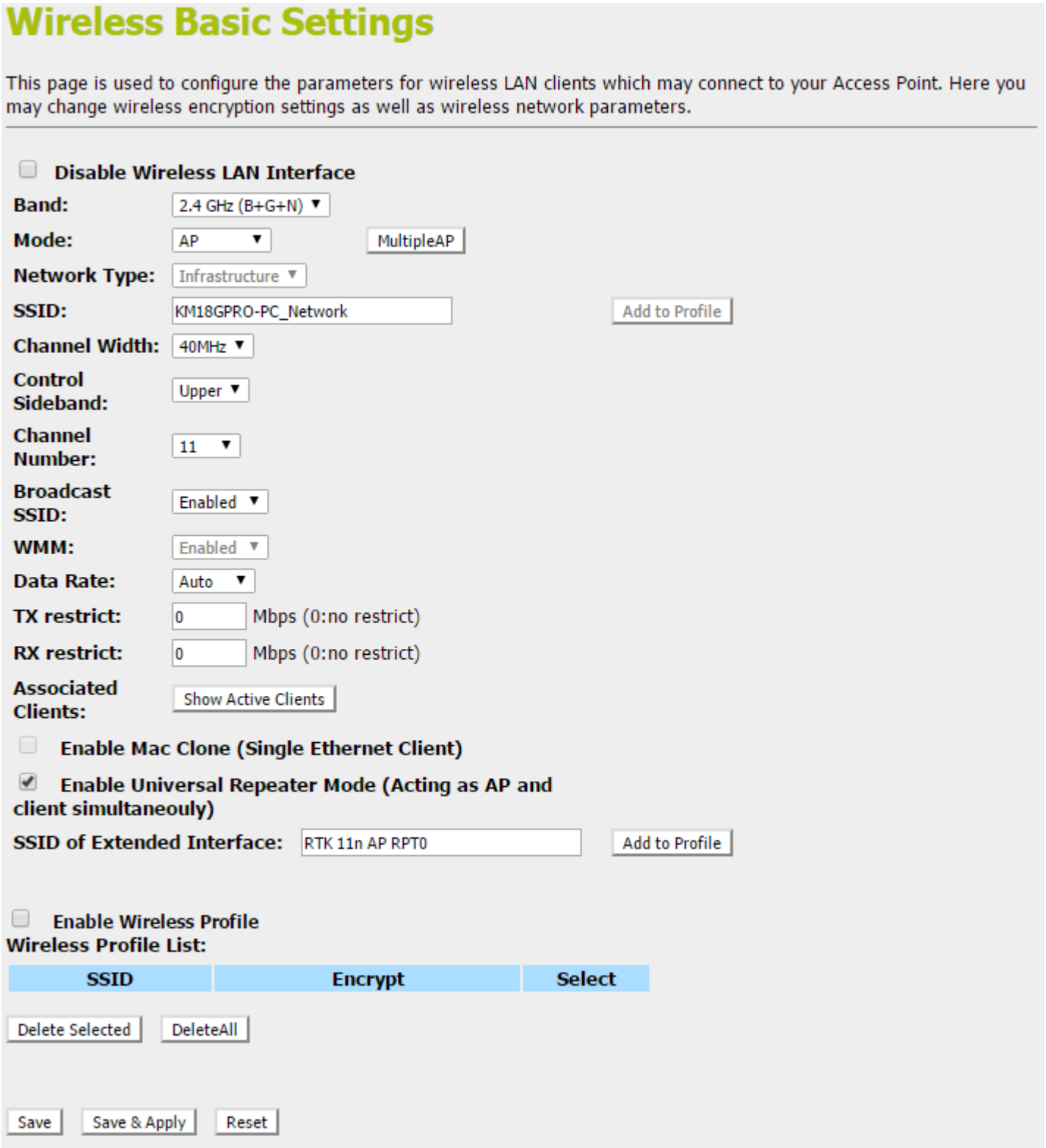
15. A User Account Control screen pops up, click Continue.
16. AP is successfully configured by WCN.



17. Finally, AP will become configured (see WPS Status). The authentication algorithm, encryption algorithm, and key assigned by WCN will be displayed below “Current Key Info”.



18. The SSID field of Wireless Basic Settings page will also be modified with the value assigned by WCN.



19. The security settings on the Wireless Security Page will be modified by WCN, too. The warning message will show up if users try to modify the security settings. The reason is the same as we explained in the previous section.

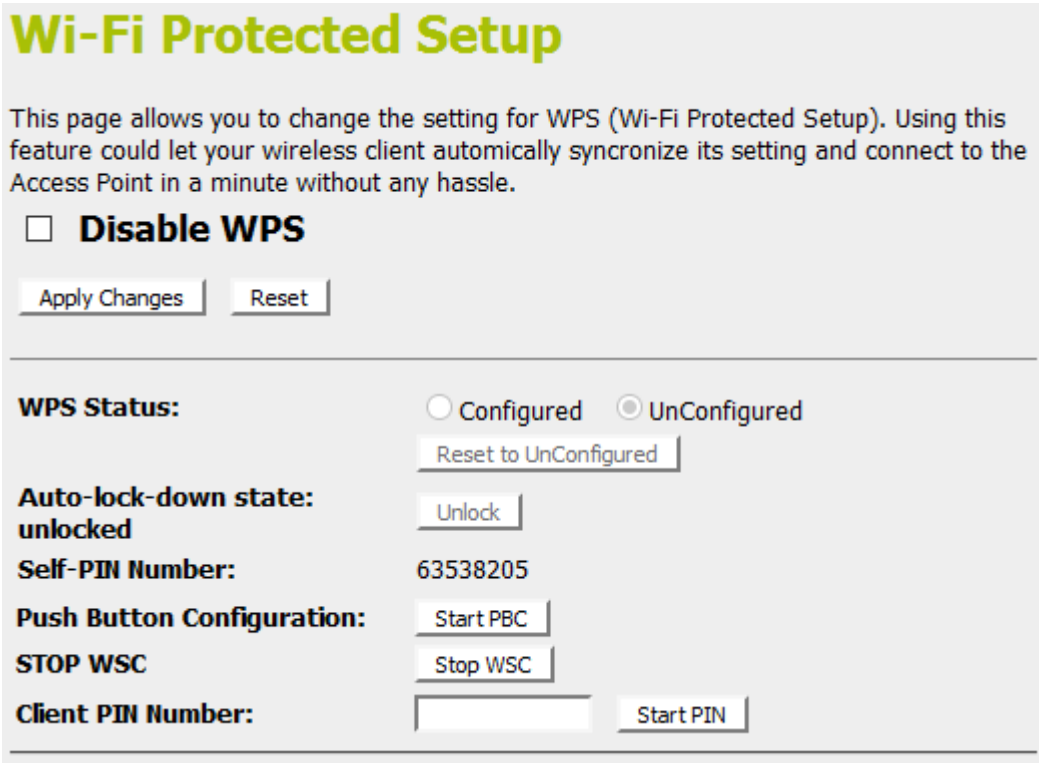
Operations of AP - AP being a registrar

AP mode

Whenever users enter station's PIN into AP's Wi-Fi Protected Setup page and click "Start PIN", AP will become a registrar. Users must start the PIN method on the station side within two minutes.

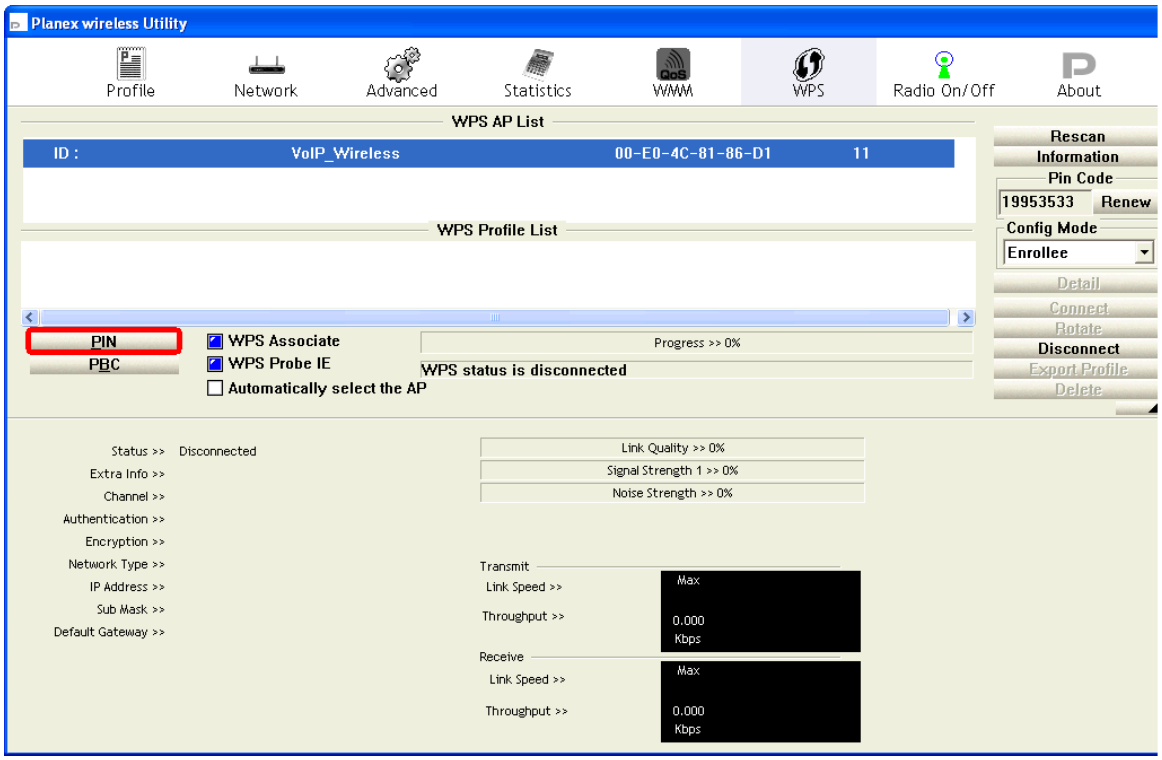
1. From the head menu, click on *WAN1*.

2. From the left-hand menu, click on *WPS*. The following page is displayed:
3. Make sure AP is in un-configured state.
4. Enter the Client PIN Number.
5. Click *Start PIN*.

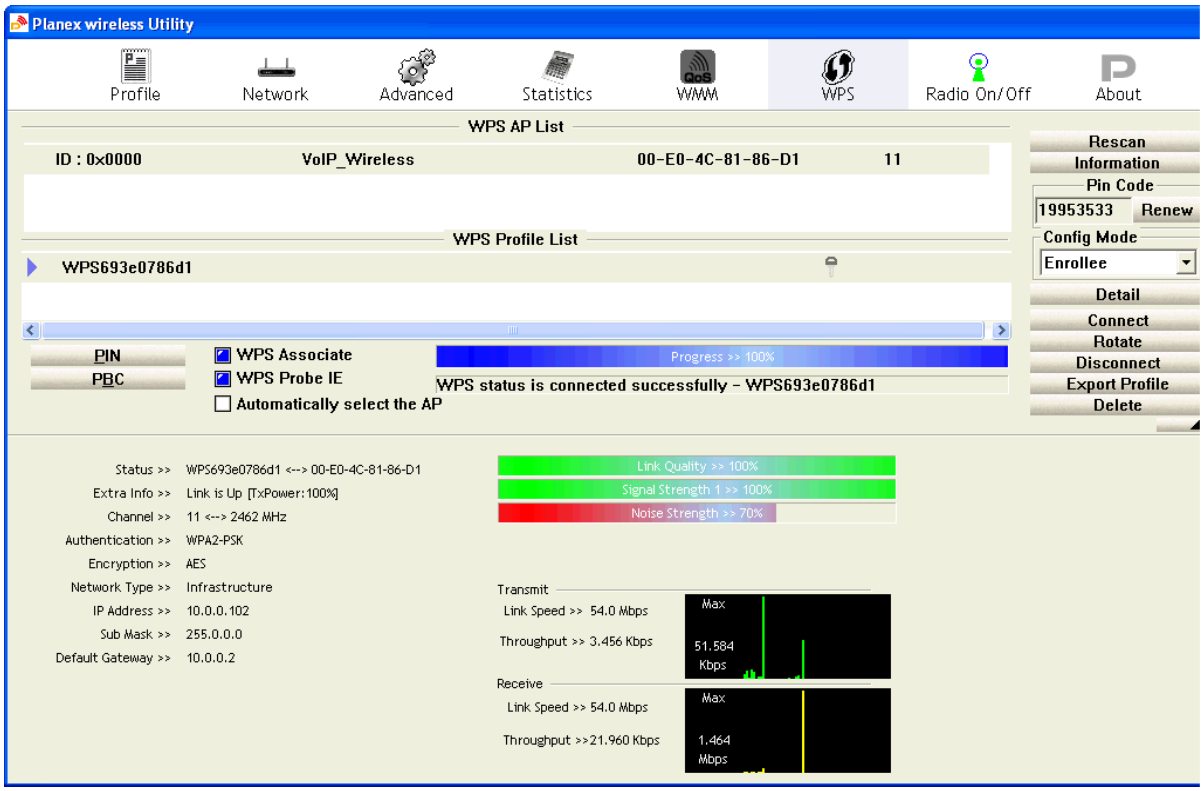


6. Users must start the PIN method on the station side within two minutes.

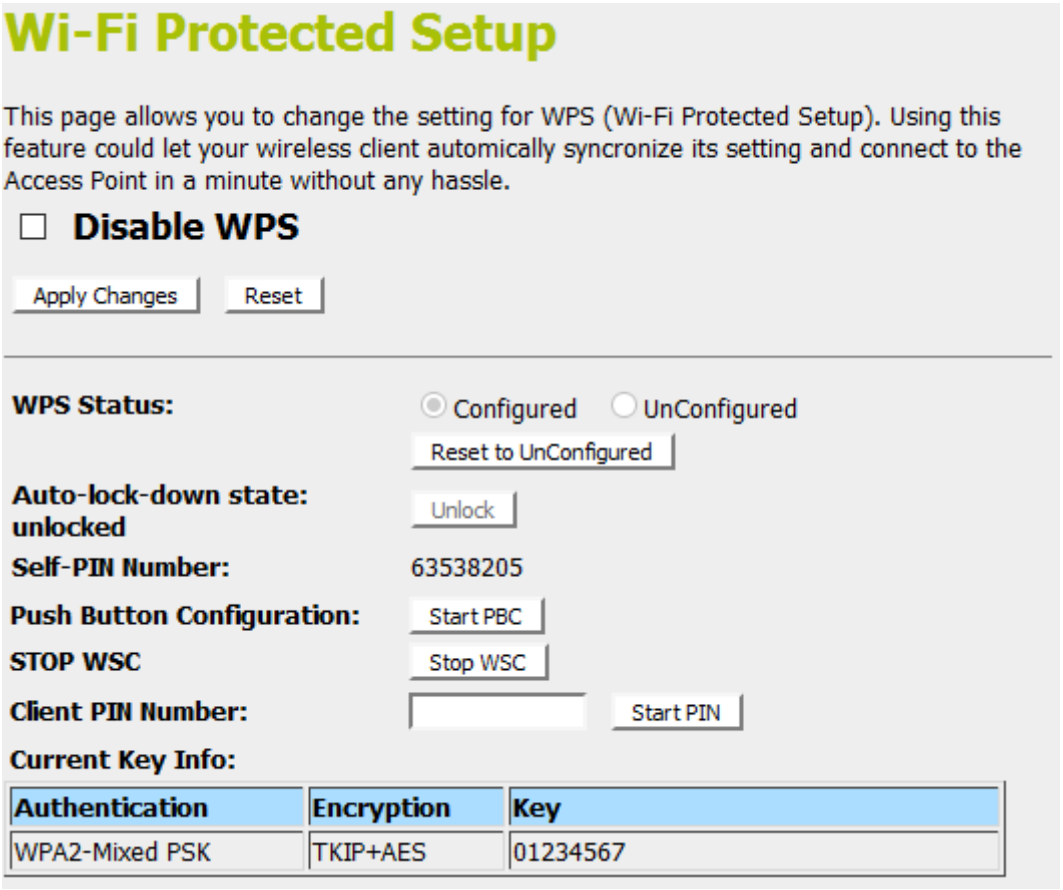
7. Users must start the PIN method on the station side within two minutes.



8. If the device PIN is correct and the WPS handshake is successfully doneon the station side, User's Wi-Fi Protected status will be shown as below.



9. If the device PIN is correct and the WPS handshake is successfully done, AP's Wi-Fi Protected Setup page will be shown as below.



Other pages such as *Wireless Basic Settings page* and *Wireless Security Setup page* will also be updated appropriately as described in previous sections. In this case, AP is in un-configured state before the station initiates the WPS handshake. According to the WPS spec, AP will create a wireless profile with WPA2-mixed mode and a random-generated key upon successfully doing the WPS handshake. However, AP will use the original wireless profile and give it to the station if AP is already in configured state. That means all settings of AP will not change. Hence, all WPS related pages keep the same.

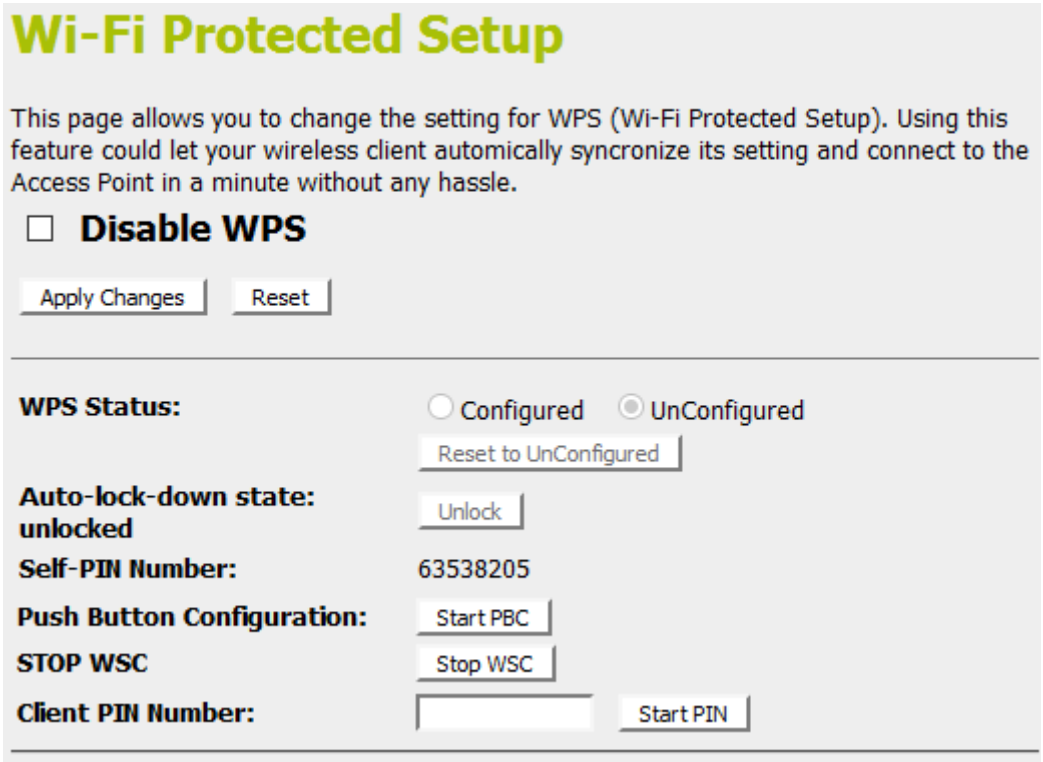
Push Button method

Wireless Gateway supports a virtual button “Start PBC” on the *Wi-Fi Protected Setup page* for Push Button method. If userspush a virtual button “Start PBC”, AP will initiate a WPS session and wait for any station to join. At this moment, AP will detect whether there is more than one station that starts the PBC method. When multiple PBC sessions occur, users should try PIN method.

After users push AP’s virtual button “Start PBC”, they must go to station side to push its button within two minutes. If the WPS is successfully done, AP will give its wireless profile to that station. The station could use this profile to associate with AP.

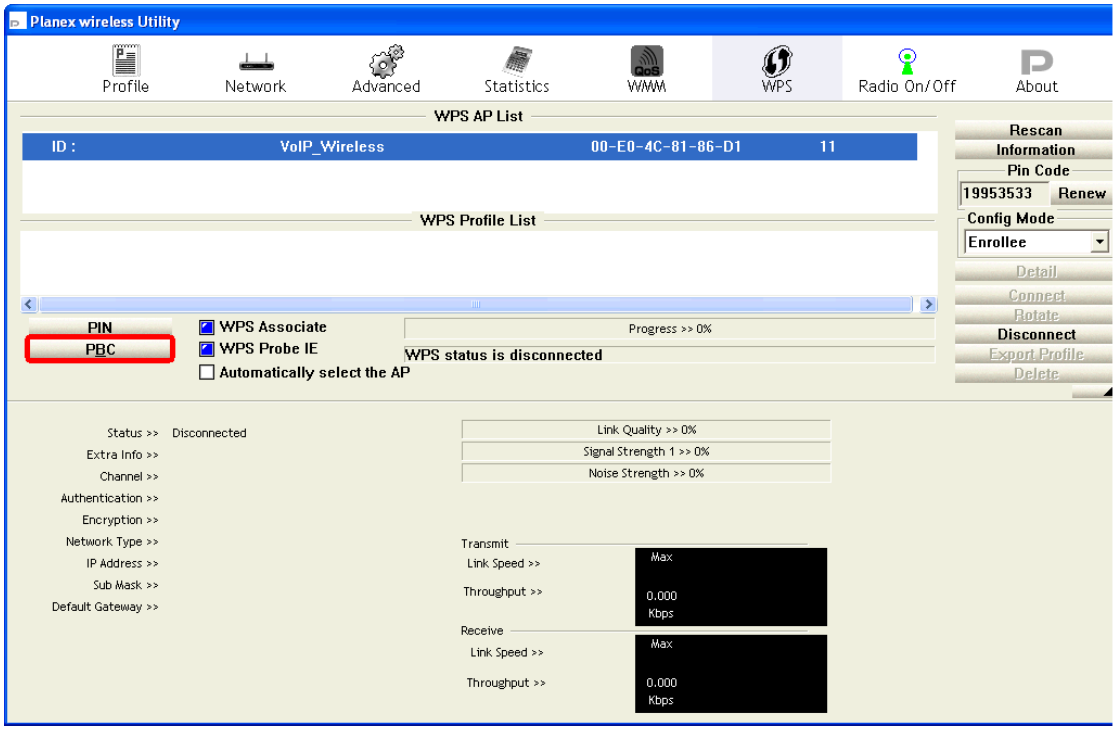
1. From the head menu, click on *WAN1*.

2. From the left-hand menu, click on *WPS*. The following page is displayed:
3. Make sure AP is in un-configured state.
4. Click *Start PBC*.

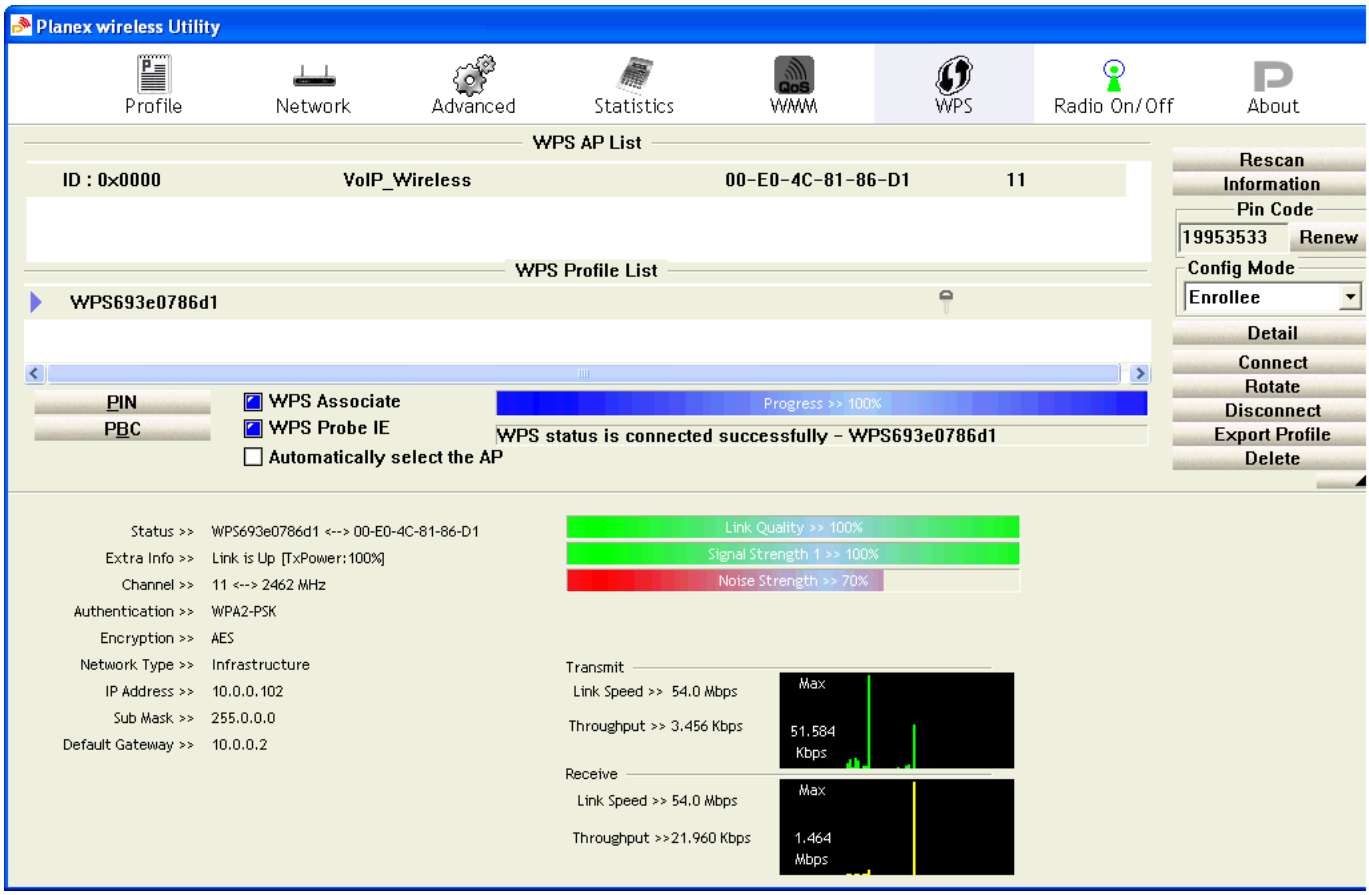


5. Users must start the PBC method on the station side within two minutes.

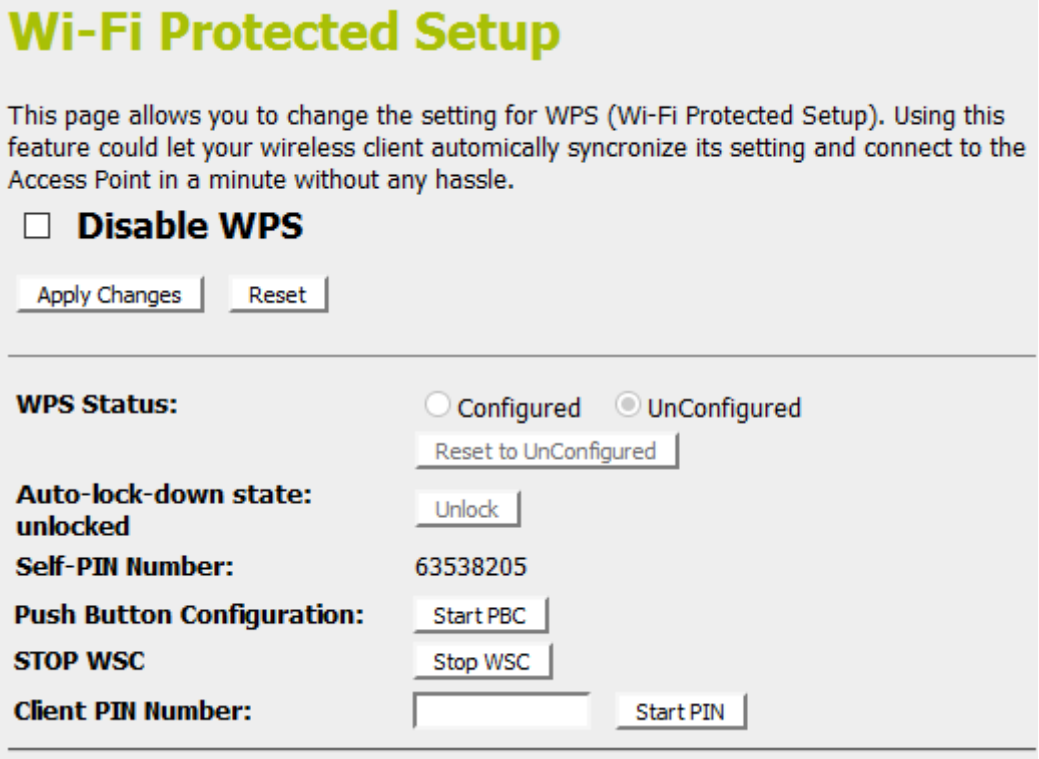
6. Users must start the PBC method on the station side within two minutes.



7. If the device PCB and the WPS handshake is successfully doneon the station side, User's Wi-Fi Protected status will be shown as below.



8. If the device PIN is correct and the WPS handshake is successfully done, AP's Wi-Fi Protected Setup page will be shown as below.



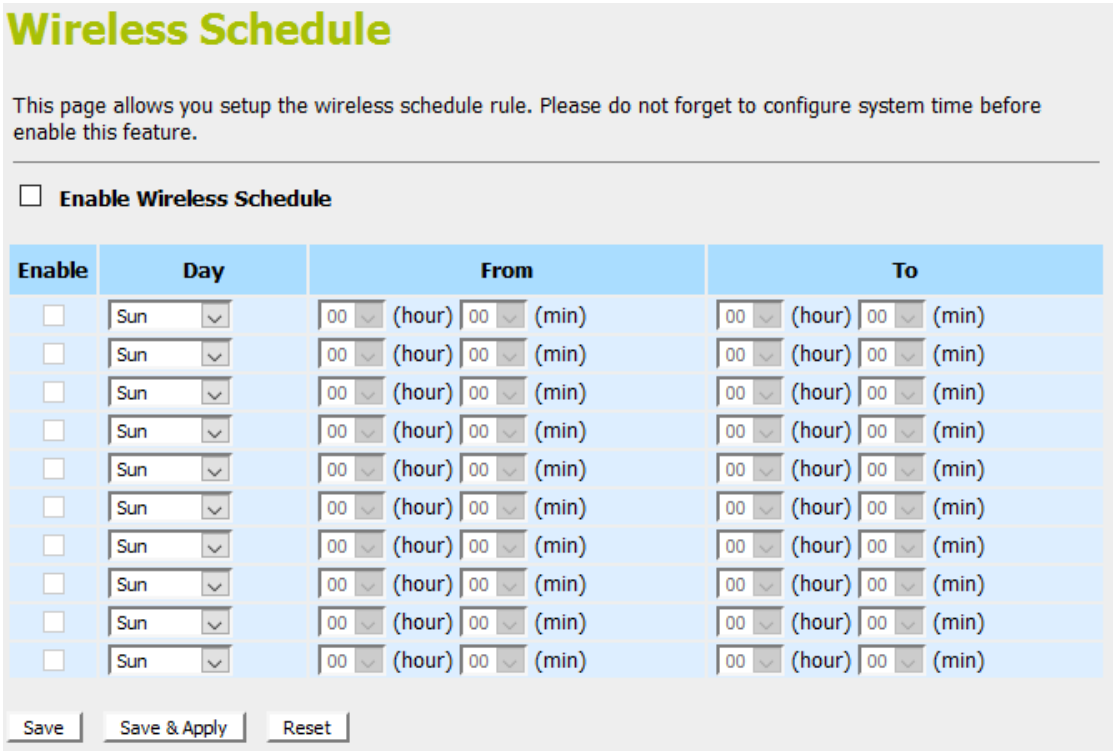
Other pages such as *Wireless Basic Settings page* and *Wireless Security Setup page* will also be updated appropriately as described in previous sections. In this case, AP is in un-configured state before the station initiates the WPS handshake. According to the WPS spec, AP will create a wireless profile with WPA2-mixed mode and a random-generated key upon successfully doing the WPS handshake. However, AP will use the original wireless profile and give it to the station if AP is already in configured state. That means all settings of AP will not change. Hence, all WPS related pages keep the same.

Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature. To access the *Wireless Schedule*page:

1. From the head menu, click on *WAN1*.

2. From the left-hand menu, click on *Wireless Schedule*. The following page is displayed:



11 LAN Interface

This chapter is to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc...

Note

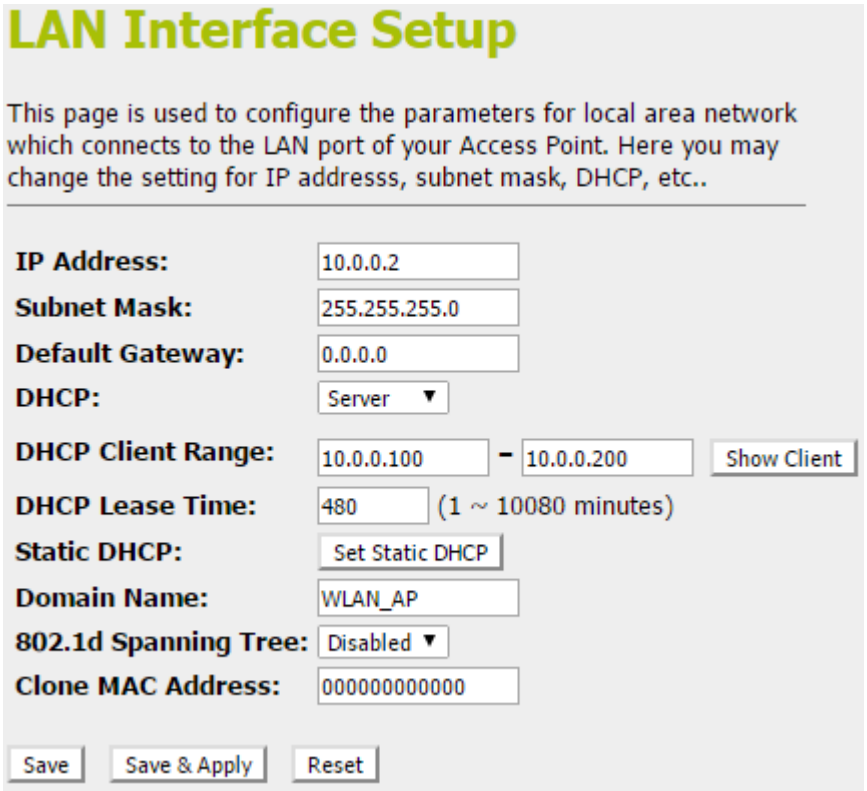
You should only change the addressing details if your ISP asks you to, or if you are familiar with network configuration. In most cases, you will not need to make any changes to this configuration.

LAN Interface Setup

To check the configuration of LAN Interface:

1. From the head menu, click on *TCP/IP*.

2. From the left-hand menu, click on *LAN Setting*. The following page is displayed:



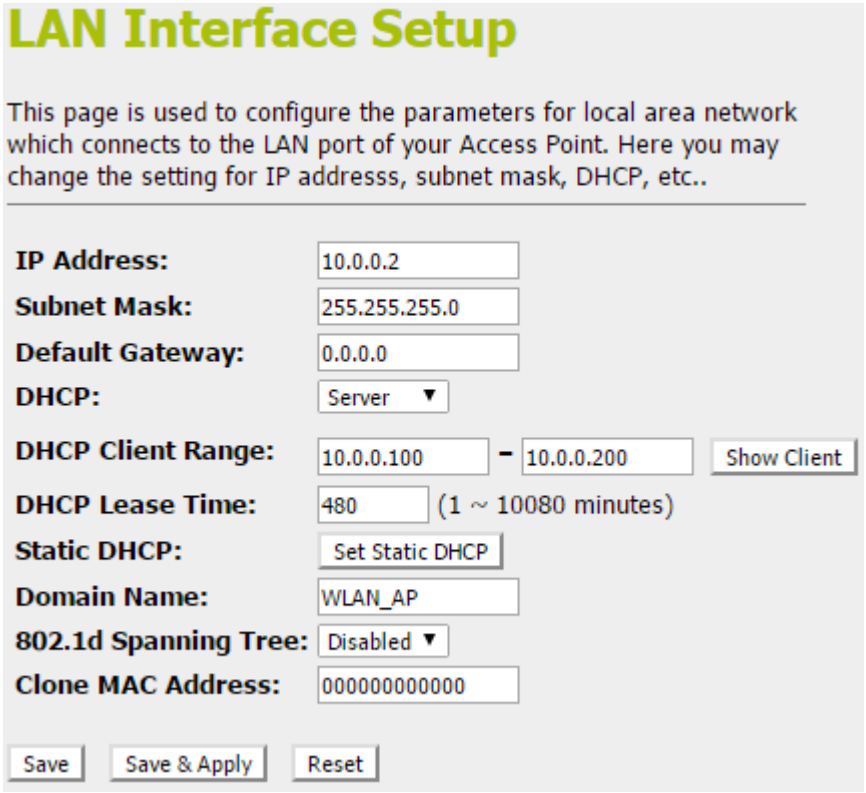
Field	Description
IP Address	**The LAN IP address** **Default: 10.0.0.2**
Subnet Mask	**The LAN netmask** **Default: 255.255.255.0**
Default Gateway	**The LAN Gateway** **Default: 0.0.0.0**
DHCP	**DHCP Type: Disable, DHCP Client or Server** **Default: DHCP Server**
DHCPClientRange	**Specify the starting/ending IP address of the IP address pool.** **Default Start IP: 10.0.0.100** **Default Ending IP: 10.0.0.200**
DHCP Lease Time	**Configure DHCP Lease Time**
Static DHCP	**Set Static DHCP**
Show Client	**DHCP client computers/devices connected to the device will have their information displayed in the DHCP Client List table. The table will show the IP Address, MAC Address, and Expired Time of the DHCP lease for each client computer/device.**
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.**
802.1d Spanning Tree	**Enable or Disable Spanning Tree**
Clone MAC Address	**MAC Spoofing on LAN** **Default: 000000000000**

Changing the LAN IP address and subnet mask

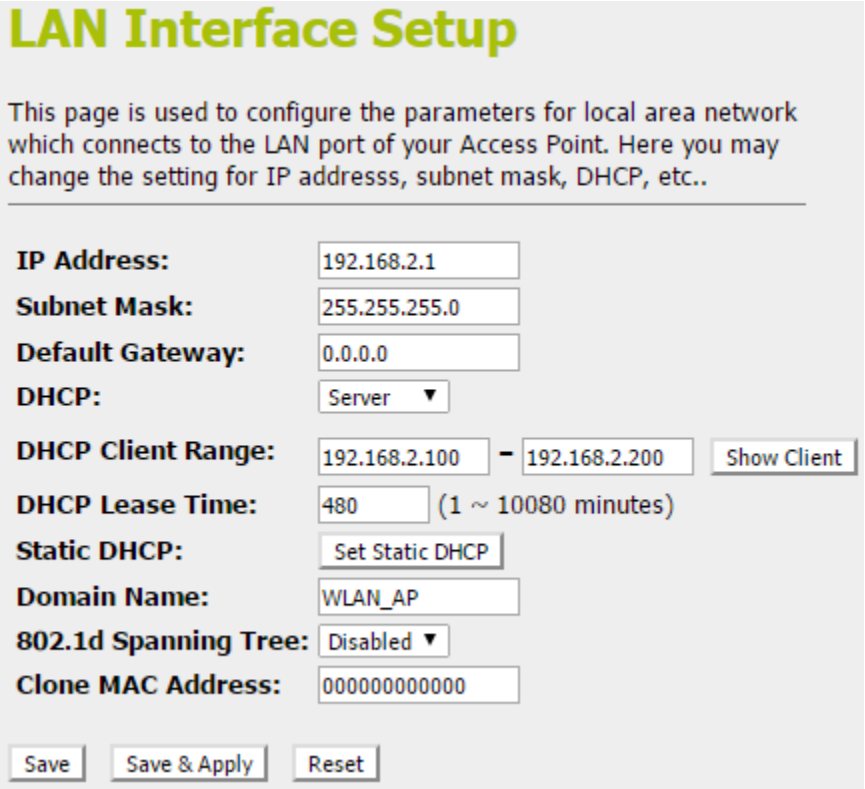
To check the configuration of LAN Interface:

1. From the head menu, click on *TCP/IP*.

2. From the left-hand menu, click on *LAN Setting*. The following page is displayed:



3. Type IP Address and*Change default LAN port IP address*.
4. Click in the *IP Address and Subnet Mask* box and type a new IP Address and Subnet Mask.
5. Change the *default DHCPClientRange*.
6. Click *Save & Apply*.



7. Change setting successfully! Please wait 20 seconds….

You may also need to renew your DHCP lease:

Windows 95/98

a. Select **Run...** from the **Start** menu.

b. Enter **winipcfg** and click **OK**.

c. Select your ethernet adaptor from the pull-down menu

d. Click **Release All** and then **Renew All**.

e. **Exit** the winipcfg dialog.

Windows NT/Windows 2000/Windows XP

a. Bring up a command window.

b. Type **ipconfig /release** in the command window.

c. Type **ipconfig /renew**.

d. Type **exit** to close the command window.

Linux

a. Bring up a shell.

b. Type **pump -r** to release the lease.

c. Type **pump** to renew the lease.

Note

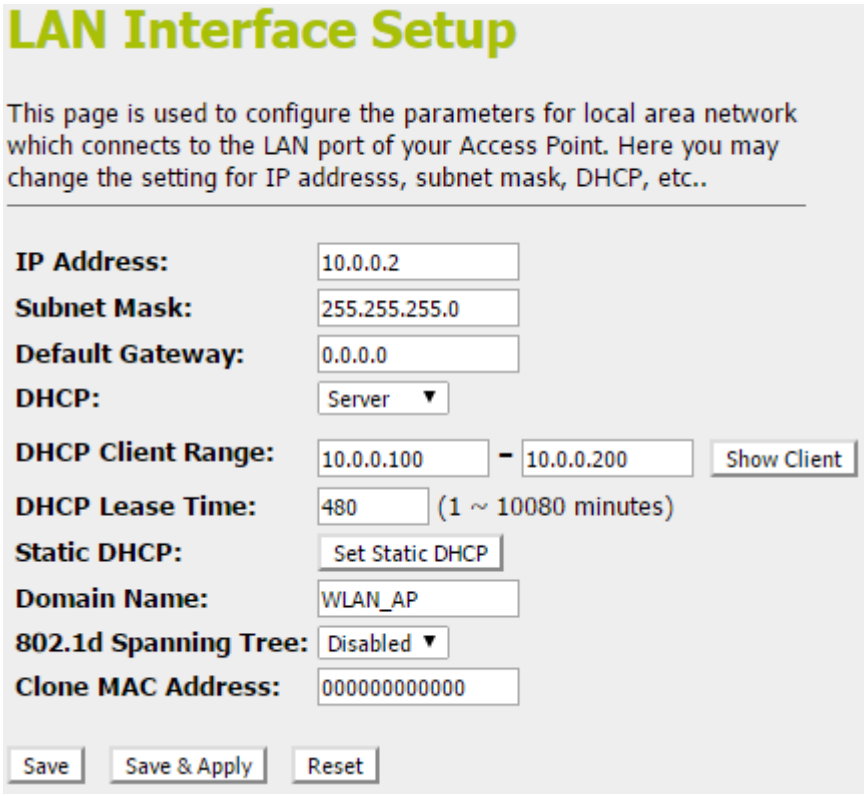
If you change the LAN IP address of the device while connected through your Web browser, you will be disconnected. You must open a new connection by entering your new LAN IP address as the URL.

Show Client

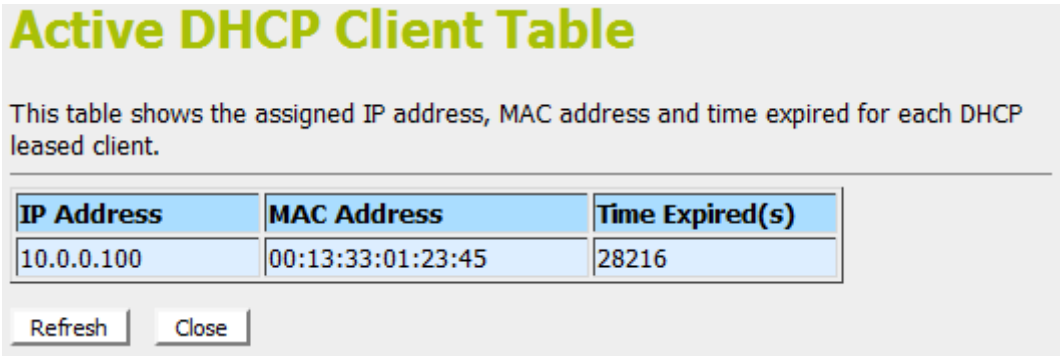
To the IP Address, MAC Address, and Expired Time of the DHCP lease for each client computer/device:

1. From the head menu, click on *TCP/IP*.

2. From the left-hand menu, click on *LAN Setting*. The following page is displayed:



3. Click on *Show Client* button. The following page is displayed:



12 WAN Interface

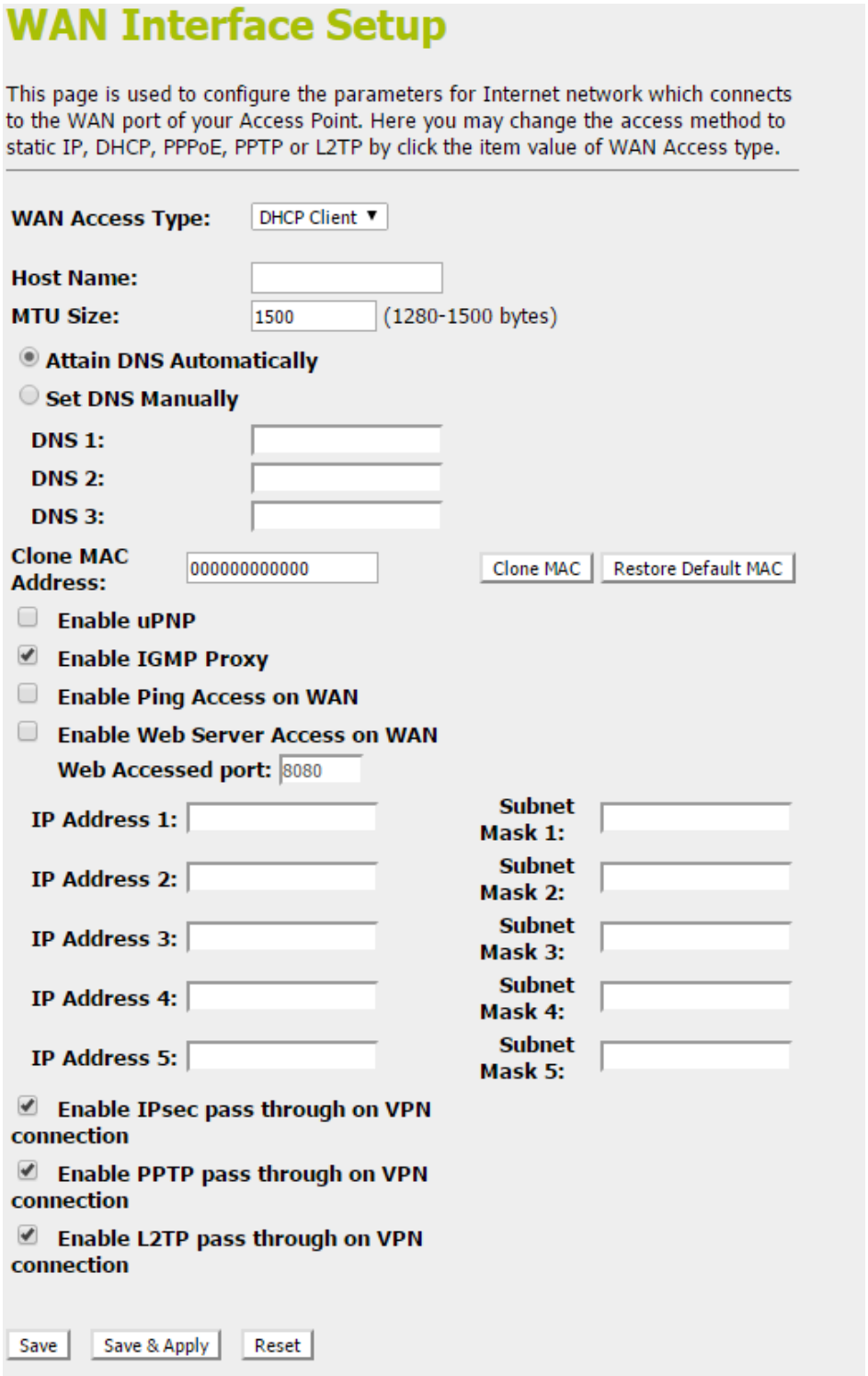
This chapter describes how to configure the way that your device connects to the Internet. Your ISP determines what type of Internet access you should use and provides you with any information that you need in order to configure the Internet access to your device.

Wireless Gateway supports four methods of obtaining the WAN IP address:

Option	Description
Static IP	**Choose this option if you are a leased line user with a fixed IP address.**
DHCP Client	**Choose this option if you are connected to the Internet through a Cable modem line.**
PPPoE	**Choose this option if you are connected to the Internet through a DSL line**
PPTP	**Choose this option if you are connected to the PPTP Server**
L2TP	**Choose this option if you are connected to the L2TP Server**

1. From the head menu, click on *TCP/IP*.

2. From the left-hand menu, click on *WAN Setting*. The following page is displayed:



Option		Description
WAN Access Type	**Static IP**	**Choose this option if you are a leased line user with a fixed IP address.**
	DHCP Client	**Choose this option if you are connected to the Internet through a Cable modem line.**
	PPPoE	**Choose this option if you are connected to the Internet through a DSL line**
	PPTP	**Choose this option if you are connected to the PPTP Server**
	L2TP	**Choose this option if you are connected to the L2TP Server**
Host Name		**The name of the DHCP host**
IP Address		**Check with your ISP provider**
Subnet Mask		**Check with your ISP provider**
Default Gateway		**Check with your ISP provider**
User Name		**User name for PPPoE registration recognized by the Internet service provider**
Password		**Password for PPPoE registration recognized by the Internet service provider**
Service Name		**Service Name for PPPoE registration recognized by the Internet service provider**
Connection Type	**Continuous**	**The connection is always on**
	Connect on Demand	**Enter the minutes after which the session must be disconnected, if no activity takes place**
	Manual	**Manually connect**
Idle Time		**Enter the minutes after which the session must be disconnected**
WAN Physical		**Dynamic IP or Static IP for PPP Connection**
MTU Size		**Specify the network MTU rate**
Attain DNS Automatically		**Obtain DNS server address automatically**
DNS 1 (Primary DNS Server)		**Check with your ISP provider**
DNS 2 (Secondary DNS Server)		**Check with your ISP provider**
DNS 3 (Third DNS Server)		**Check with your ISP provider**

Option	Description
Clone MAC Address	**Clone MAC lets the device identify itself as another computer or device**
Enable uPNP	**Enable or Disable uPNP**
Enable IGMP Proxy	**Enable or Disable IGMP Proxy**
Enable Ping Access on WAN	**Enable or Disable Ping Access on WAN**
Enable Web Server Access on WAN	**Enable or Disable Web Server Access on WAN**
Enable IPsec pass through on VPN connection	**Enable or Disable IPsec pass through on VPN connection**
Enable PPTP pass through on VPN connection	**Enable or Disable PPTP pass through on VPN connection**
Enable L2TP pass through on VPN connection	**Enable or Disable L2TP pass through on VPN connection**

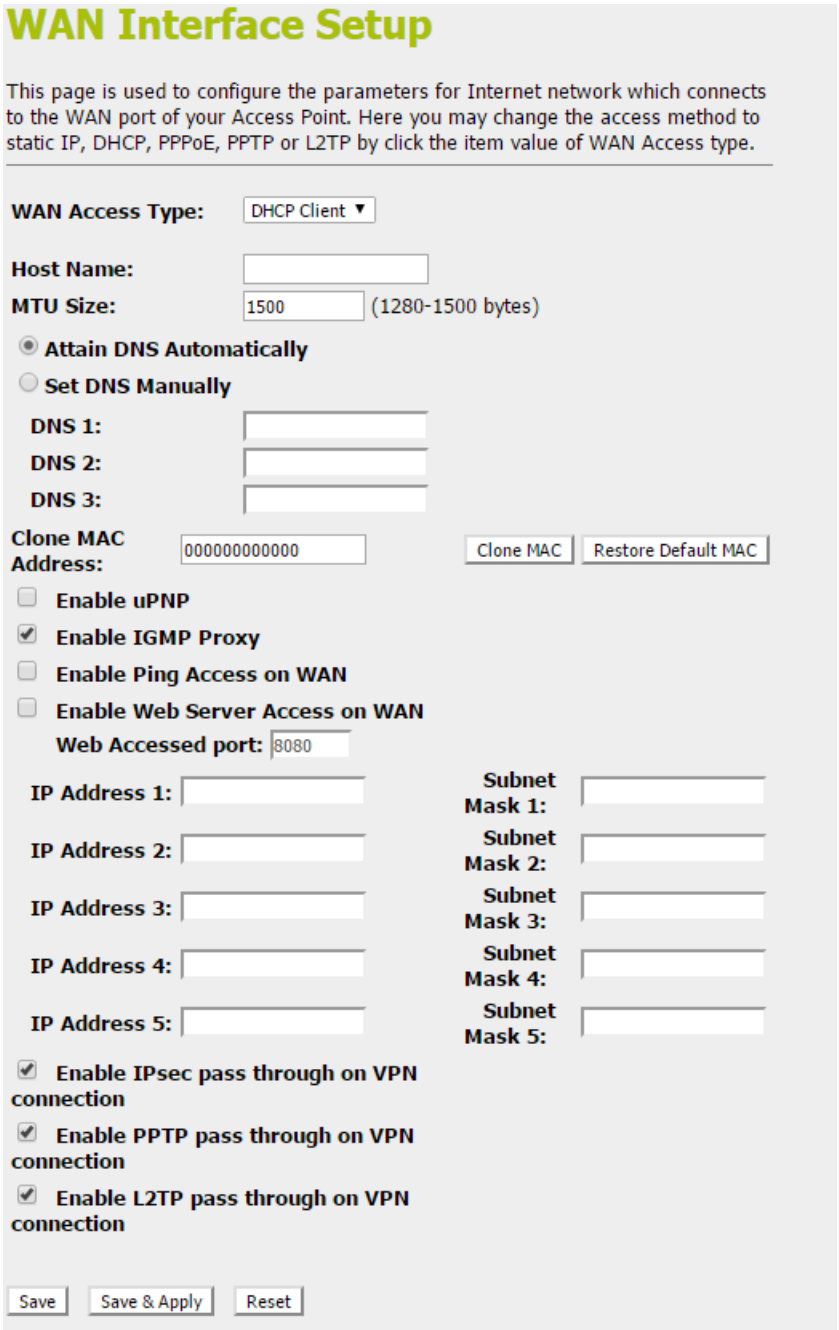
Configuring Static IP connection

If you are a leased line user with a fixed IP address, enter in the IP address, subnet mask, gateway address, and DNS (domain name server) address(es) provided to you by your ISP.

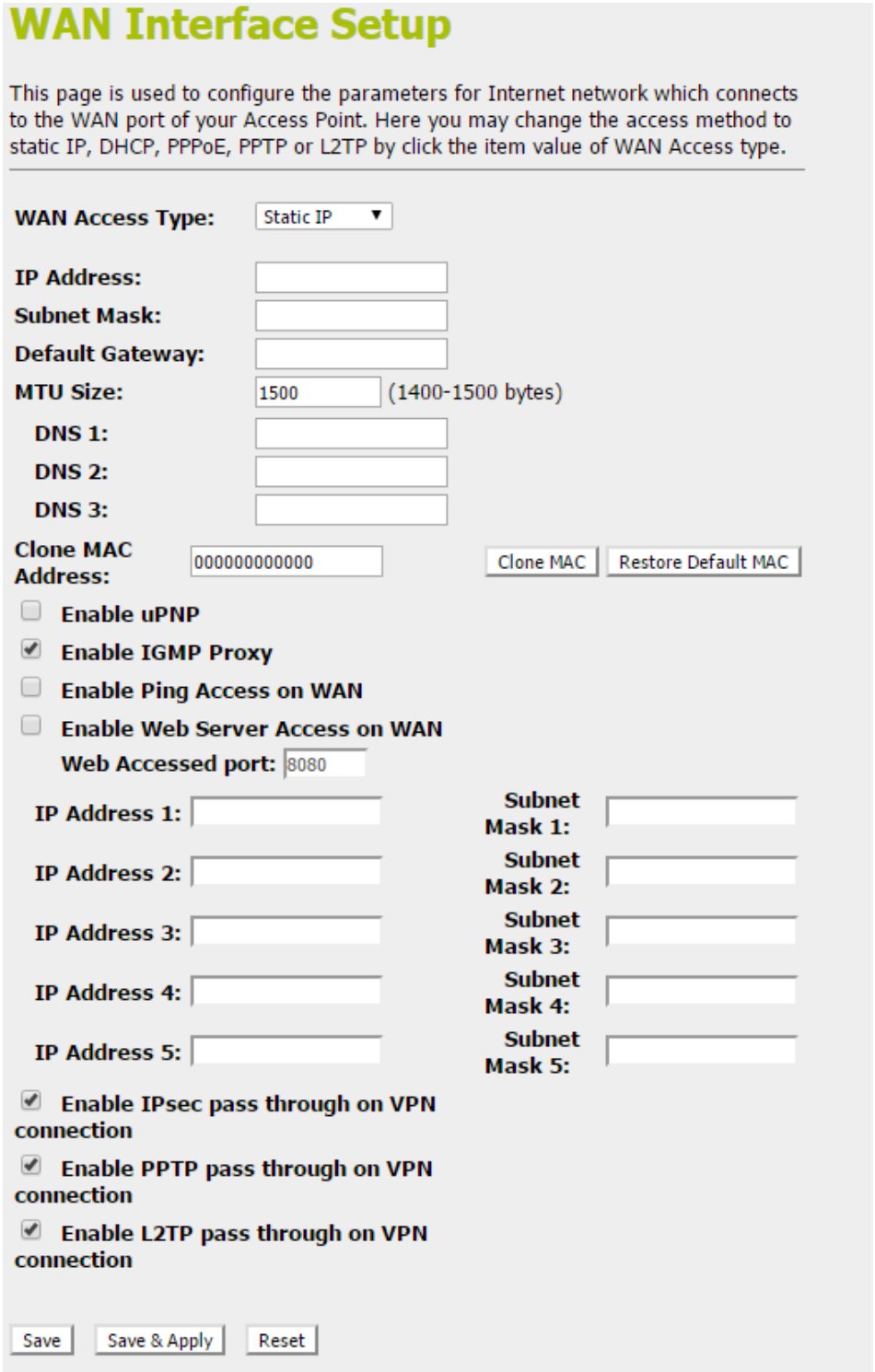
If your ISP wants you to connect to the Internet using Static IP, follow the instructions below.

1. From the head menu, click on *TCP/IP*.

2. From the left-hand menu, click on *WAN Setting*. The following page is displayed:



3. From the *WAN Access Type*drop-down list, select *Static IP*setting.
4. Enter*WAN IP Address,WAN Subnet Mask, Default Gateway* and*DNS* which was given by Telecom or by your Internet Service Provider (ISP).
5. Click *Save & Apply*.



6. Change setting successfully! Please wait 20 seconds….

Configuring DHCP Client connection

Dynamic Host Configuration Protocol (DHCP), Dynamic IP (Get WAN IP Address automatically). If you are connected to the Internet through a Cable modem line, then a dynamic IP will be assigned.

If your ISP wants you to connect to the Internet using DHCP Client, follow the instructions below.

1. From the head menu, click on *TCP/IP*.

2. From the left-hand menu, click on *WAN Setting*. The following page is displayed:

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client ▼

Host Name:

MTU Size: 1500 (1280-1500 bytes)

- (•) **Attain DNS Automatically**
- ( ) **Set DNS Manually**

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000 Clone MAC | Restore Default MAC

- [ ] **Enable uPNP**
- [x] **Enable IGMP Proxy**
- [ ] **Enable Ping Access on WAN**
- [ ] **Enable Web Server Access on WAN**

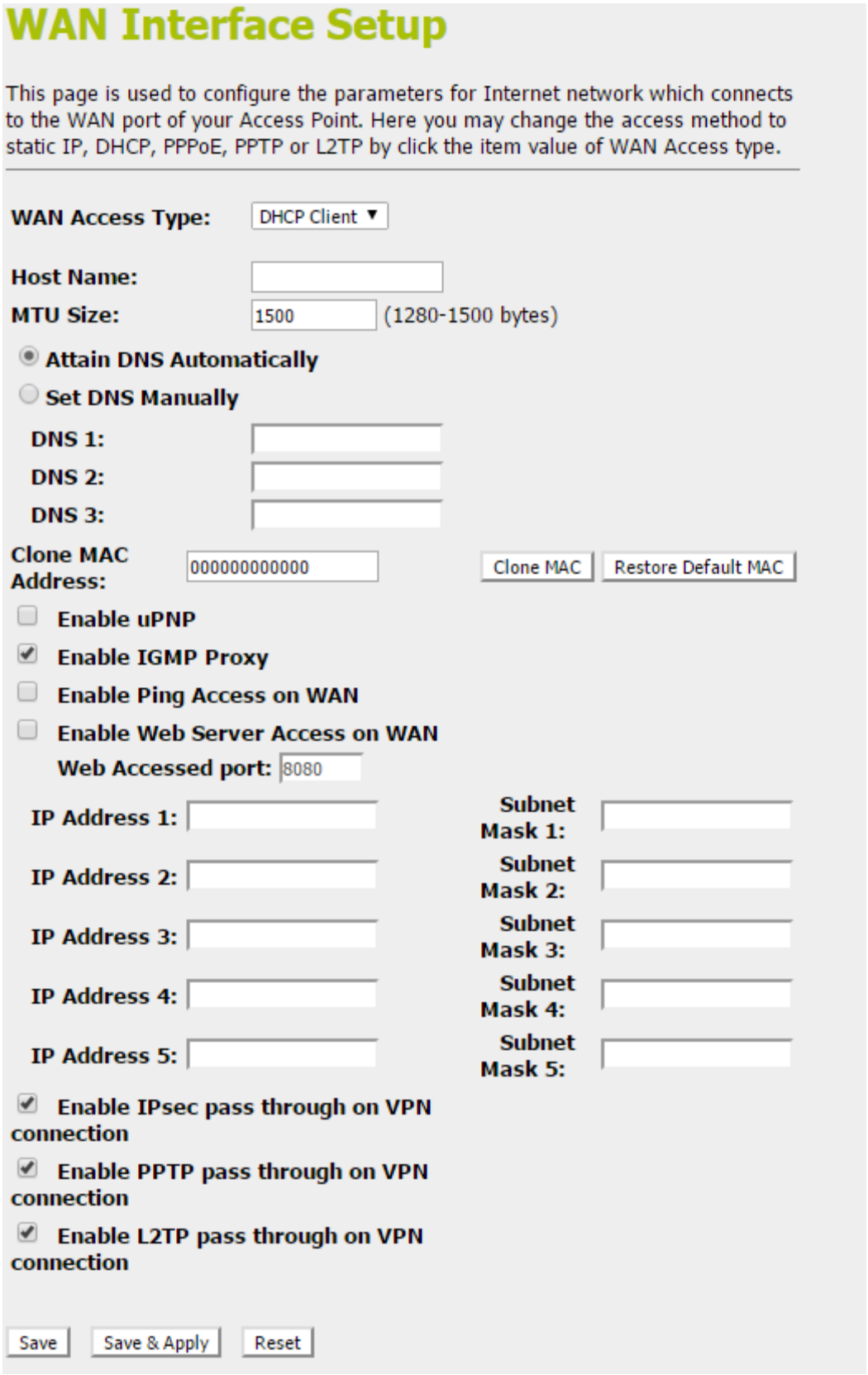
Web Accessed port: 8080

IP Address 1:		**Subnet Mask 1:**	
IP Address 2:		**Subnet Mask 2:**	
IP Address 3:		**Subnet Mask 3:**	
IP Address 4:		**Subnet Mask 4:**	
IP Address 5:		**Subnet Mask 5:**	

- [x] **Enable IPsec pass through on VPN connection**
- [x] **Enable PPTP pass through on VPN connection**
- [x] **Enable L2TP pass through on VPN connection**

Save | Save & Apply | Reset

3. From the *WAN Access Type*drop-down list, select *DHCP Client*setting.
4. Click *Save & Apply*.



5. Change setting successfully! Please wait 20 seconds….

Configuring PPPoE connection

If your ISP's Internet service uses PPPoE you need to set up a PPP login account. The first time that you login to the Internet, your ISP will ask you to enter a username and password so they can check that you are a legitimate, registered Internet service user. Your device stores these authentication details, so you will not have to enter this username and password every time you login.

If your ISP wants you to connect to the Internet using PPP, follow the instructions below.

1. From the head menu, click on *TCP/IP*.

2. From the left-hand menu, click on *WAN Setting*. The following page is displayed:

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client ▼

Host Name:

MTU Size: 1500 (1280-1500 bytes)

- (•) **Attain DNS Automatically**
- ( ) **Set DNS Manually**

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000 Clone MAC | Restore Default MAC

- [ ] **Enable uPNP**
- [x] **Enable IGMP Proxy**
- [ ] **Enable Ping Access on WAN**
- [ ] **Enable Web Server Access on WAN**

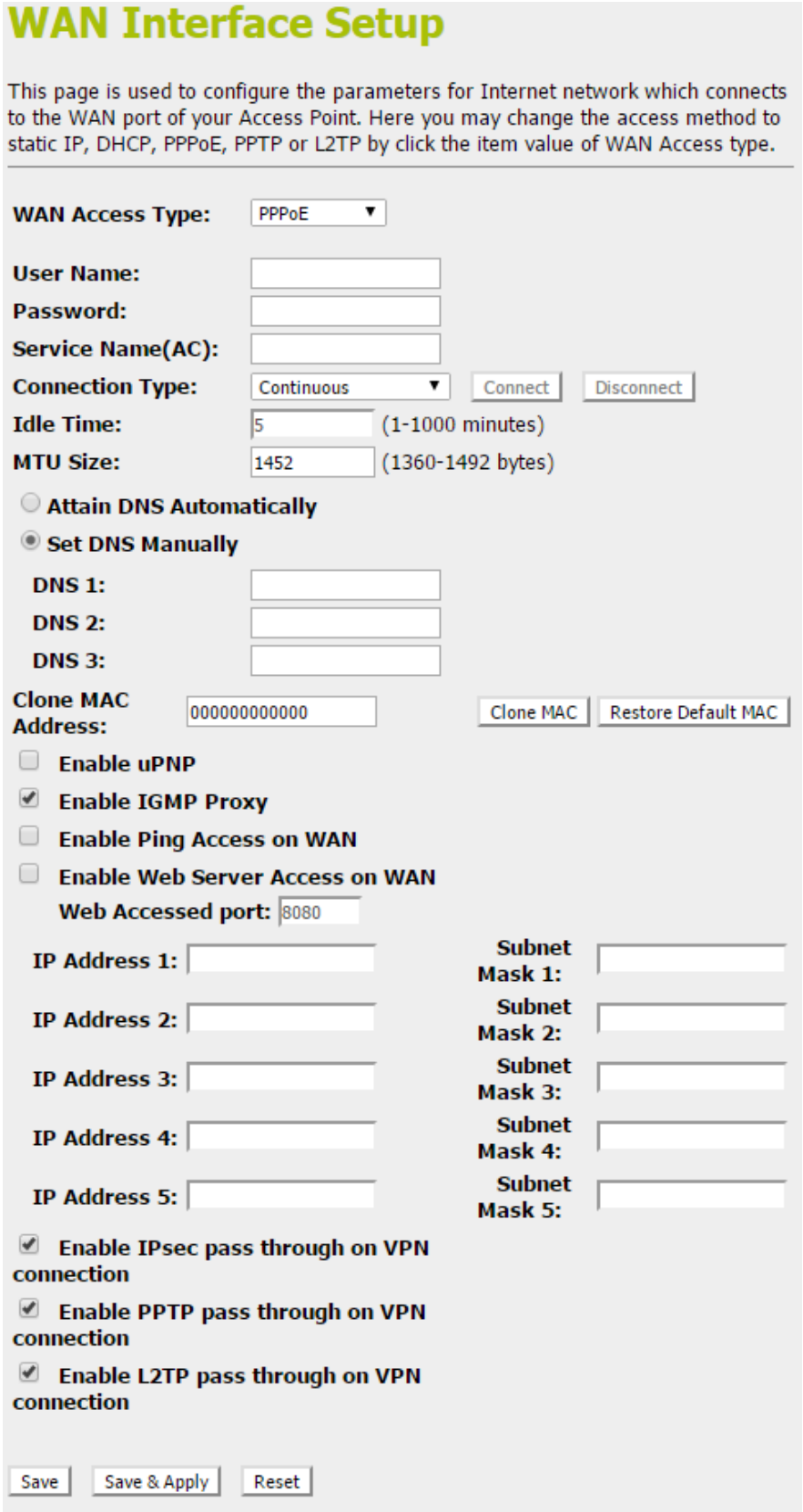
Web Accessed port: 8080

IP Address 1:		**Subnet Mask 1:**	
IP Address 2:		**Subnet Mask 2:**	
IP Address 3:		**Subnet Mask 3:**	
IP Address 4:		**Subnet Mask 4:**	
IP Address 5:		**Subnet Mask 5:**	

- [x] **Enable IPsec pass through on VPN connection**
- [x] **Enable PPTP pass through on VPN connection**
- [x] **Enable L2TP pass through on VPN connection**

Save | Save & Apply | Reset

3. From the *WAN Access Type*drop-down list, select *PPPoE*setting.
4. Enter*User Name/Password* provided by your ISP. Type them in the relevant boxes.
5. Click *Save & Apply*.



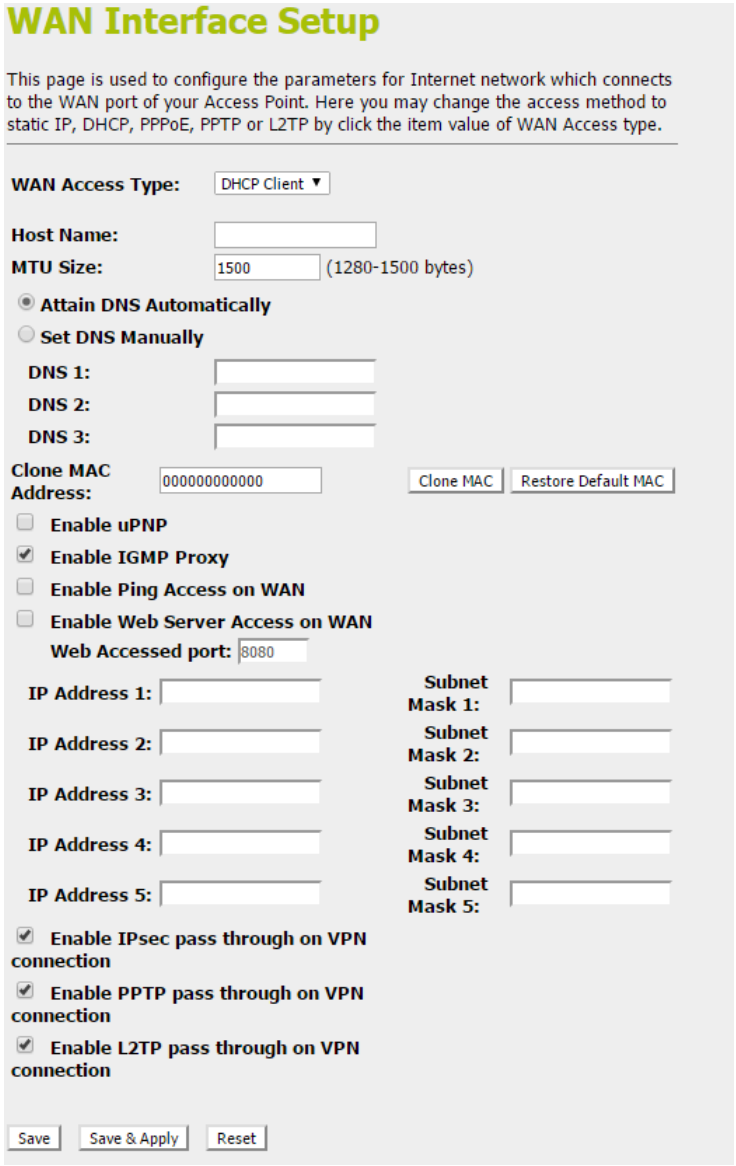
6. Change setting successfully! Please wait 20 seconds….

Configuring PPTP connection

If your ISP/Network Administrator wants you to connect to the Internet using PPTP, follow the instructions below.

1. From the head menu, click on *TCP/IP*.

2. From the left-hand menu, click on *WAN Setting*. The following page is displayed:



3. From the *WAN Access Type* drop-down list, select *PPTP* setting.
4. Enter *IP Address/Subnet Mask/Default Gateway* provided by your ISP. Type them in the relevant boxes. (for Static IP only)
5. Select *PPTP Server Mode*.
6. Enter *Server Domain Address/User Name/Password* provided by your ISP. Type them in the relevant boxes.
7. Click *Save & Apply*.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: PPTP

- Dynamic IP (DHCP)
- Static IP

IP Address: 172.1.1.2
Subnet Mask: 255.255.255.0
Default Gateway: 172.1.1.254

- Attain Server By Domain Name
- Attain Server By Ip Address

Domain Name:
Server IP Address: 172.1.1.1
User Name:
Password:
Connection Type: Continuous Connect Disconnect
Idle Time: 5 (1-1000 minutes)
MTU Size: 1460 (1400-1460 bytes)

- Request MPPE Encryption
- Request MPPC Compression

- Attain DNS Automatically
- Set DNS Manually

DNS 1:
DNS 2:
DNS 3:

Clone MAC Address: 000000000000 Clone MAC Restore Default MAC

- Enable uPNP
- Enable IGMP Proxy
- Enable Ping Access on WAN
- Enable Web Server Access on WAN

Web Accessed port: 8080

IP Address 1:		**Subnet Mask 1:**	
IP Address 2:		**Subnet Mask 2:**	
IP Address 3:		**Subnet Mask 3:**	
IP Address 4:		**Subnet Mask 4:**	
IP Address 5:		**Subnet Mask 5:**	

- Enable IPsec pass through on VPN connection
- Enable PPTP pass through on VPN connection
- Enable L2TP pass through on VPN connection

Save Save & Apply Reset

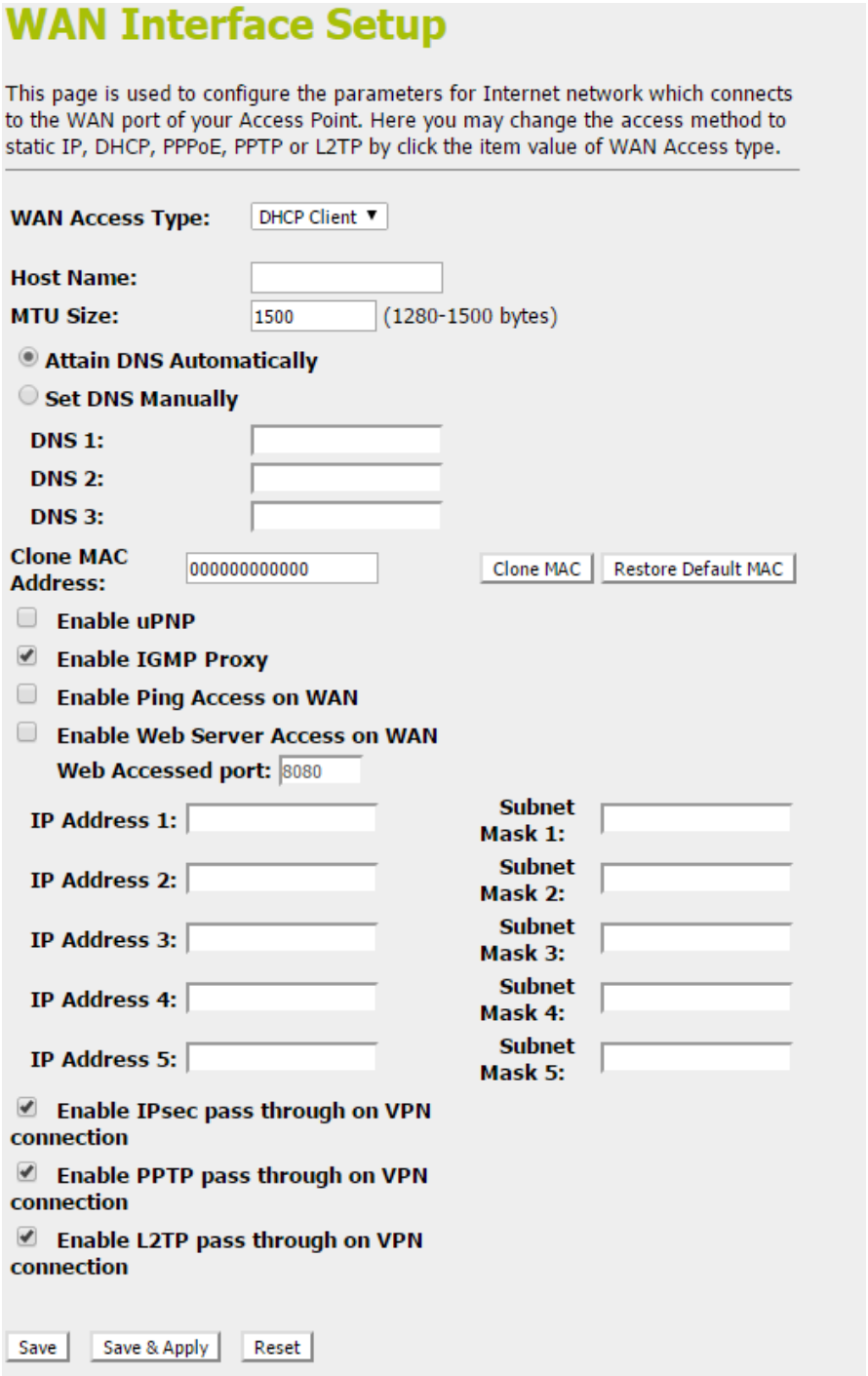
8. Change setting successfully! Please wait 20 seconds….

Configuring L2TP connection

If your ISP/Network Administrator wants you to connect to the Internet using L2TP, follow the instructions below.

1. From the head menu, click on *TCP/IP*.

2. From the left-hand menu, click on *WAN Setting*. The following page is displayed:



3. From the *WAN Access Type* drop-down list, select *L2TP* setting.
4. Enter *IP Address/Subnet Mask/Default Gateway* provided by your ISP. Type them in the relevant boxes. (for Static IP only)
5. Select *L2TP Server Mode*.
6. Enter *Server Domain Address/User Name/Password* provided by your ISP. Type them in the relevant boxes.
7. Click *Save & Apply*.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: L2TP

- (•) **Dynamic IP (DHCP)**
- ( ) **Static IP**

IP Address: 172.1.1.2
Subnet Mask: 255.255.255.0
Default Gateway: 172.1.1.254

- ( ) **Attain Server By Domain Name**
- (•) **Attain Server By Ip Address**

Domain Name:
Server IP Address: 172.1.1.1
User Name:
Password:
Connection Type: Continuous [Connect] [Disconnect]
Idle Time: 5 (1-1000 minutes)
MTU Size: 1460 (1400-1460 bytes)

- ( ) **Attain DNS Automatically**
- (•) **Set DNS Manually**

DNS 1:
DNS 2:
DNS 3:

Clone MAC Address: 000000000000 [Clone MAC] [Restore Default MAC]

- [ ] **Enable uPNP**
- [x] **Enable IGMP Proxy**
- [ ] **Enable Ping Access on WAN**
- [ ] **Enable Web Server Access on WAN**

Web Accessed port: 8080

IP Address 1:		**Subnet Mask 1:**	
IP Address 2:		**Subnet Mask 2:**	
IP Address 3:		**Subnet Mask 3:**	
IP Address 4:		**Subnet Mask 4:**	
IP Address 5:		**Subnet Mask 5:**	

- [x] **Enable IPsec pass through on VPN connection**
- [x] **Enable PPTP pass through on VPN connection**
- [x] **Enable L2TP pass through on VPN connection**

[Save] [Save & Apply] [Reset]

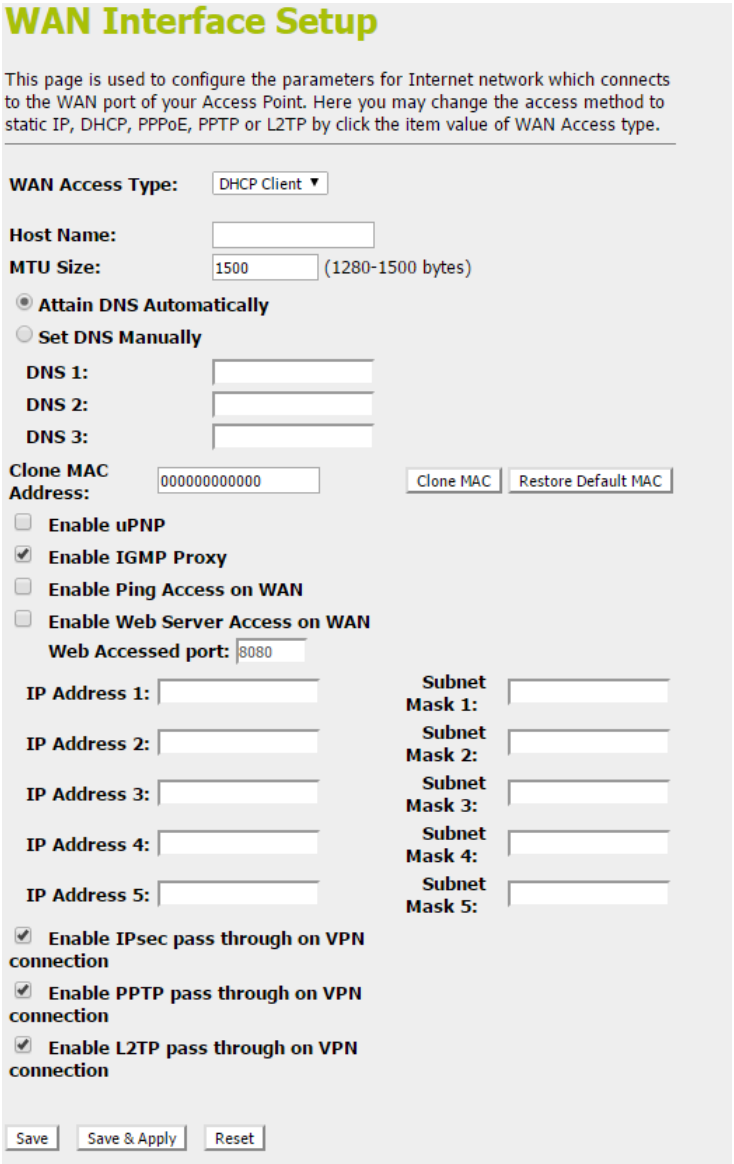
8. Change setting successfully! Please wait 20 seconds….

Configuring L2TP connection

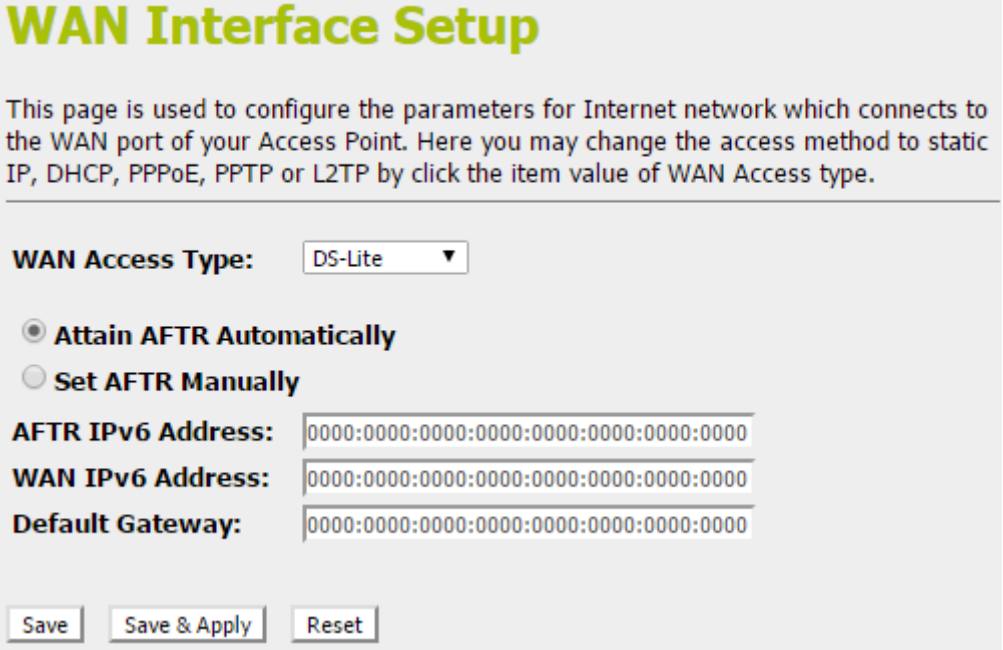
If your ISP/Network Administrator wants you to connect to the Internet using L2TP, follow the instructions below.

9. From the head menu, click on *TCP/IP*.

10. From the left-hand menu, click on *WAN Setting*. The following page is displayed:



11. From the *WAN Access Type* drop-down list, select *DS-Lite* setting.
12. Configure related settings provided by your ISP. Type them in the relevant boxes.
13. Click *Save & Apply*.



14. Change setting successfully! Please wait 20 seconds….

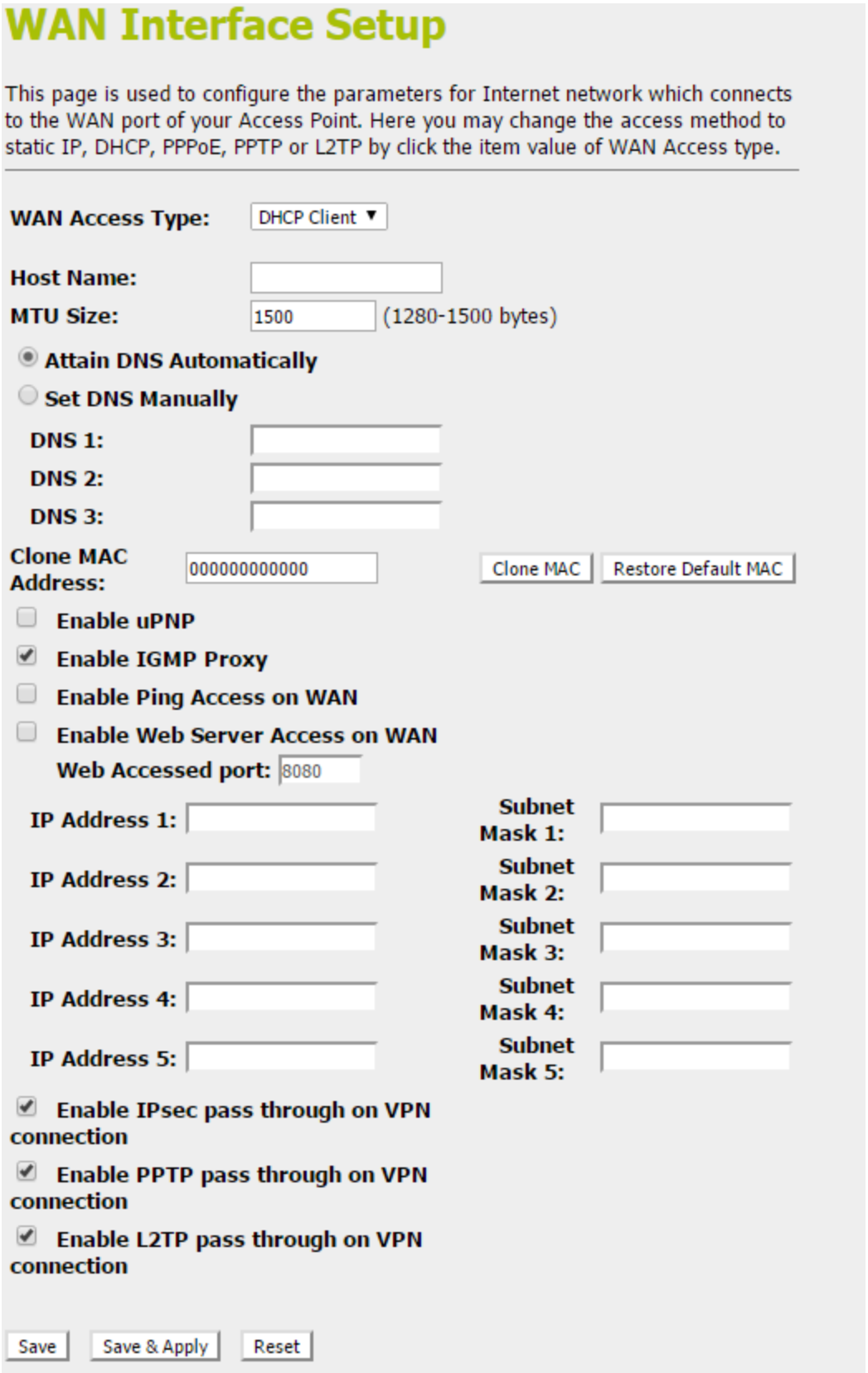
Clone MAC Address

Some particularly ISPs do not want you to have a home network and have a DSL/Cable modem that allows only 1 MAC to talk on the internet. If you change network cards, you have to call them up to change the MAC. The Wireless Gateway can it's MAC to computer's one that was originally set up for such an ISP.

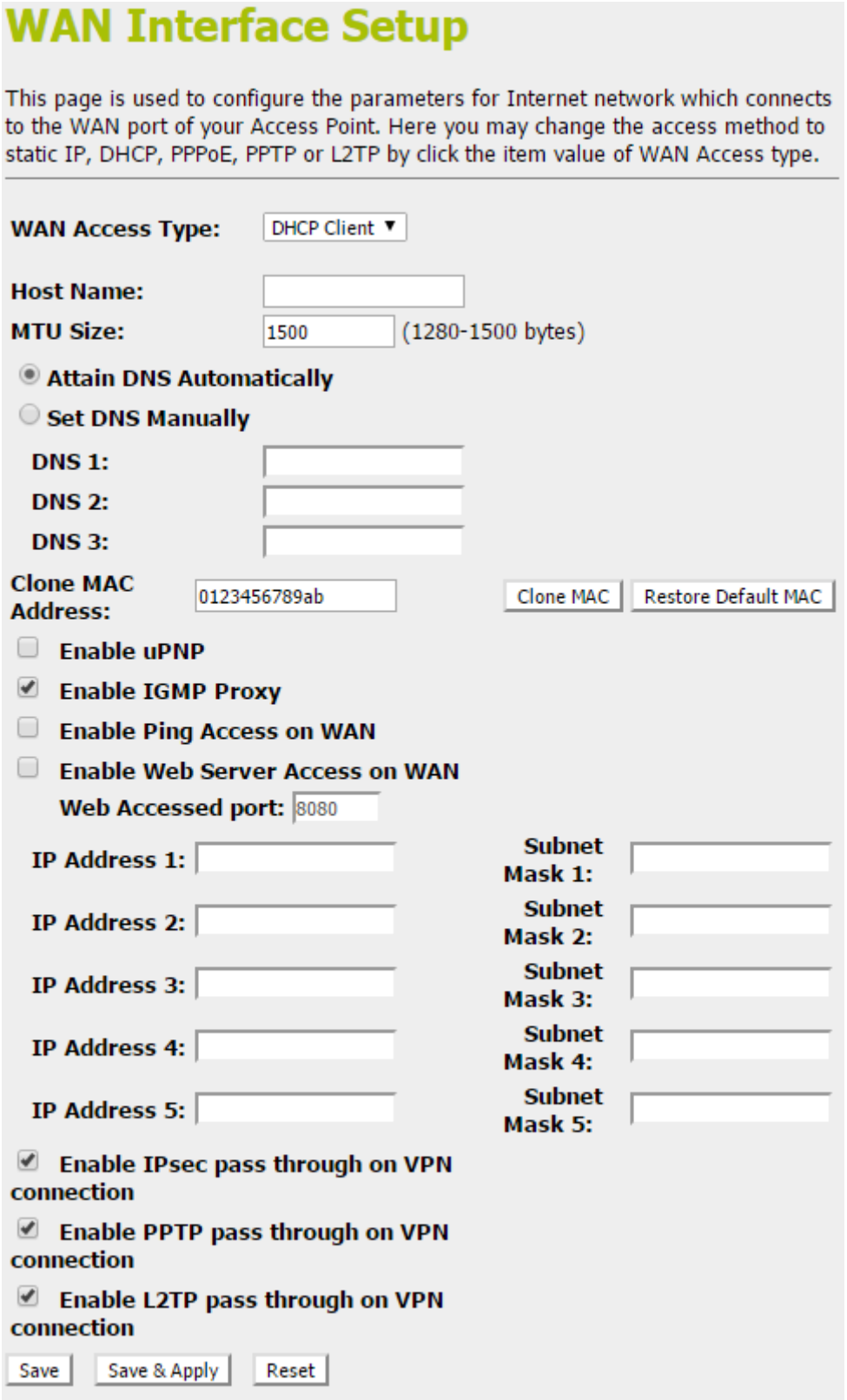
This page allows you to enable or disable *Clone MAC Address* option.

1. From the head menu, click on *TCP/IP*.

2. From the left-hand menu, click on *WAN Setting*. The following page is displayed:



3. Enterthe MAC for example 0123456789ab that you want to be instead of in the *Clone MAC Address*field.
4. If you enter 12 digits of 0in the *Clone MAC Address*field, it'll disable *Clone MAC Address* function.
5. Click *Save & Apply*.



6. Change setting successfully! Please wait 20 seconds….

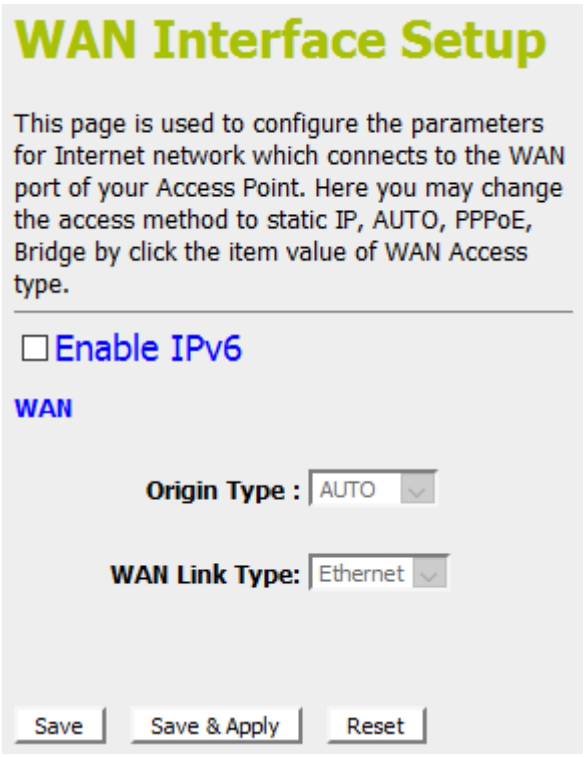
13 IPV6

IPV6 WAN SETTING

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, Bridge by click the item value of WAN Access type.

1. From the head menu, click on *IPV6*.

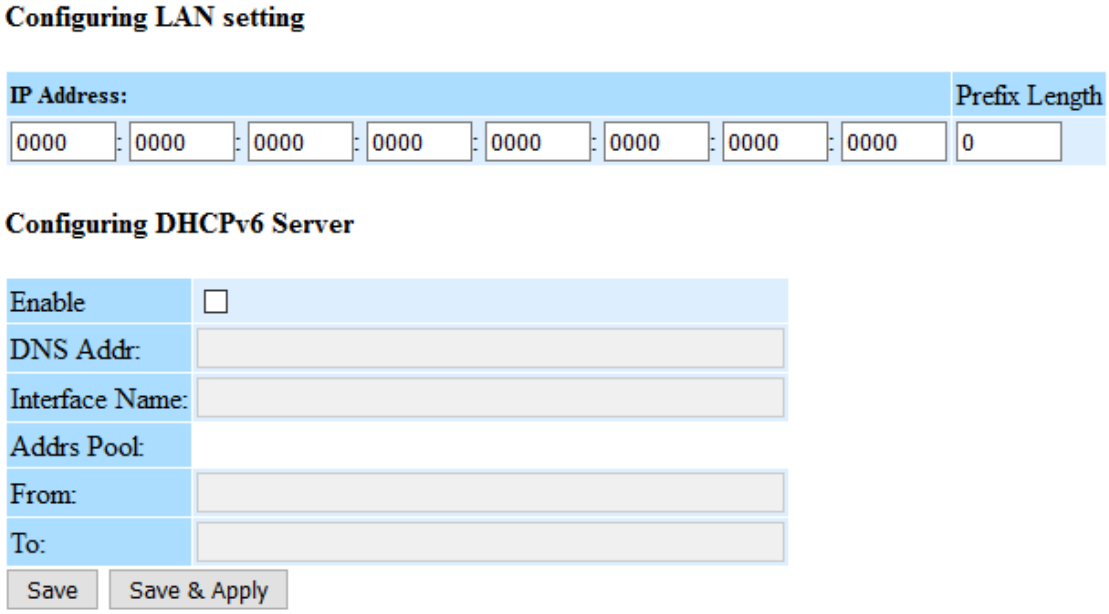
2. From the left-hand menu, click on *IPV6 WAN SETTING*. The following page is displayed:



IPV6 LAN SETTING

1. From the head menu, click on *IPV6*.

2. From the left-hand menu, click on *IPV6 LAN SETTING*. The following page is displayed:



RADVD

1. From the head menu, click on *IPV6*.

2. From the left-hand menu, click on *RADVD*. The following page is displayed:

Configuring Router Advertisement

Enable ☐

radvdinterfacename	
MaxRtrAdvInterval	0
MinRtrAdvInterval	0
MinDelayBetweenRAs	0
AdvManagedFlag	☐
AdvOtherConfigFlag	☐
AdvLinkMTU	0
AdvReachableTime	0
AdvRetransTimer	0
AdvCurHopLimit	0
AdvDefaultLifetime	0
AdvDefaultPreference	high
AdvSourceLLAddress	☐
UnicastOnly	☐

prefix1

Enabled	☐
prefix	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 / 0
AdvOnLinkFlag	☐
AdvAutonomousFlag	☐
AdvValidLifetime	0
AdvPreferredLifetime	0
AdvRouterAddr	☐
if6to4	

prefix2

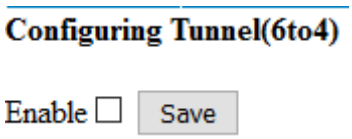
Enabled	☐
prefix	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 / 0
AdvOnLinkFlag	☐
AdvAutonomousFlag	☐
AdvValidLifetime	0
AdvPreferredLifetime	0
AdvRouterAddr	☐
if6to4	

Save | Save & Apply | default | reset

TUNNEL (6 OVER 4)

1. From the head menu, click on *IPV6*.

2. From the left-hand menu, click on *TUNNEL (6 OVER 4)*.
   The following page is displayed:

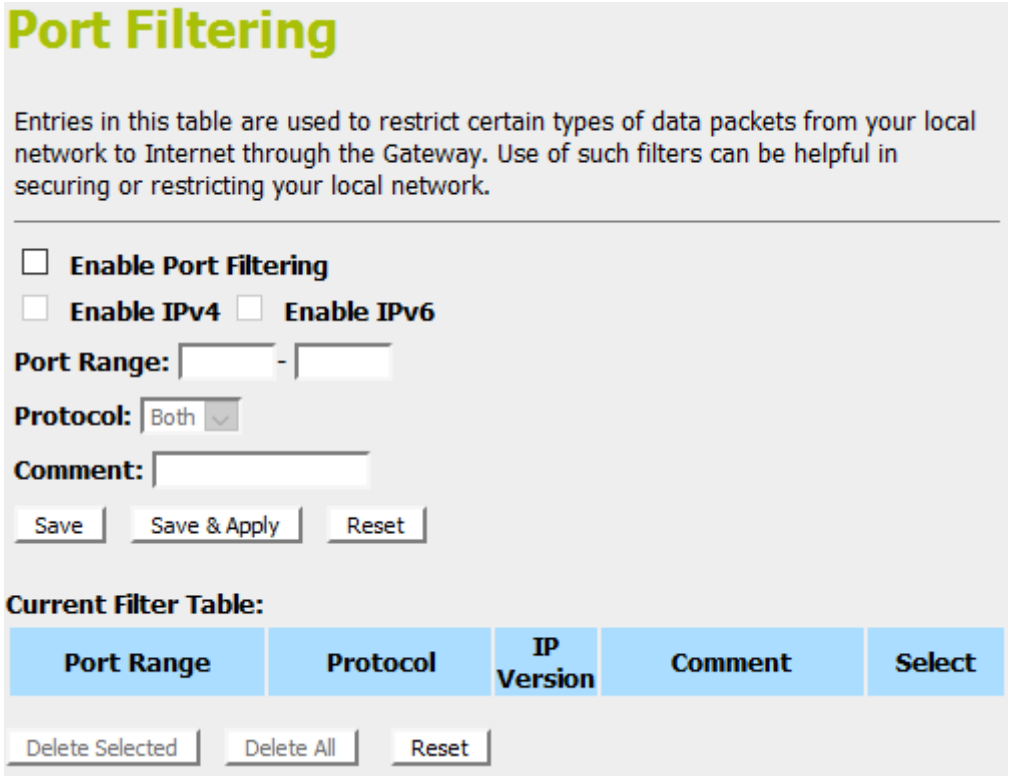


14 Port Filtering

Entries in *Current Filter Table* are used to restrict certain ports and types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *Port Filtering*. The following page is displayed:



Option	Description
EnablePort Filtering	**Enable/Disable the WAN packet filter.** **Default setting is Disable.**
PortRange	**Enter the port range to be filtered for both Outbound and Inbound packet**
Protocol	**Select the Protocol to be filtered for both Outbound and Inbound packet** **Both: To filter both TCP and UDP protocol** **TCP: To filter only TCP protocol** **UDP: filter only UDP protocol**
Comment	**Fill in the note for manager what the purpose of certain port filtering rule**
Current Filter Table	**The Port Filters that was created is listed here**

Note

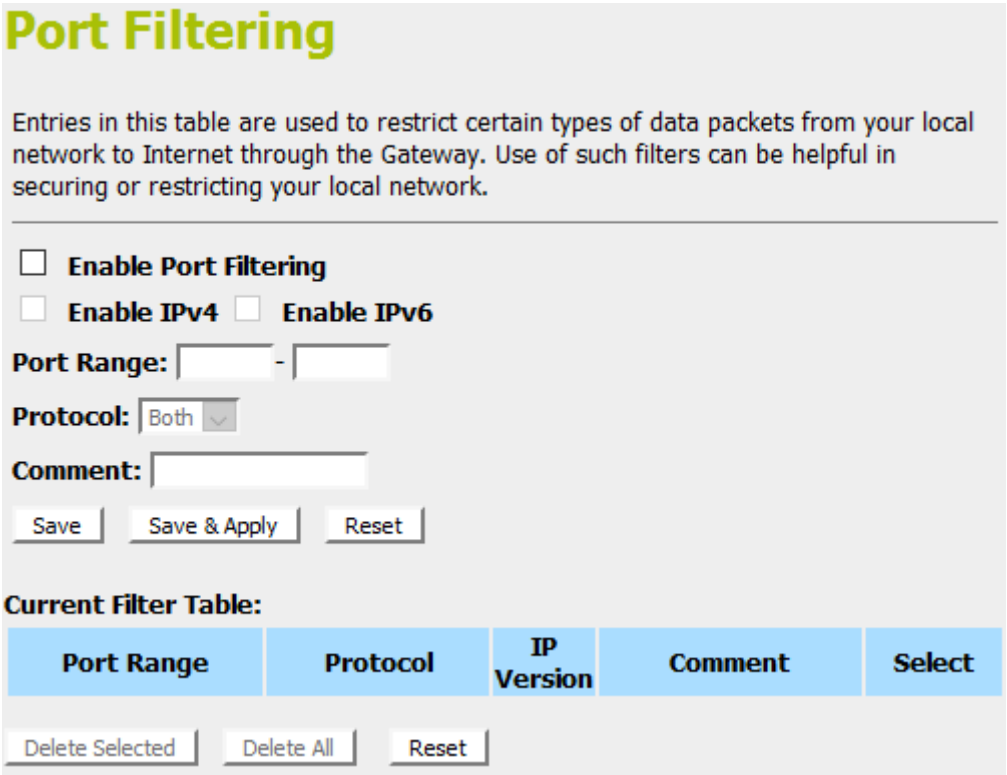
You must ensure that the single port or range specified does not overlap with a port or range for an existing common or custom application. Check the common port ranges listed in.

Port filtering for TCP port 80

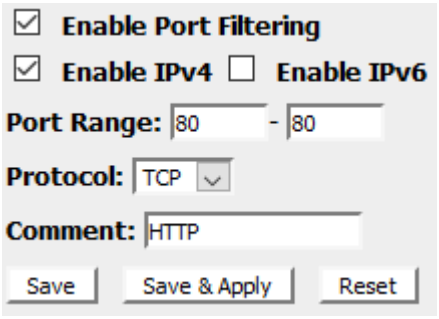
Please follow example below to deny the TCP port 80 for both Outbound and Inbound packet.

1. From the head menu, click on *Firewall*.

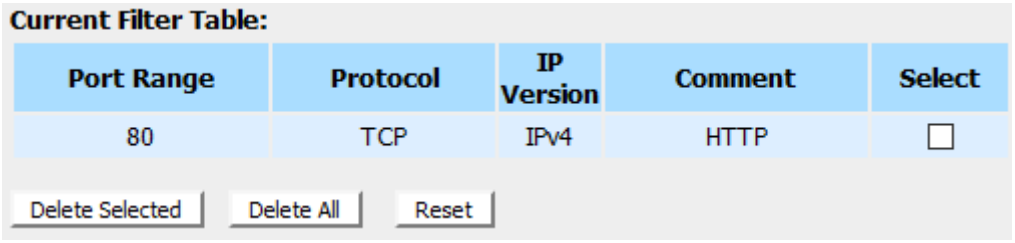
2. From the left-hand menu, click on *Port Filtering*. The following page is displayed:



3. Check the option *Enable Port Filtering* to enable the port filtering.
4. Enter*80* and *80*in *PortRange* field.
5. From the *Protocol* drop-down list, select *TCP*setting.
6. EnterHTTP in *Comment* field.
7. Click *Save & Apply*.



8. Now the port filter that you created has been added and listed in the *Current Filter Table*.
9. Now the TCP port for both Outbound and Inbound packet has been denied.



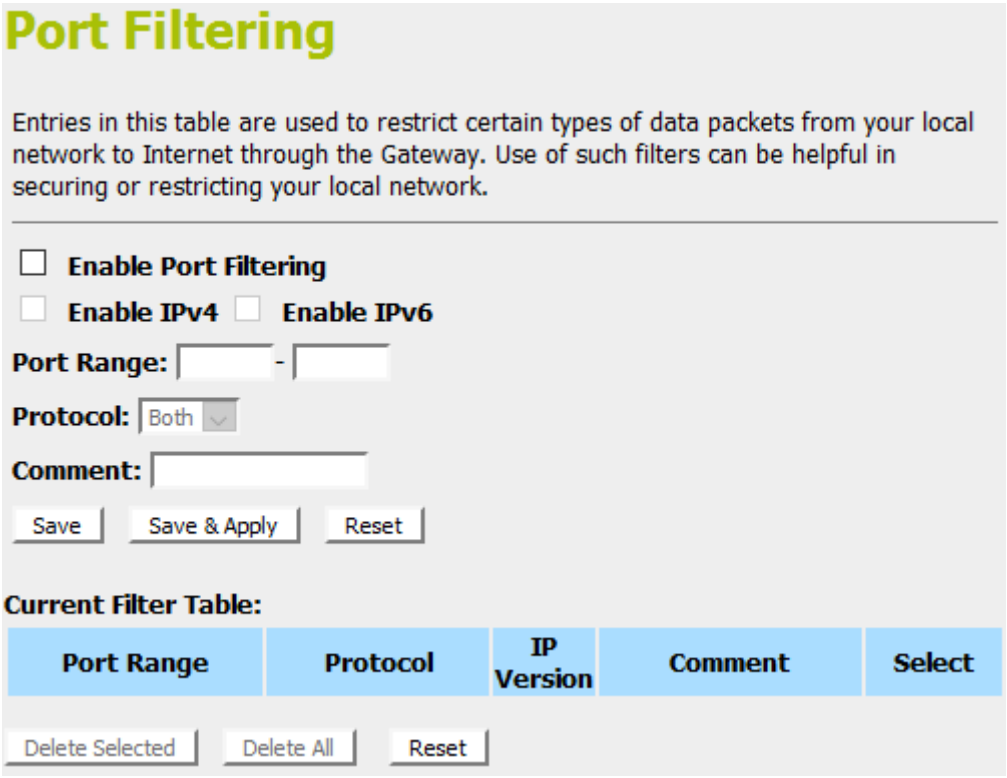
Now you cannot visit any web site due to the TCP port 80 has been blocked by the Port Filtering rule that created.

Port filtering for UDP port 53

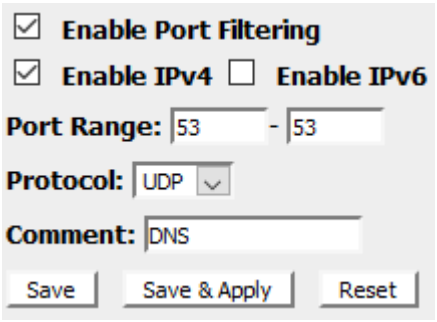
Please follow example below to deny the UDP port 53 for both Outbound and Inbound packet.

1. From the head menu, click on *Firewall*.

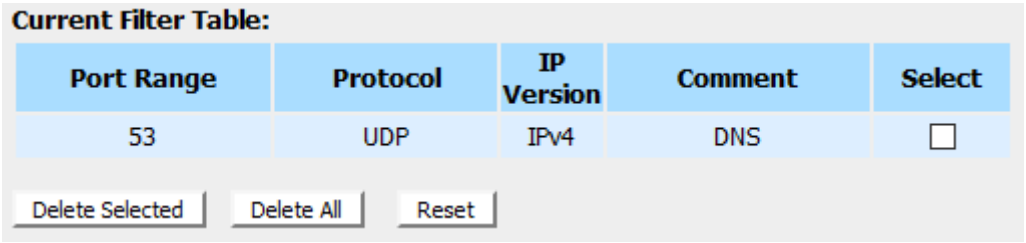
2. From the left-hand menu, click on *Port Filtering*. The following page is displayed:



3. Check the option *Enable Port Filtering* to enable the port filtering.
4. Enter*53* and *53*in *PortRange* field.
5. From the *Protocol* drop-down list, select *UDP*setting.
6. EnterDNS Resolve in *Comment* field.
7. Click *Save & Apply*.



8. Now the port filter that you created has been added and listed in the *Current Filter Table*.
9. Now the UDP port 80 for both Outbound and Inbound packet has been denied.



Now you cannot visit any web site by domain due to the UDP port 53 has been blocked by the Port Filtering rule that created.

You can enter the IP Address of that web site to visit.

15 IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

The IP filter feature enables you to create rules that control the forwarding of incoming and outgoing data between the LAN and WAN side.

You can create IP filter rules to block attempts by certain computers on your LAN to access certain types of data or Internet locations. You can also block accesses to your LAN computers from the WAN side.

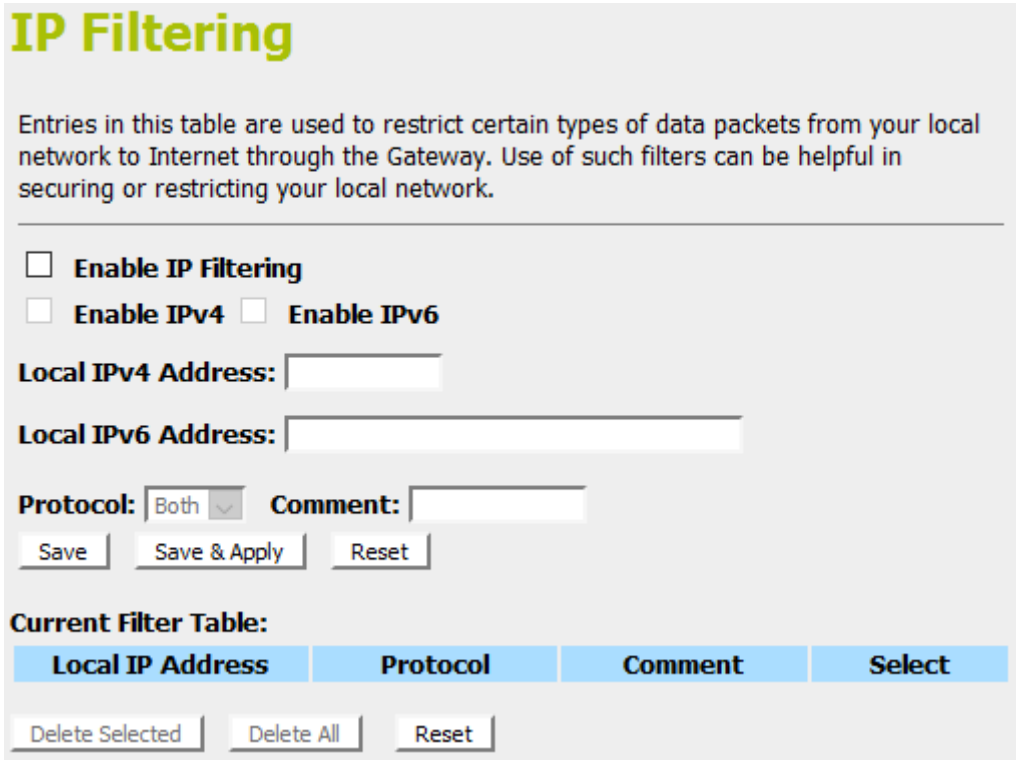
When you define an IP filter rule and enable the feature, you instruct the ADSL/Ethernet router to examine data packets to determine whether they meet criteria set forth in the rule. The criteria can include the network or internet protocol, the packet carries, the direction in which it is traveling (for example, from the LAN to the WAN and vice versa).

If the packet matches the criteria established in a rule, the packet can either be accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.

The IP Filter Configuration page provides the capability to enable/disable the IP filter feature and the IP Filter rule entries for all currently established rules.

1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *IP Filtering*. The following page is displayed:

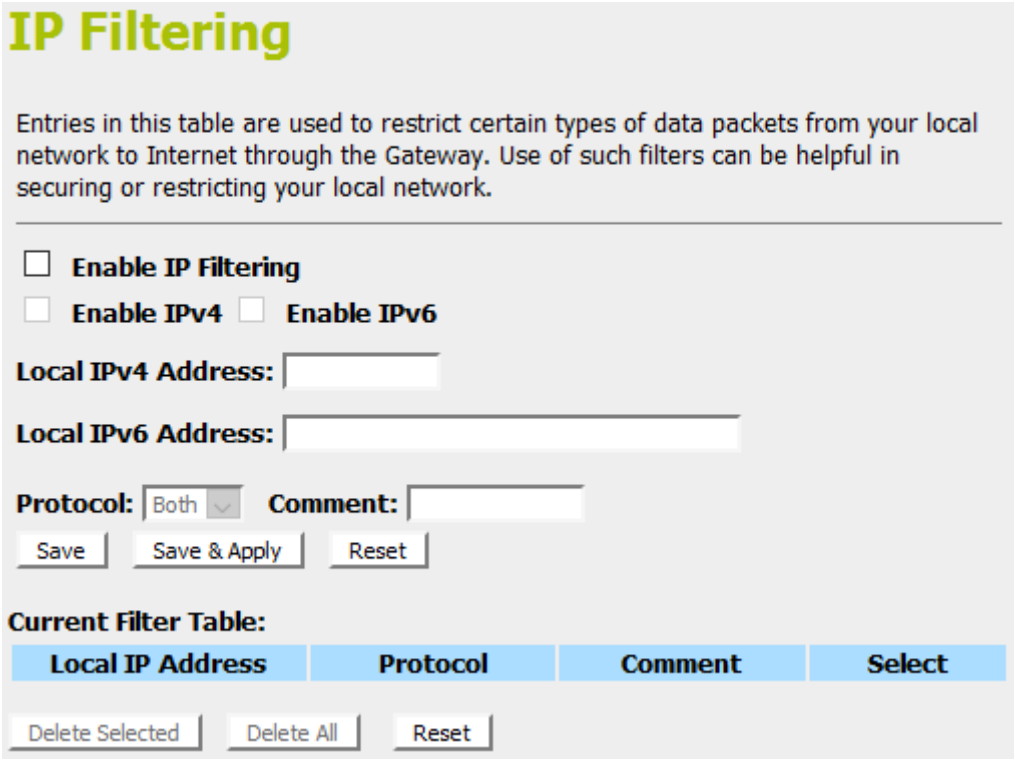


IP filtering for TCP with specified IP

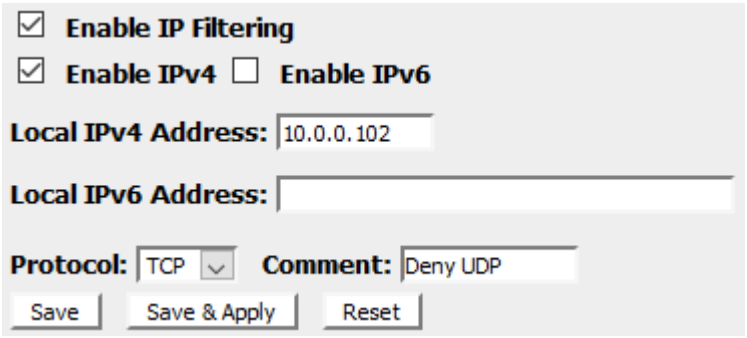
Please follow example below to deny the TCP protocol for specified IP.

1. From the head menu, click on *Firewall*.

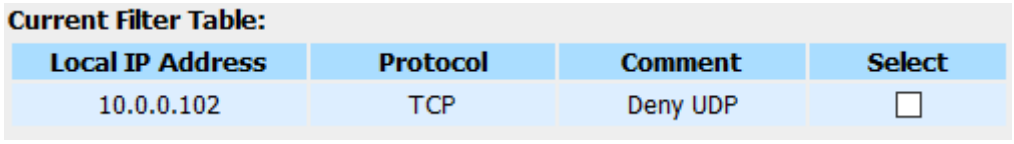
2. From the left-hand menu, click on *IP Filtering*. The following page is displayed:



3. Check the option *Enable IP Filtering* to enable the IP Filtering.
4. Enterthe IP Address that you want to be deniedin *Loal IP Address* field.
5. From the *Protocol* drop-down list, select *TCP*setting.
6. Enterany comment in *Comment* field.
7. Click *Save & Apply*.



8. Now the IP Filter that you created has been added and listed in the *Current Filter Table*.
9. Now the TCP protocol for both Outbound and Inbound packet has been denied.



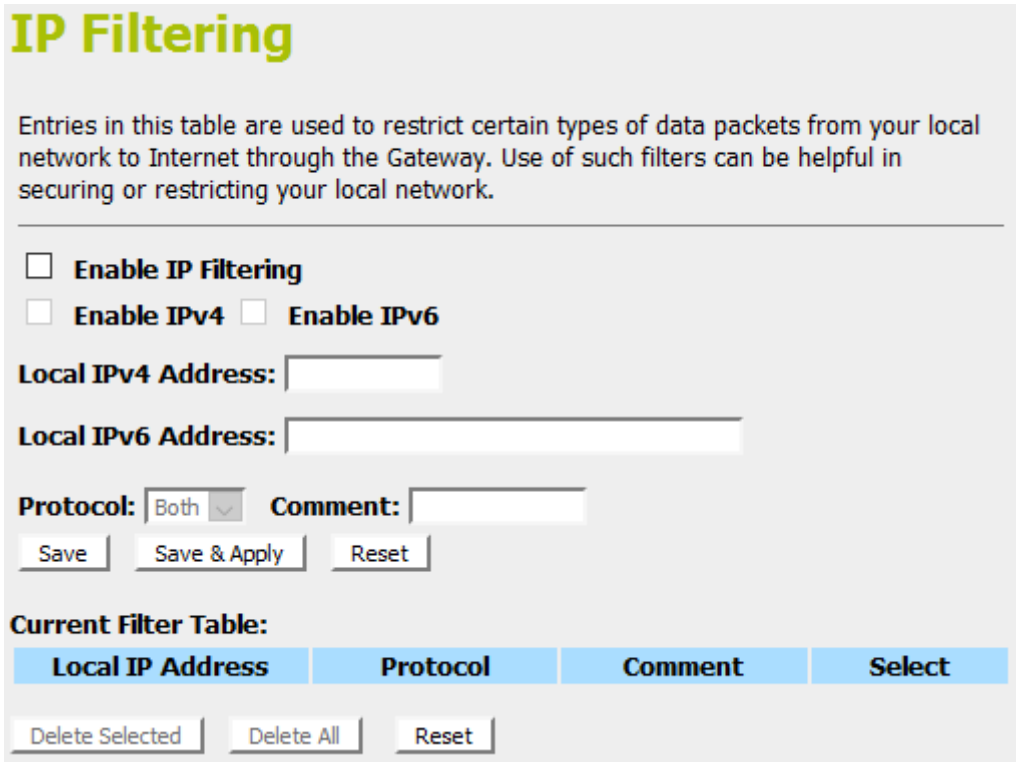
Now The Local IP Address for example 10.0.0.102 that listed in the *Current Filter Table* cannot visit any application that use TCP protocol for example web site due to the Protocol TCP has been blocked by the IP Filtering rule that created.

IP filtering for UDP with specified IP

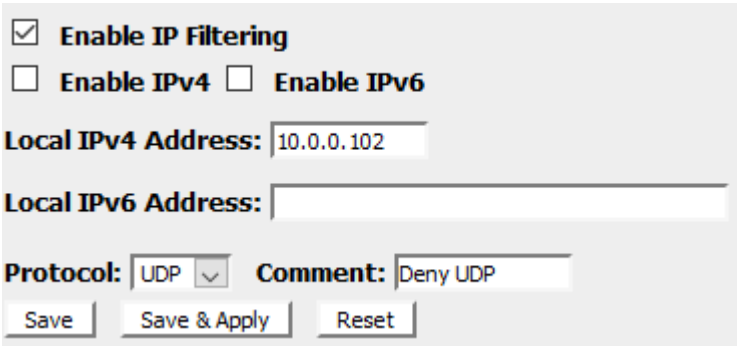
Please follow example below to deny the UDP protocol for specified IP.

1. From the head menu, click on *Firewall*.

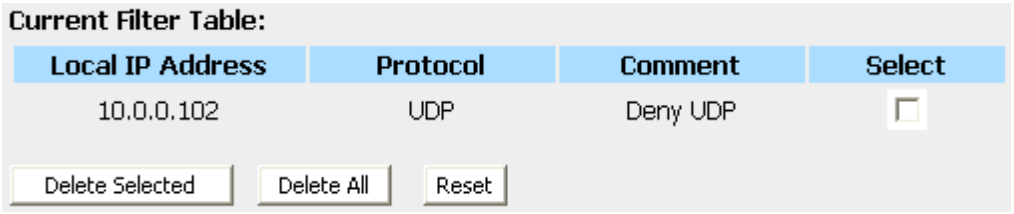
2. From the left-hand menu, click on *IP Filtering*. The following page is displayed:



3. Check the option *Enable IP Filtering* to enable the IP Filtering.
4. Enterthe IP Address that you want to be deniedin *Local IP Address* field.
5. From the *Protocol* drop-down list, select *UDP*setting.
6. Enterany comment in *Comment* field.
7. Click *Save & Apply*.



8. Now the IP Filter that you created has been added and listed in the *Current Filter Table*.
9. Now the UDP protocol for both Outbound and Inbound packet has been denied.



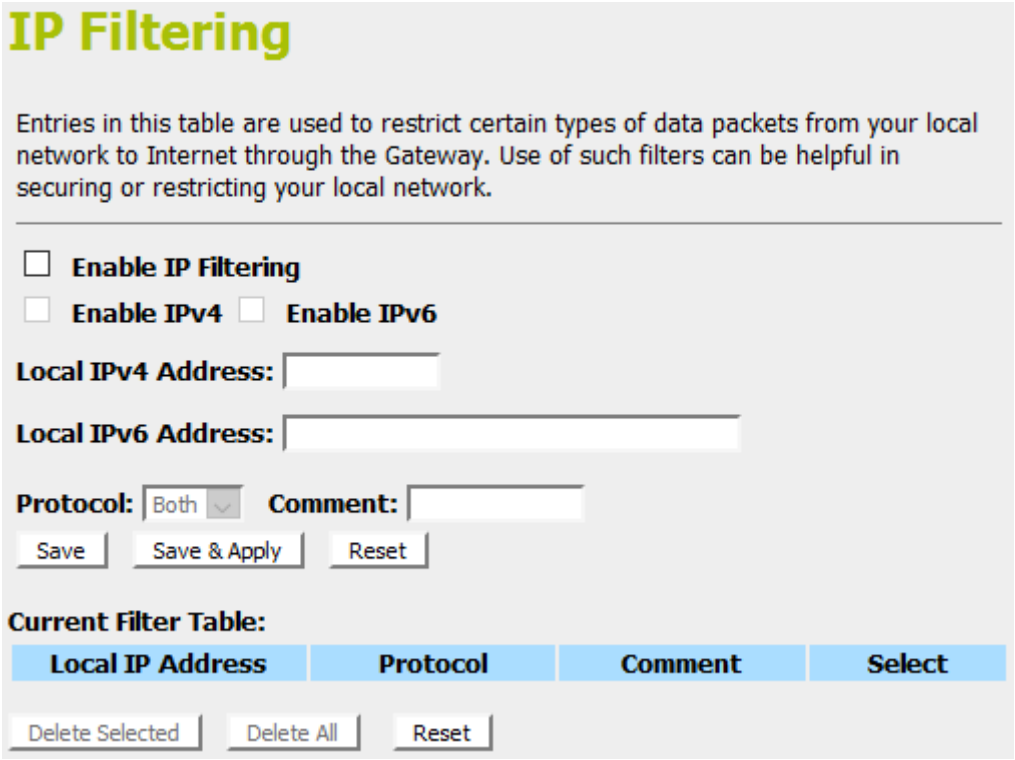
Now The Local IP Address for example 10.0.0.102 that listed in the *Current Filter Table* cannot visit any application that use UDP protocol for example TFTP Service due to the Protocol UDP has been blocked by the IP Filtering rule that created.

IP filtering for both TCP and UDP with specified IP

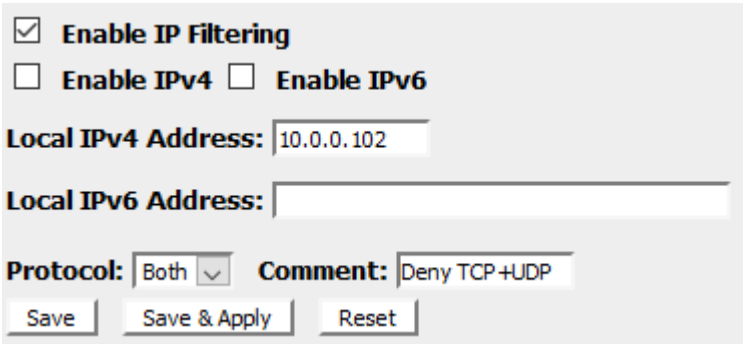
Please follow example below to deny the both TCP and UDP protocol for specified IP.

1. From the head menu, click on *Firewall*.

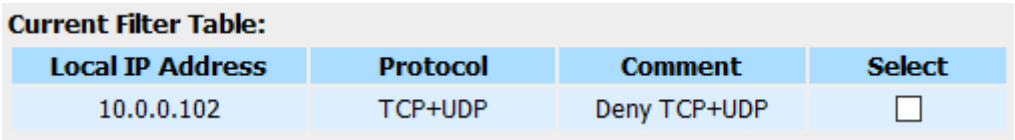
2. From the left-hand menu, click on *IP Filtering*. The following page is displayed:



3. Check the option *Enable IP Filtering* to enable the IP Filtering.
4. Enterthe IP Address that you want to be deniedin *Local IP Address* field.
5. From the *Protocol* drop-down list, select *Both*setting.
6. Enterany comment in *Comment* field.
7. Click *Save & Apply*.



8. Now the IP Filter that you created has been added and listed in the *Current Filter Table*.
9. Now the TCP and UDP protocol for both Outbound and Inbound packet has been denied.

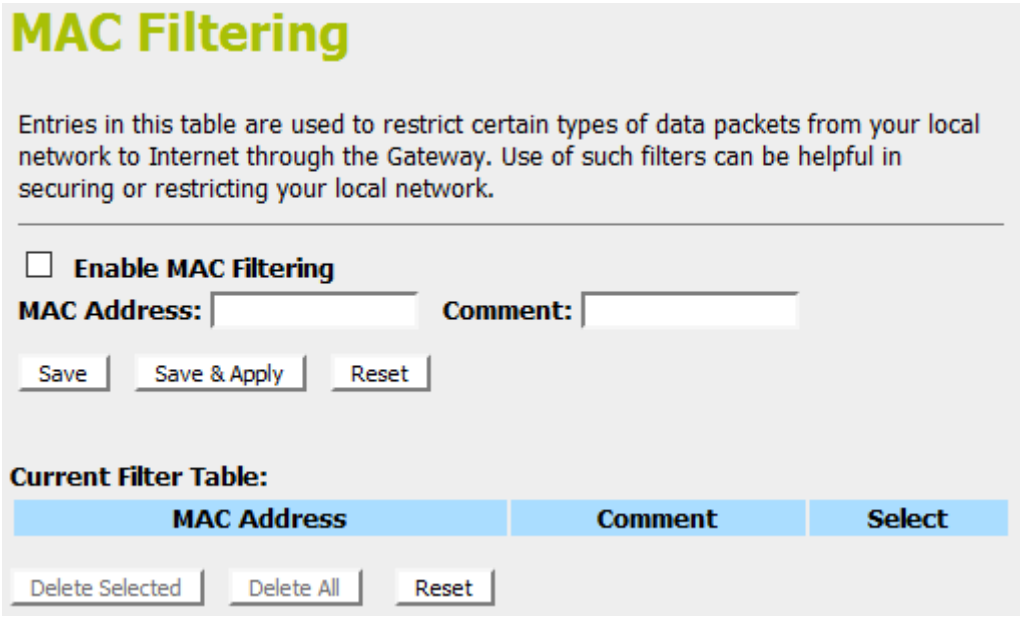


16 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Wireless Gateway. Use of such filters can be helpful in securing or restricting your local network.

1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *MAC Filtering*. The following page is displayed:

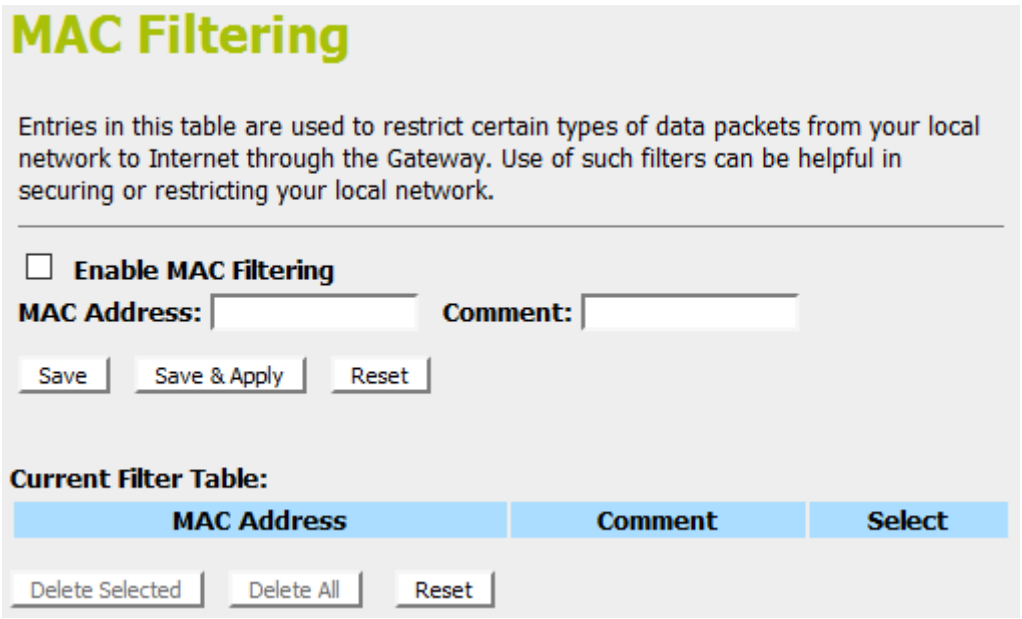


MAC filtering for specified MAC Address

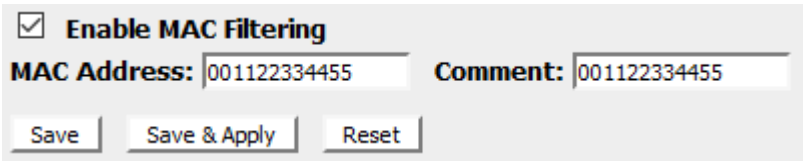
Please follow example below to deny the specified MAC Address has the Internet Access.

1. From the head menu, click on *Firewall*.

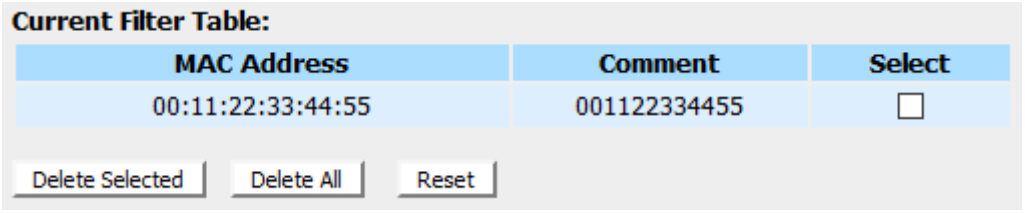
2. From the left-hand menu, click on *MAC Filtering*. The following page is displayed:



3. Check the option *Enable MAC Filtering* to enable the MAC Filtering.
4. Enterthe MAC Address that you want to be deniedin *MAC Address*field.
5. Enterany comment in *Comment* field.
6. Click *Save & Apply*.



7. Now the MAC Filter that you created has been added and listed in the *Current Filter Table*.
8. Now the MAC Address in the*Current Filter Table* cannot have the Internet Access.



17 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Your device has built in advanced Security features that protect your network by blocking unwanted traffic from the Internet.

If you simply want to connect from your local network to the Internet, you do not need to make any changes to the default Security configuration. You only need to edit the configuration if you wish to do one or both of the following:

- allow Internet users to browse the user pages on your local network (for example, by providing an FTP or HTTP server)
- play certain games which require accessibility from the Internet

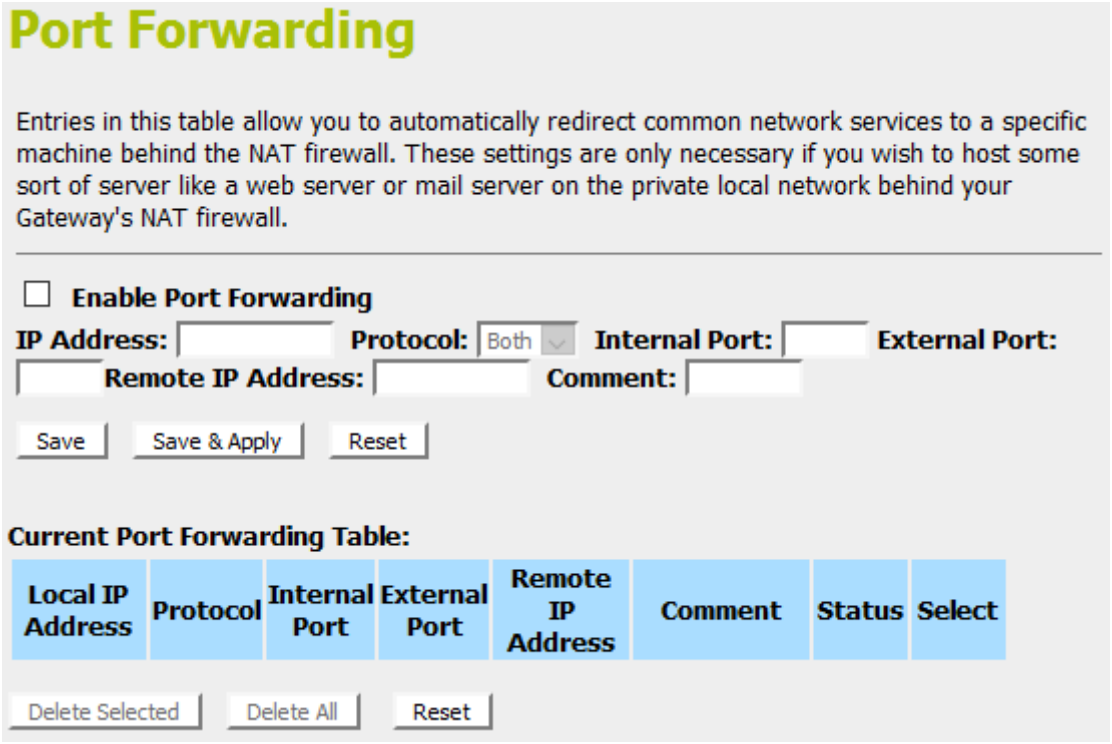
This chapter describes how to configure Security to suit the needs of your network.

By default, the IP addresses of your LAN PCs are hidden from the Internet. All data sent from your LAN PCs to a PC on the Internet appears to come from the IP address of your device.

In this way, details about your LAN PCs remain private. This security feature is called *Port Forwarding*.

1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *Port Forwarding*. The following page is displayed:

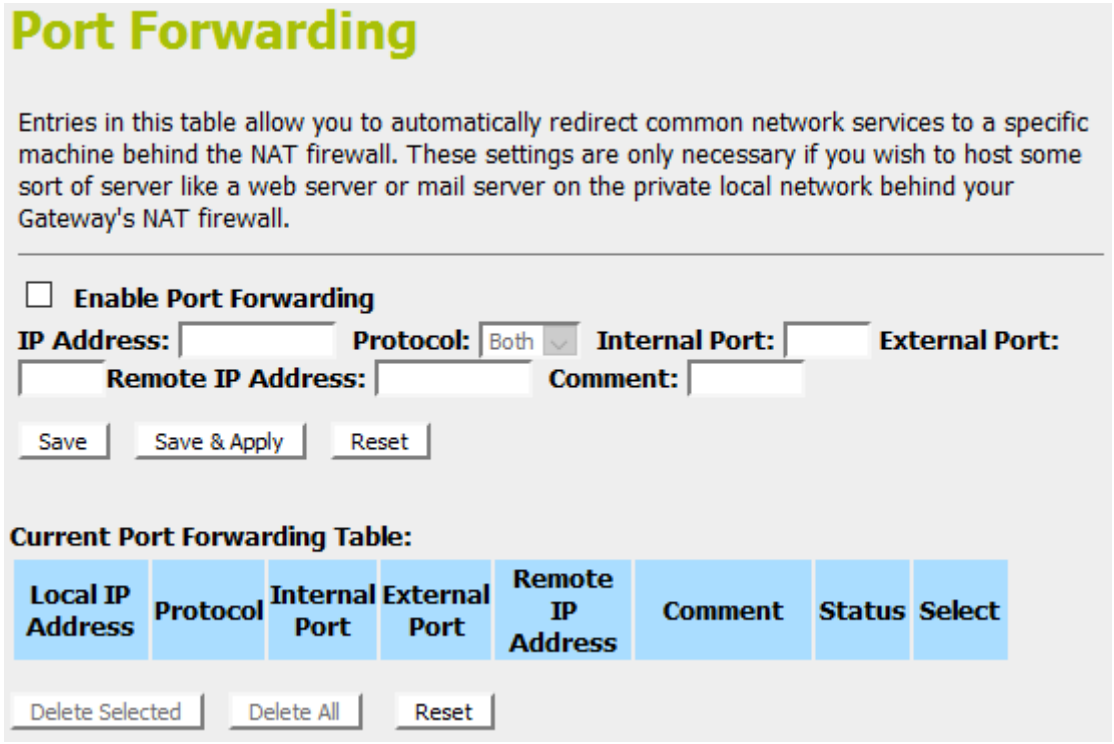


Port Forwarding for TCP with specified IP

Please follow example below to configure the Port Forwarding to Specified IP with TCP.

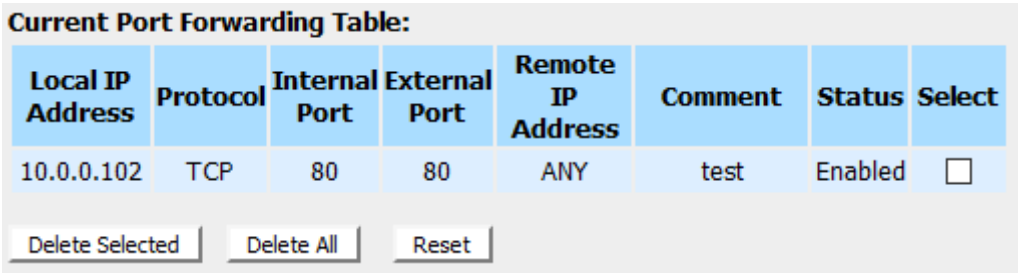
1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *Port Forwarding*. The following page is displayed:



3. Check the option *Enable Port Forwarding* to enable the Enable Port Forwarding.
4. Enterthe IP Address that the port you want to be forwarded in *IP Address* field.
5. From the *Protocol* drop-down list, select *TCP*setting.
6. Enterany comment in *Comment* field.
7. Click *Save & Apply*.

8. Now the IP Address and port range that you created has been added and listed in the *Current Filter Table*.
9. Now the port range of the IP Address in the*Current Filter Table* can be access from Internet by TCP protocol.

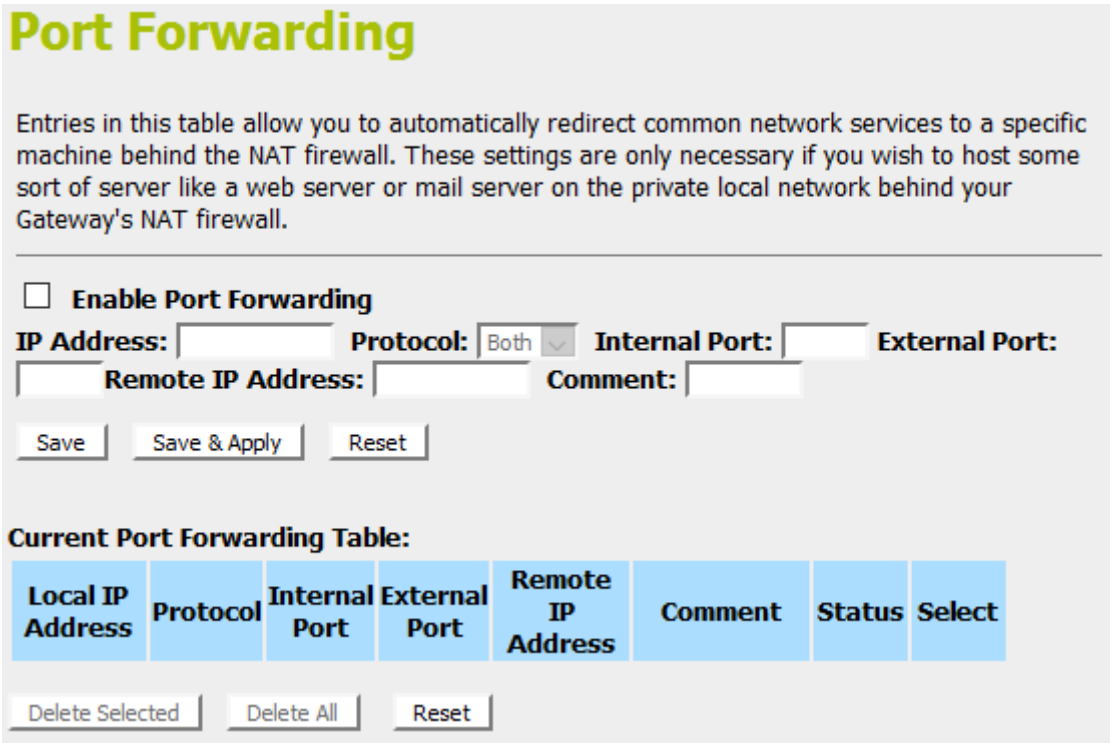


Port Forwarding for UDP with specified IP

Please follow example below to configure the Port Forwarding to Specified IP with UDP.

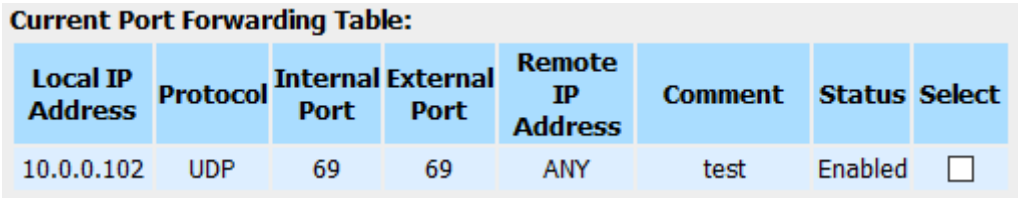
1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *Port Forwarding*. The following page is displayed:



3. Check the option *Enable Port Forwarding* to enable the Enable Port Forwarding.
4. Enterthe IP Address that the port you want to be forwarded in *IP Address* field.
5. From the *Protocol* drop-down list, select *UDP*setting.
6. Enterany comment in *Comment* field.
7. Click *Save & Apply*.

8. Now the IP Address and port range that you created has been added and listed in the *Current Filter Table*.
9. Now the port range of the IP Address in the*Current Filter Table* can be access from Internet by UDP protocol.

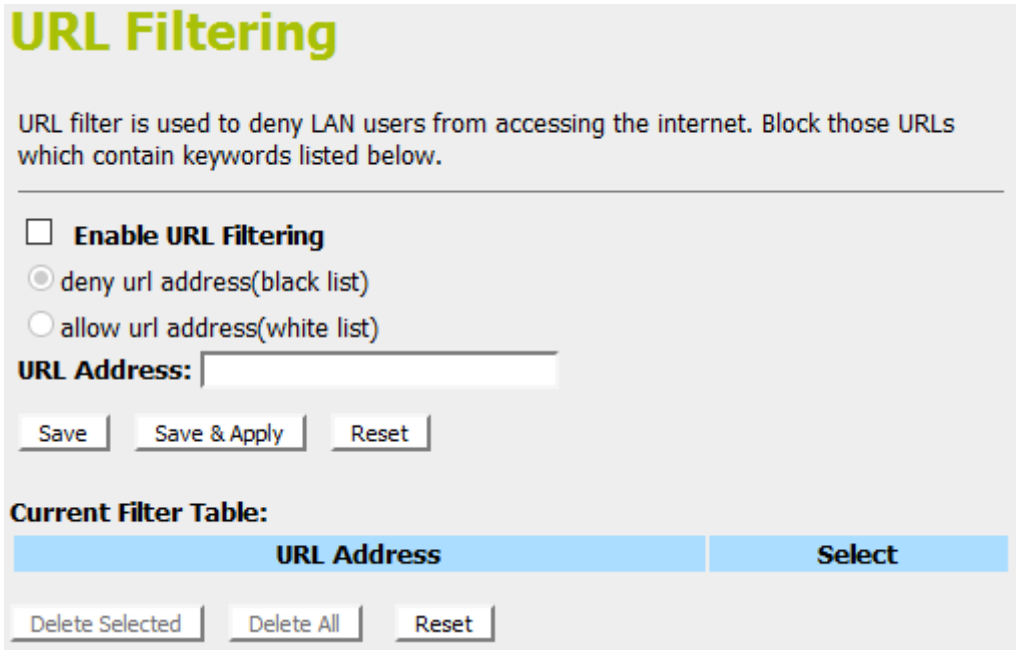


18 URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *URL Forwarding*. The following page is displayed:

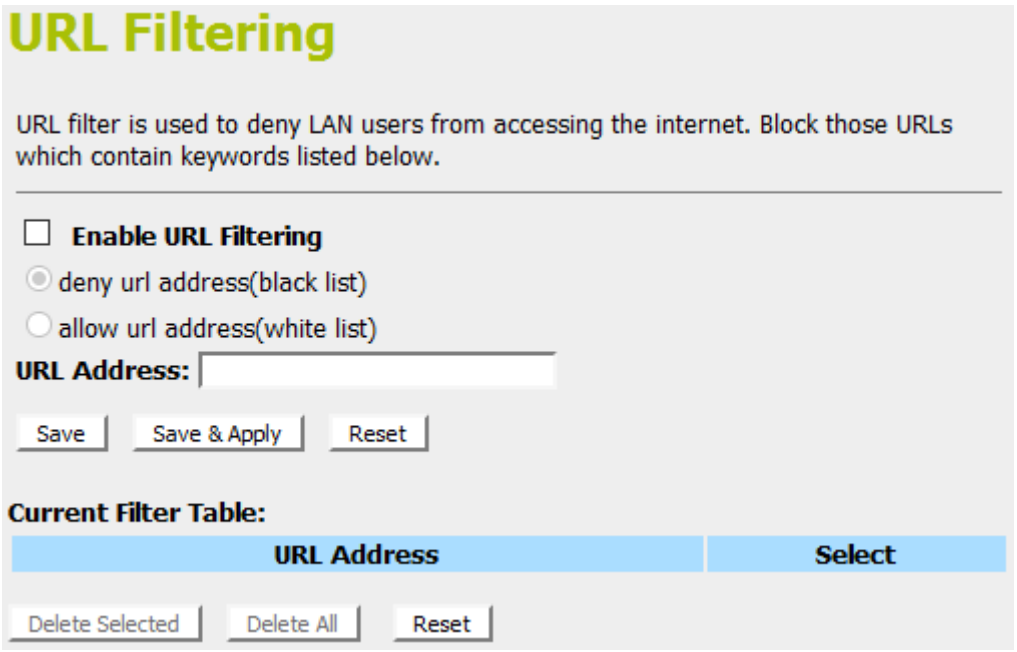


URL filtering for specified URL Address

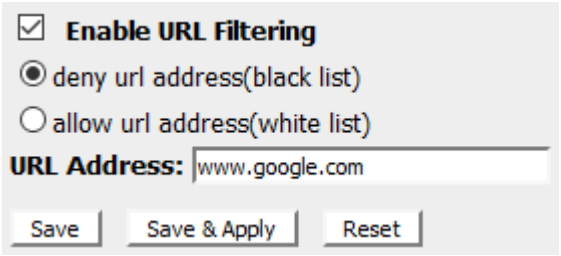
Please follow example below to deny LAN users from accessing the Internet.

1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *URL Forwarding*. The following page is displayed:



3. Check the option *Enable URL Filtering* to enable the URL Filtering.
4. Check the option *deny url address(black list)* to deny url address(black list)
5. Enterthe URL Address that you want to be denied for LAN user.
6. Click *Save & Apply*.



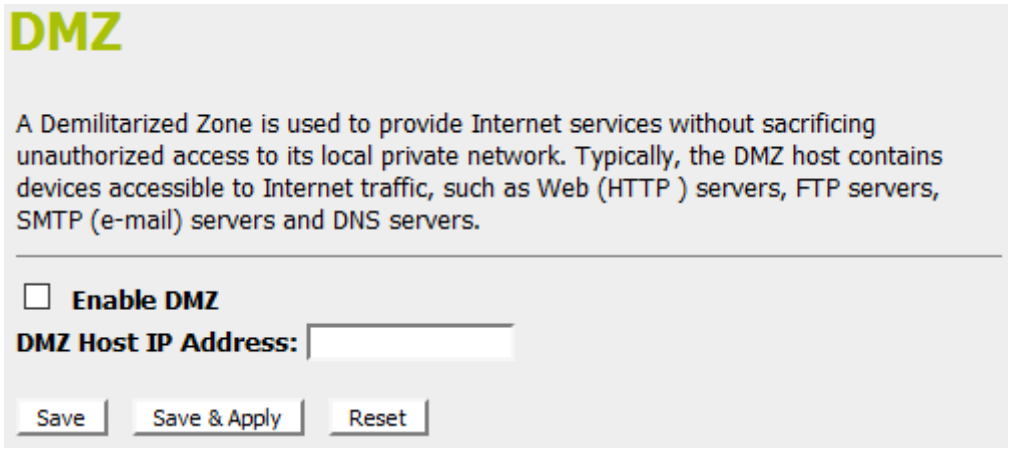
7. Now the URL Filter that you created has been added and listed in the *Current Filter Table*.
8. Now the URL Address in the*Current Filter Table* cannot be visited.

19 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *DMZ*. The following page is displayed:

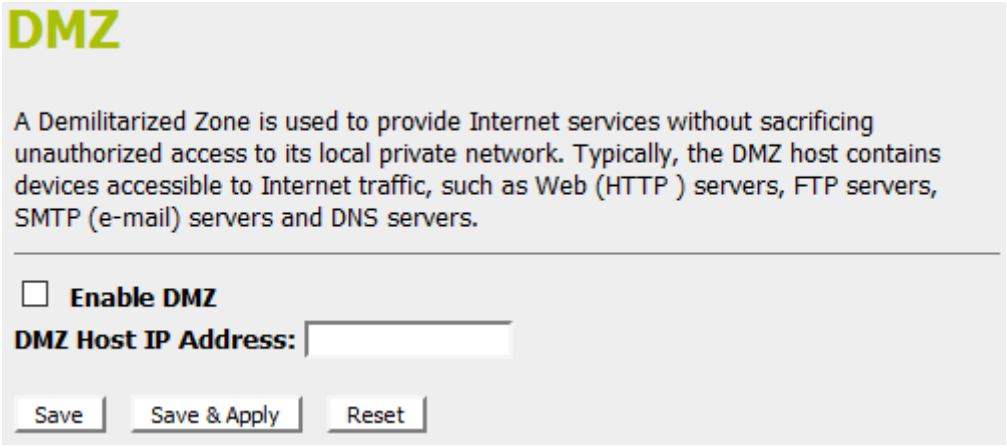


DMZ Host IP Address

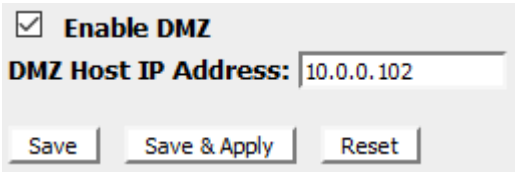
Please follow example below to configure the DMZ to Host IP Address.

1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *DMZ*. The following page is displayed:



3. Check the option *Enable DMZ* to enable the Enable DMZ.
4. Enterthe IP Address that to be the DMZ Host in *DMZ Host IP Address*field.
5. Click *Save & Apply*.

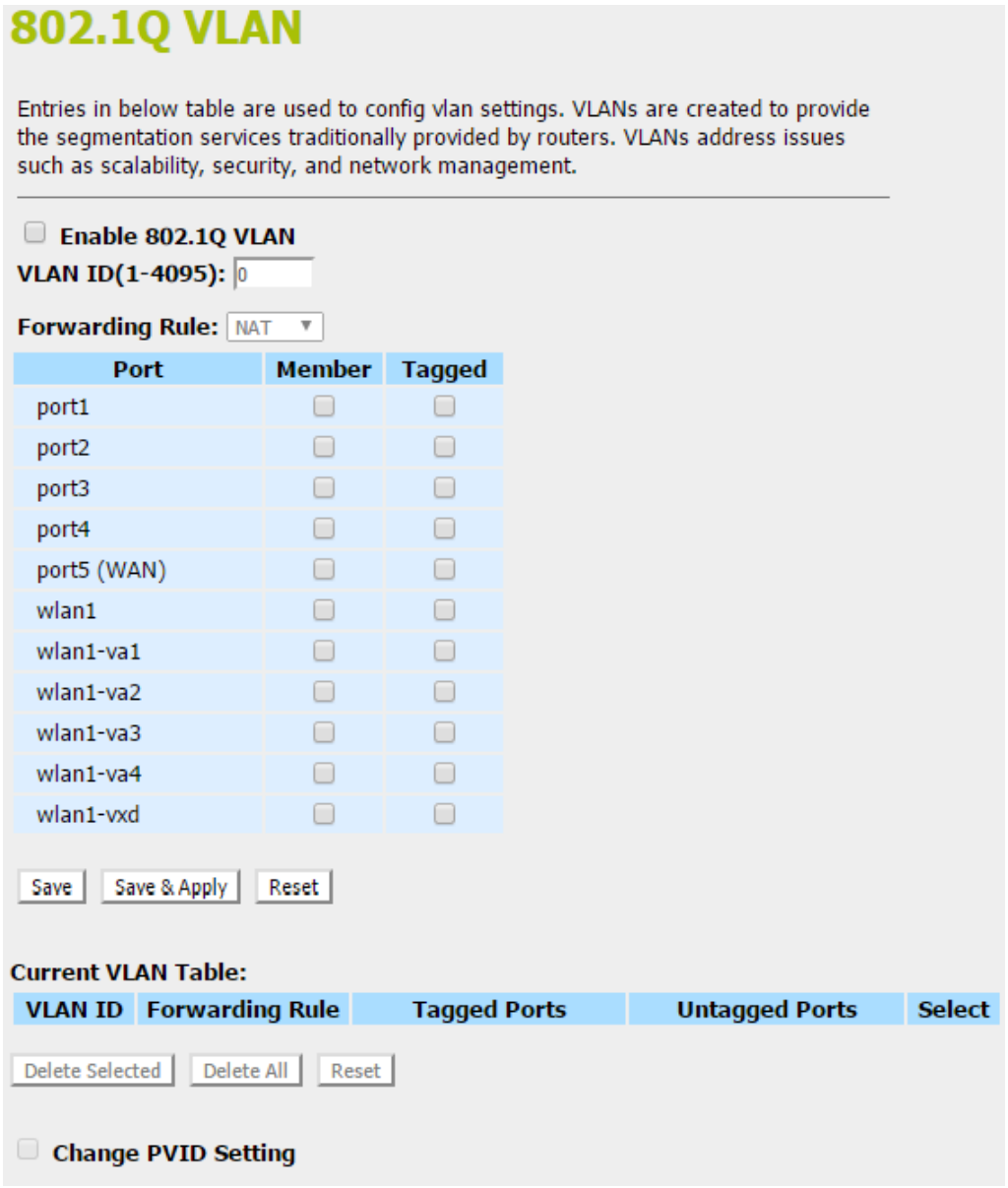


20 802.1Q VLAN

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

1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *802.1Q VLAN*. The following page is displayed:

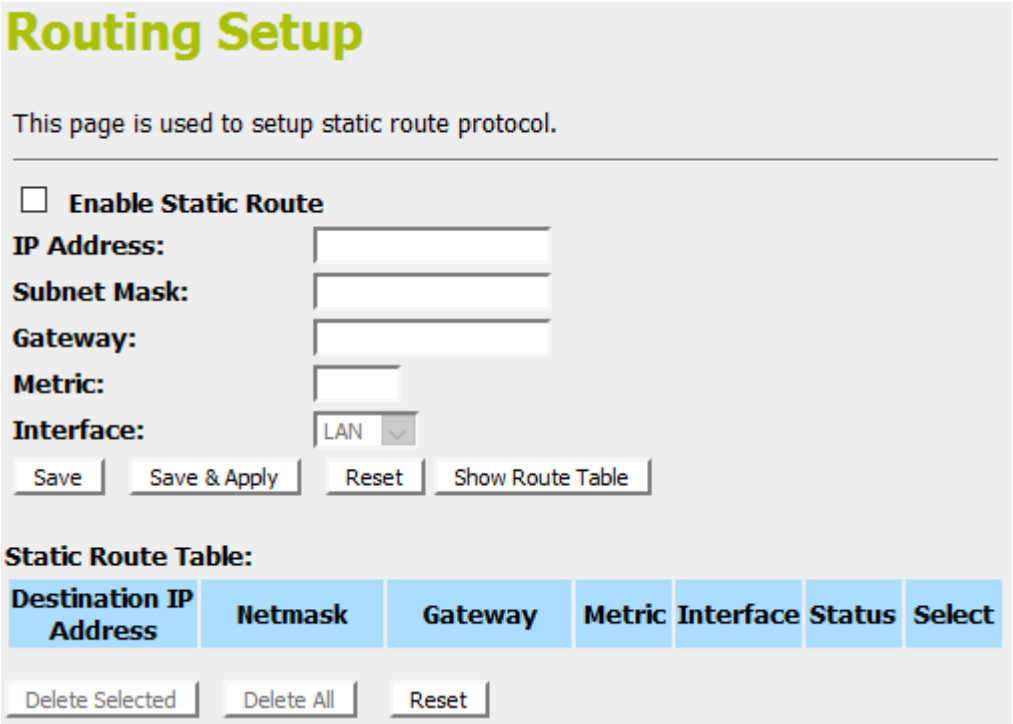


21 ROUTE SETUP

This page is used to setup dynamic routing protocol or edit static route entry.

1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *ROUTE SETUP*. The following page is displayed:

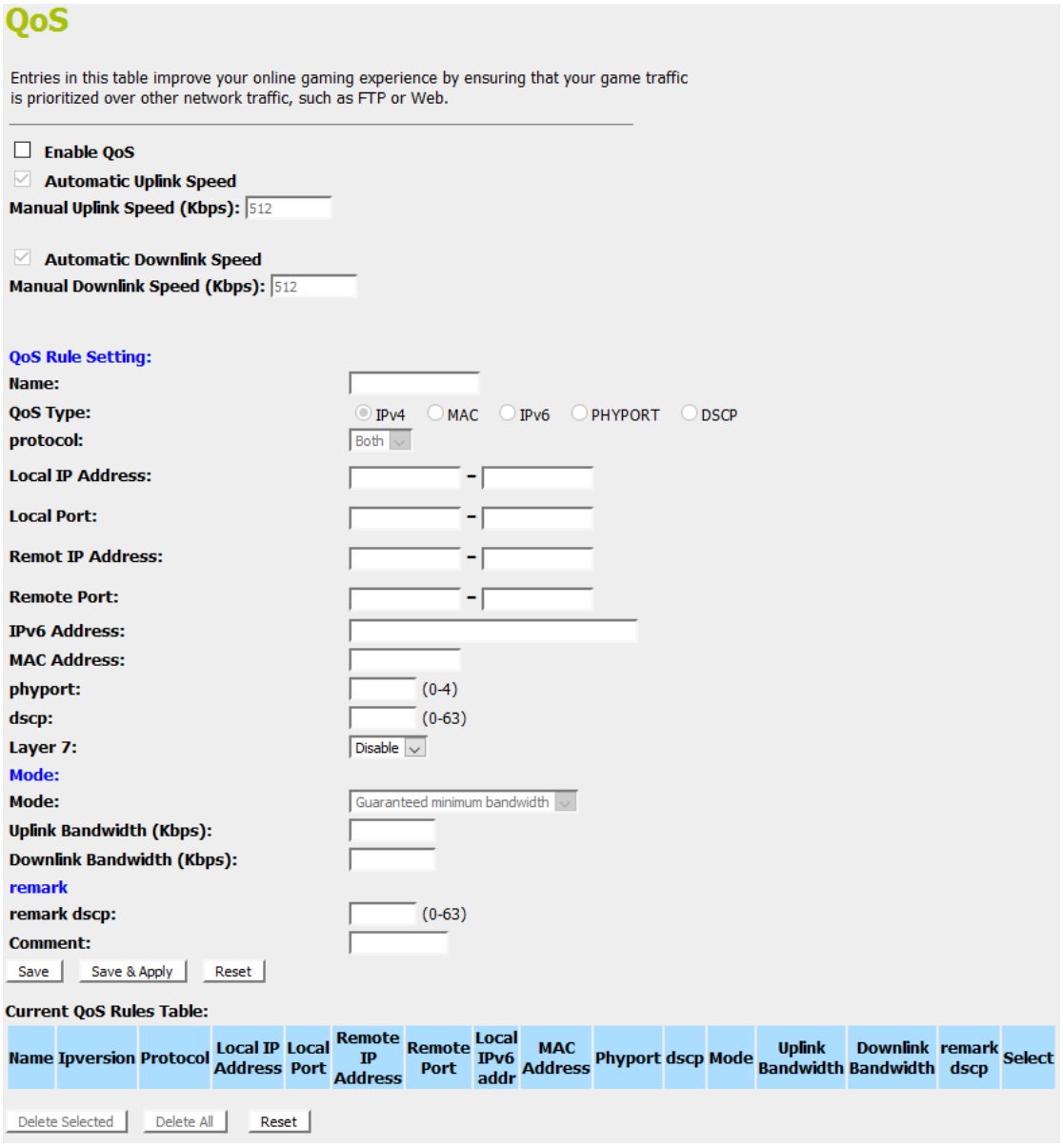


22 QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

1. From the head menu, click on *Firewall*.

2. From the left-hand menu, click on *QOS*. The following page is displayed:



23 Status

This page displays the current information for the device. It will display the LAN, WAN, and system firmware information. This page will display different information, according to WAN setting (Static IP, DHCP, or PPPoE).

1. From the head menu, click on *Management*.

2. From the left-hand menu, click on *Status*. The following page is displayed:

Access Point Status

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

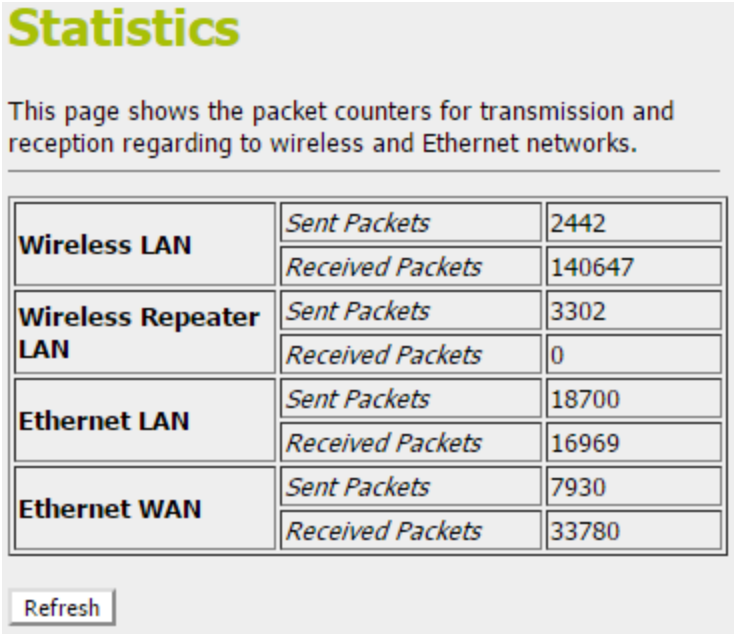
System	
Uptime	0day:2h:32m:48s
Firmware Version	RER4_A_v3411_2T2R_STD_01_160824
Build Time	Wed Aug 24 17:22:55 CST 2016
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	11n
Channel Number	11
Encryption	Disabled
BSSID	94:46:96:11:95:a9
Associated Clients	0
Wireless Repeater Interface Configuration	
Mode	Infrastructure Client
SSID	RTK 11n AP RPT0
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	10.0.0.2
Subnet Mask	255.255.255.0
Default Gateway	10.0.0.2
DHCP Server	Enabled
MAC Address	94:46:96:11:95:a7
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.88.204
Subnet Mask	255.255.255.0
Default Gateway	192.168.88.1
MAC Address	94:46:96:11:95:a8
DNS Address	192.168.88.1
LAN IPv6 Configuration	
Global Address	
LL Address	fe8000000000000964696fffe1195a7/64
Default Gateway	fe8000000000000964696fffe1195a7/64
MAC Address	94:46:96:11:95:a7
WAN IPv6 Configuration	
Link Type	IP link
Connection Type	DHCPv6
Global Address	
LL Address	fe8000000000000964696fffe1195a8/64
Default Gateway	
DNS server	00000000000000000000000000000000
MAC Address	94:46:96:11:95:a8

24 Statistics

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

1. From the head menu, click on *Management*.

2. From the left-hand menu, click on *Statistics*. The following page is displayed:



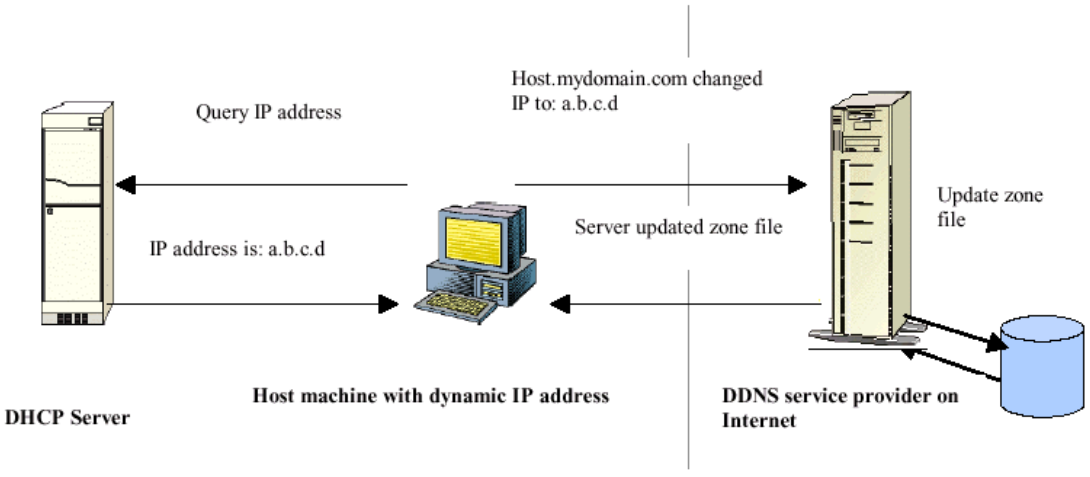
25 Dynamic DNS

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address, you can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname.

This chapter provides you an overview of the Dynamic DNS feature of the modem and configurationdetails related to it.

Overview

If some host has a dynamic IP address that keeps changing frequently, it is difficult to keep updatingthe IP record that is associated with the domain name of this host in the zone files. This will resultin non-accessibility of this host on the Internet. Dynamic DNS service allows to keep mapping of adynamic IP address of such host to a static hostname. Dynamic DNS services are provided bymany websites. The host needs to register with some website and get a domain name. When theIP address of the host changes, it just needs to send a message to the website that's providingdynamic DNS service to this host. For this to work, an automated update client needs to beimplemented. These update clients send update messages to the servers whenever there is somechange in the IP address of that host. Then, the server updates the entries for that host and repliesback with some return code.



Above Figure explains one such scenario in which a host gets a dynamic IP address for itself from aDHCP server. As the host has registered with one of the dynamic DNS service providers on theInternet, it sends an update message to the service provider with host name and changed IPaddress. The service provider updates the new IP address of the host in the zone files that haveentry for that host name and replies back with some return code. The return code communicatesthe success or failure of the update message. This process is repeated every time the host's IPaddress changes.

If the dynamic DNS service provider is notified of the same IP address again and again, then itconsiders it an abuse and might block the host name. To avoid this scenario, the IP address thatwas successfully updated to the ISP is stored on the unit. Whenever we receive an IP addresschange notification, the new IP address is compared with the IP address that was stored on the lastupdate. If they differ, then only an update request is sent. However, when the system comes upthere is no way of knowing what was the IP address on last successful update before the systemwent down. You need to give the command “system config save“ periodically to save this IP addresson Flash.

Registering With Dynamic DNS Service Provider

Currently, Wireless Gateway supports two Dynamic DNS service providers, www.tzo.com andwww.dyndns.com. To use their Dynamic DNS service, you first need to visit the Web site of a serviceprovider and register. While registering, you need to provide your username, password, andhostname as mandatory parameters. A service provider may also prompt you to fill some optionalparameters.

Configuring IP Interfaces

You need to create a Dynamic DNS interface per IP interface and can only create one DynamicDNS interface service on one IP interface. For more information on creating IP interfaces, refer tosection Creating IP interfaces.

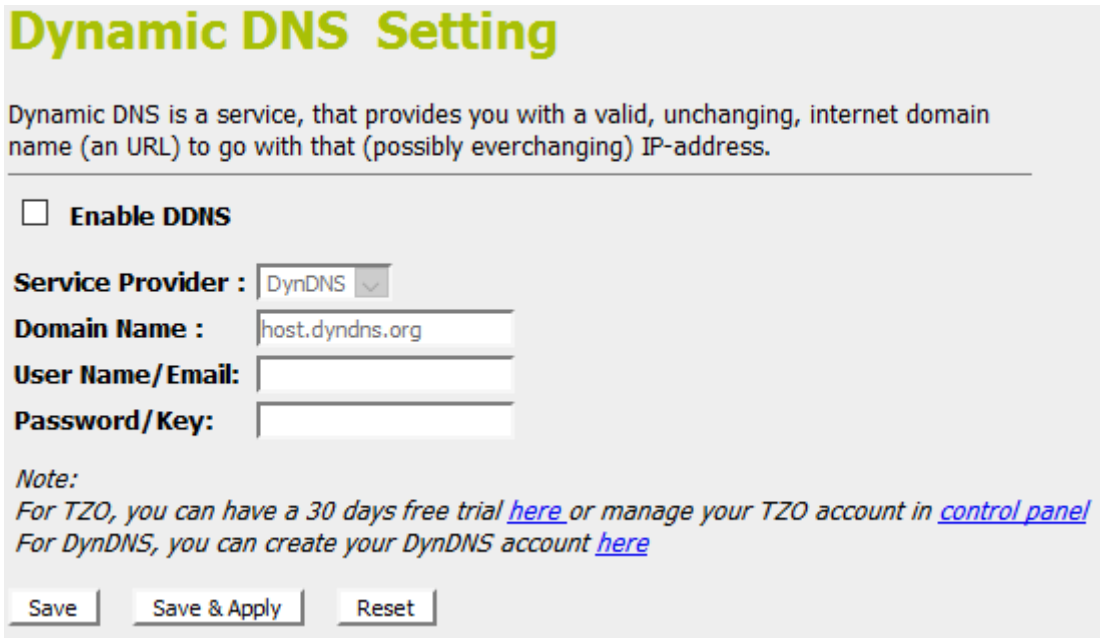
Note

www.dyndns.org provides three kinds of services - Dynamic DNS, Custom DNS and Static DNS. You can create different domains in these systems. Custom DNS service is a full DNS solution for newly purchased domains or domains you already own. A web-based interface provides complete control over resource records and your entire domain, including support for dynamic IPs and automated updates. Static DNS service points a DNS hostname in some domain owned by dyndns.org to the user's ISP-assigned static or pseudo-static IP address.

DynDNS service points a fixed hostname in some domain owned by dyndns.org to the user's ISP-assigned dynamic IP address. This allows more frequent update of IP addresses, than allowed by Static DNS.

1. From the head menu, click on *Management*.

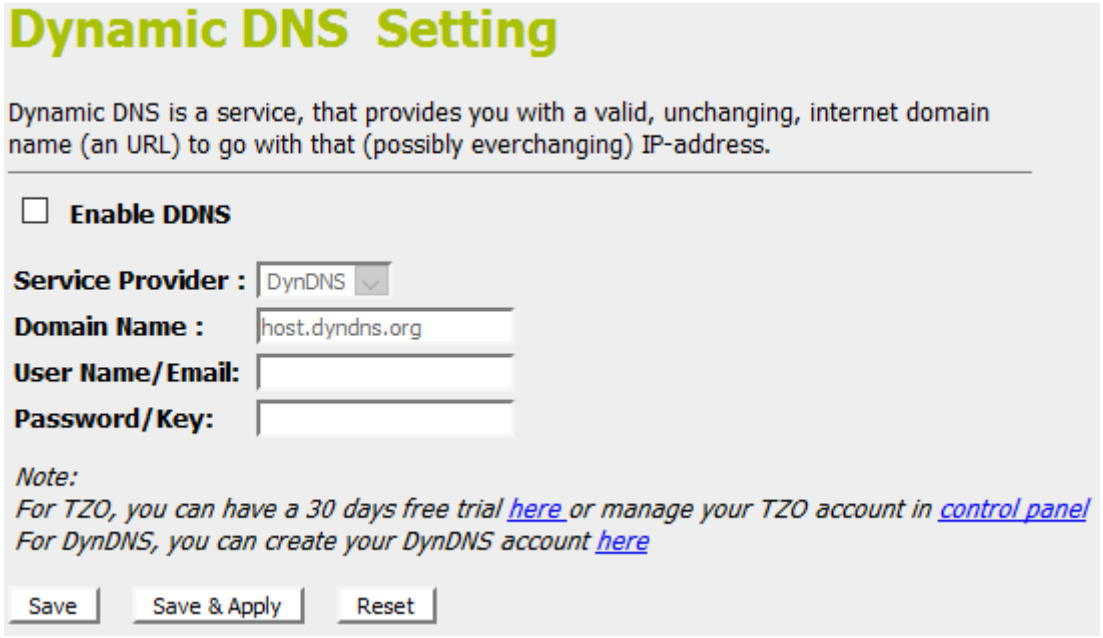
2. From the left-hand menu, click on *DDNS*. The following page is displayed:



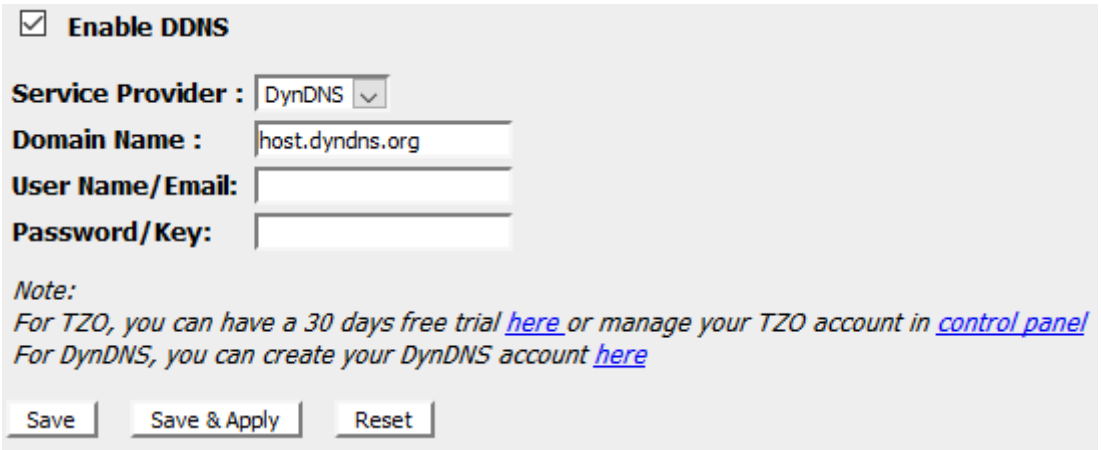
Configure DynDNS

1. From the head menu, click on *Management*.

2. From the left-hand menu, click on *DDNS*. The following page is displayed:



3. Click on *Enable DDNS*
4. Select the DynDNS from the *Service Provider* drop-down list.
5. Type your own unique *User Name*, *Password*and *Domain Name* which you applied from www.dyndns.comin the relevant boxes. They can be any combination of letters or numbers with a maximum of 20 characters.
6. Click *Save & Apply*.

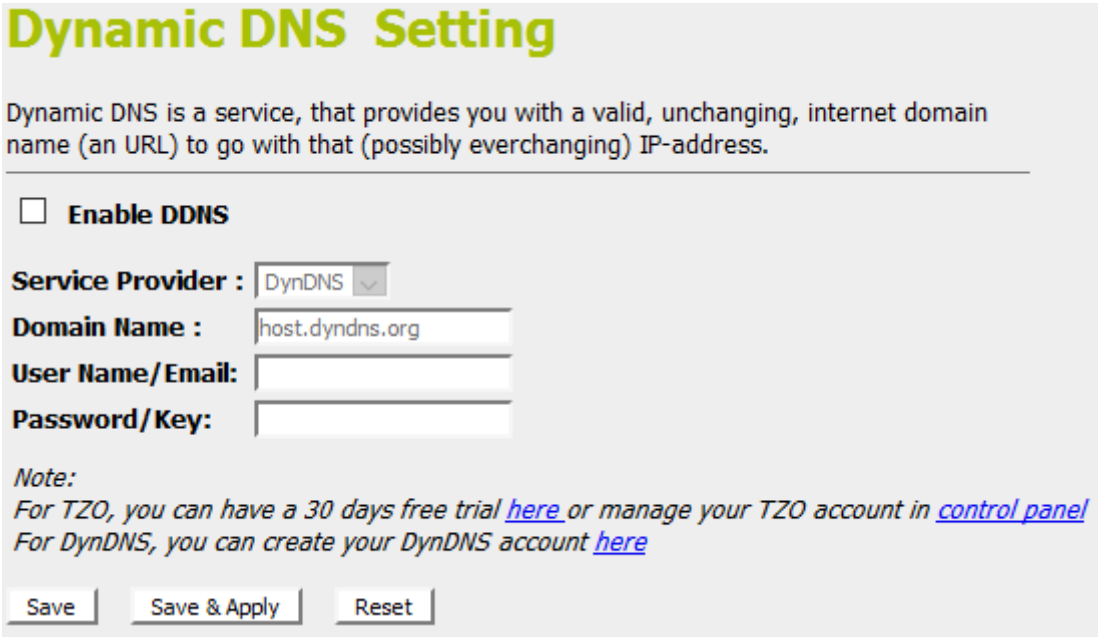


7. Change setting successfully! Please wait 20 seconds….

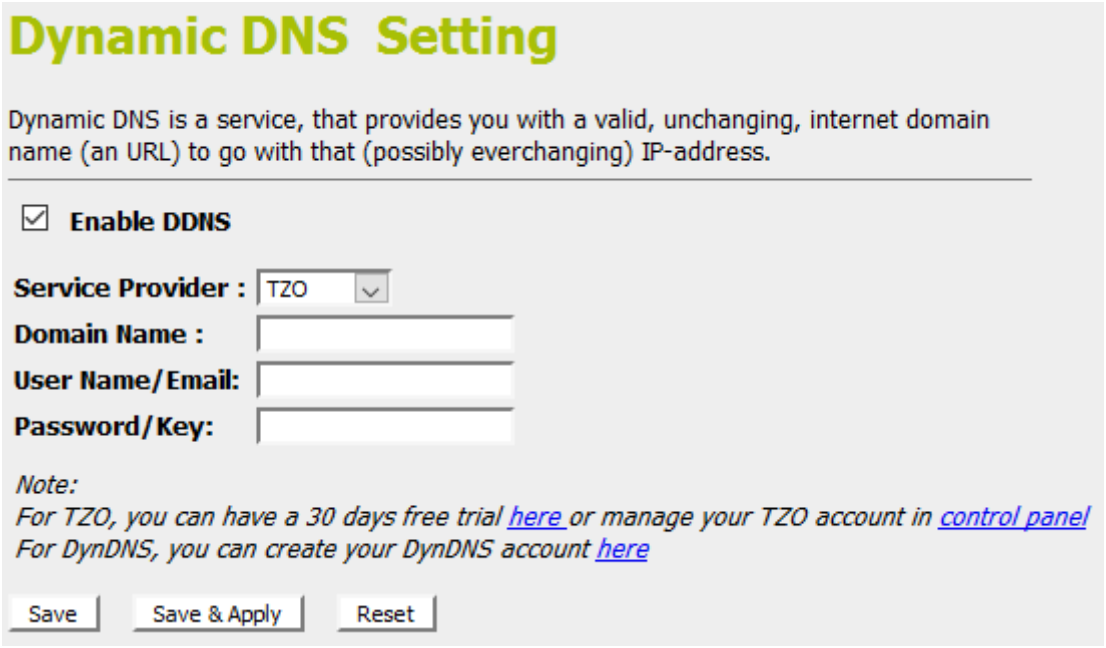
Configure TZO

1. From the head menu, click on *Management*.

2. From the left-hand menu, click on *DDNS*. The following page is displayed:



3. Click on *Enable DDNS*
4. Select the TZO from the *Service Provider* drop-down list.
5. Type your own unique *Email*, *Key*and *Domain Name* which you applied from http://www.tzo.com/MainPageWebClient/clientsignup.htmlin the relevant boxes. They can be any combination of letters or numbers with a maximum of 20 characters.
6. Click *Save & Apply*.



7. Change setting successfully! Please wait 20 seconds….

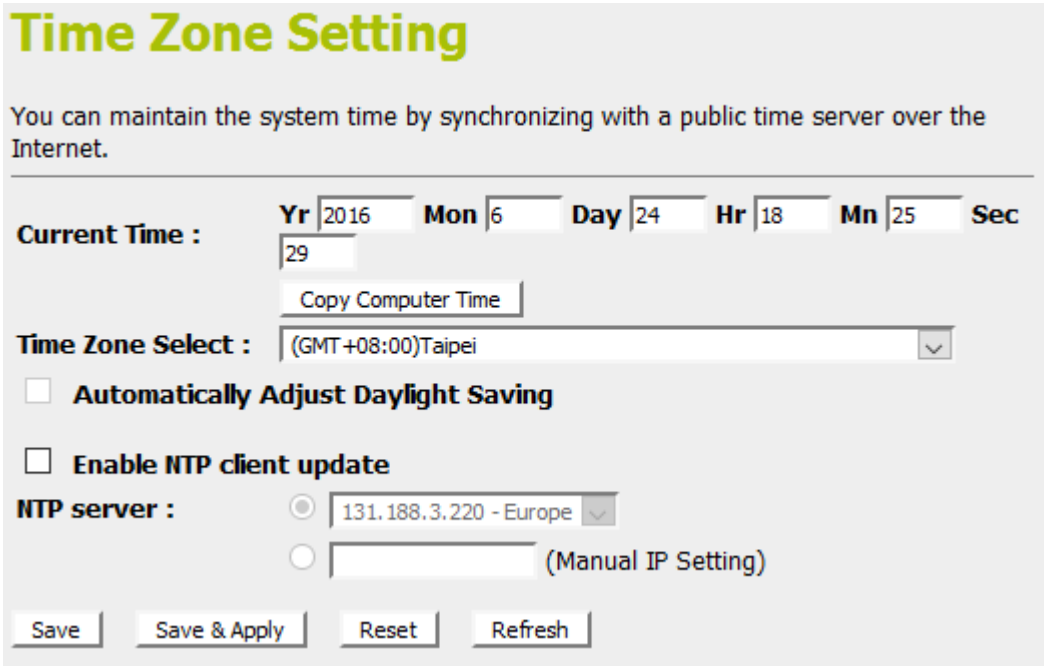
26 Time Zone Setting

Certain systems may not have a date or time mechanism or may be using inaccurate time/day information. the Simple Network Time Protocol feature provides a way to synchronize the device's own time of day setting with a remote time server as described in RFC 2030 (SNTP) and RFC 1305 (NTP).

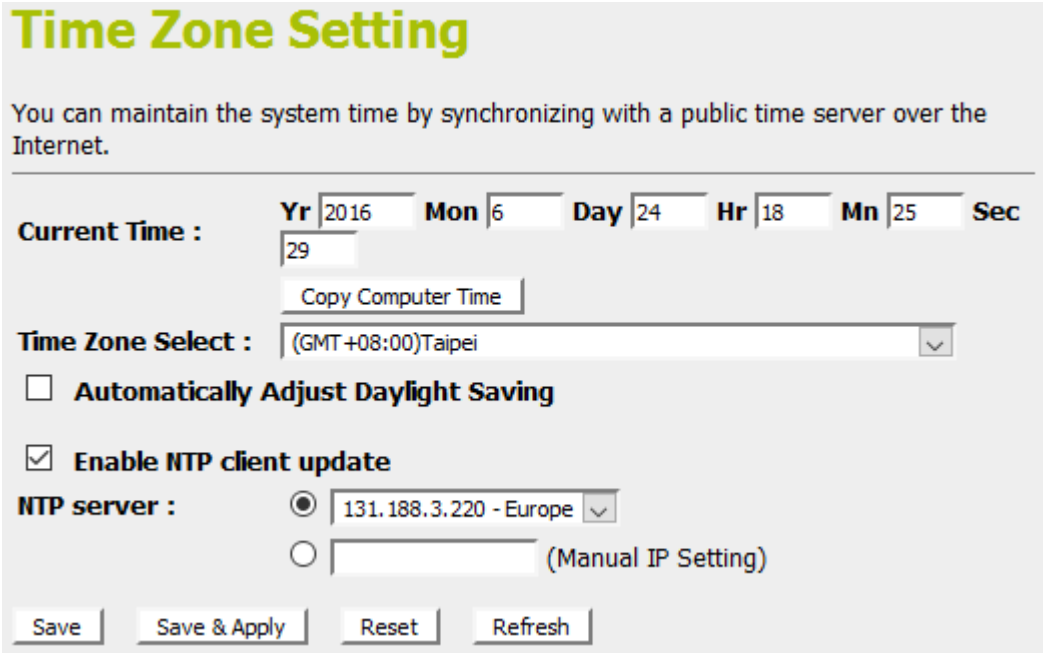
SNTP Server and SNTP Client Configuration settings

1. From the head menu, click on *Management*.

2. From the left-hand menu, click on *Time Zone Setting*. The following page is displayed:



3. From the *Time Zone Select*drop-down list, select *Your Own Time Zone*.
4. Check the option*Enable NTP client update*.
5. From the *NTP server*drop-down list, select a*NTP Server*. Or you can add server to the SNTP association list using IP address. Adding a server to the association list automatically starts the synchronization process.
6. Click *Save & Apply*.



7. Change setting successfully! Please wait 20 seconds….

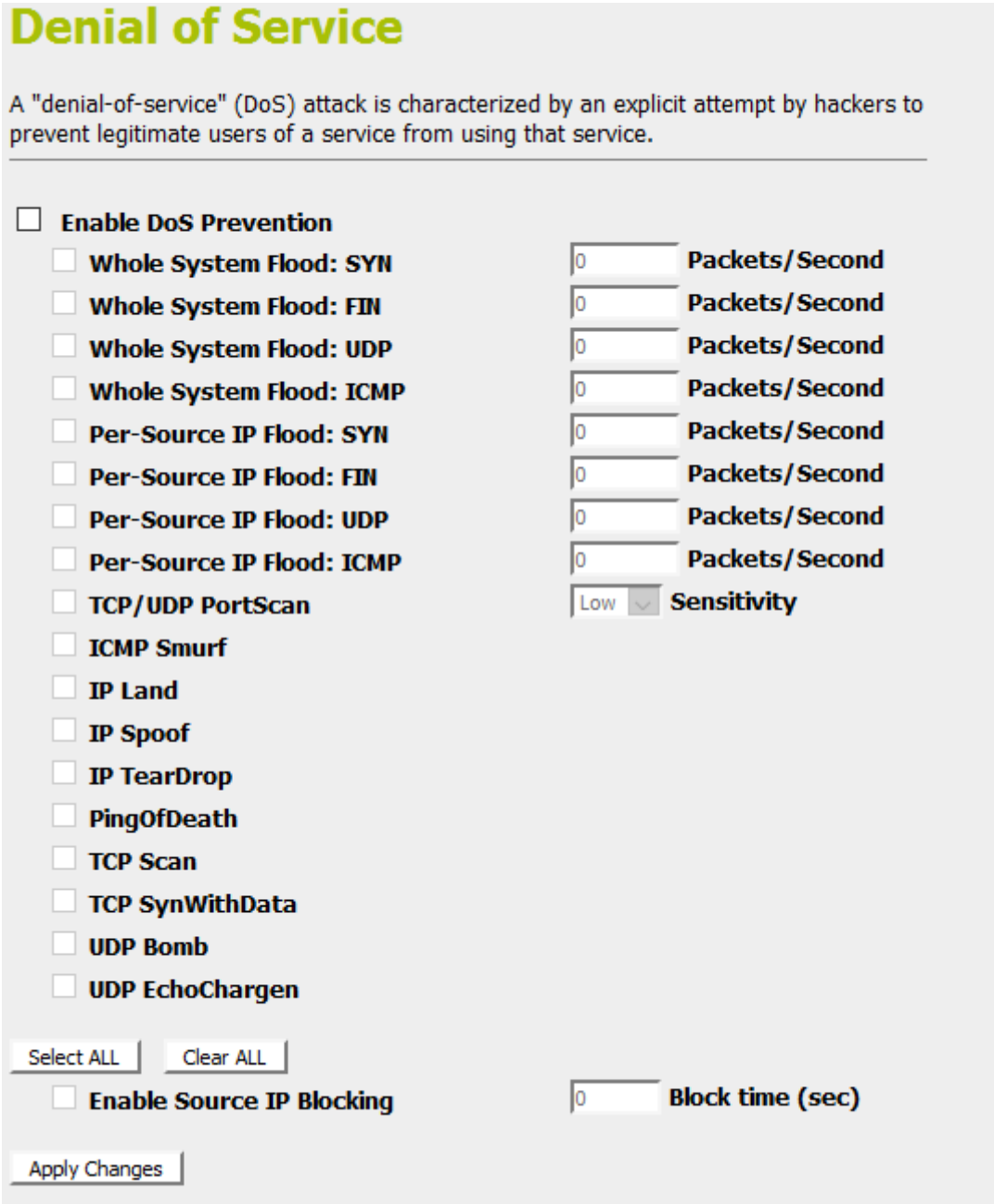
27 Denial-of-Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

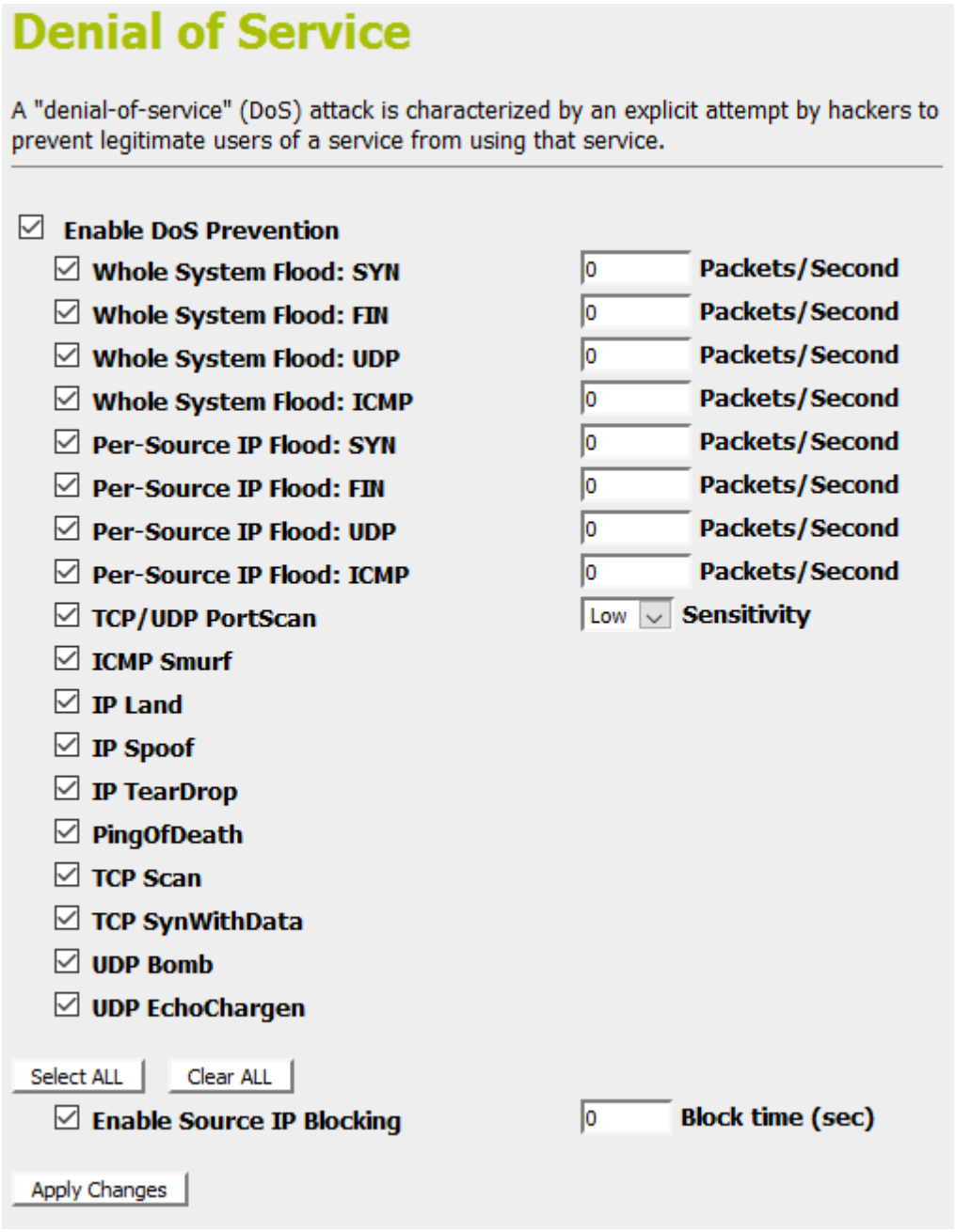
Denial-of-Service

1. From the head menu, click on *Management*.

2. From the left-hand menu, click on *Deny Of Service*. The following page is displayed:



3. Check the option*Enable DoS Prevention*.
4. Check the option of each*Service*.
5. Check the option*Enable Source IP Blocking*.
6. Click *Save & Apply*.



7. Change setting successfully! Please wait 20 seconds….

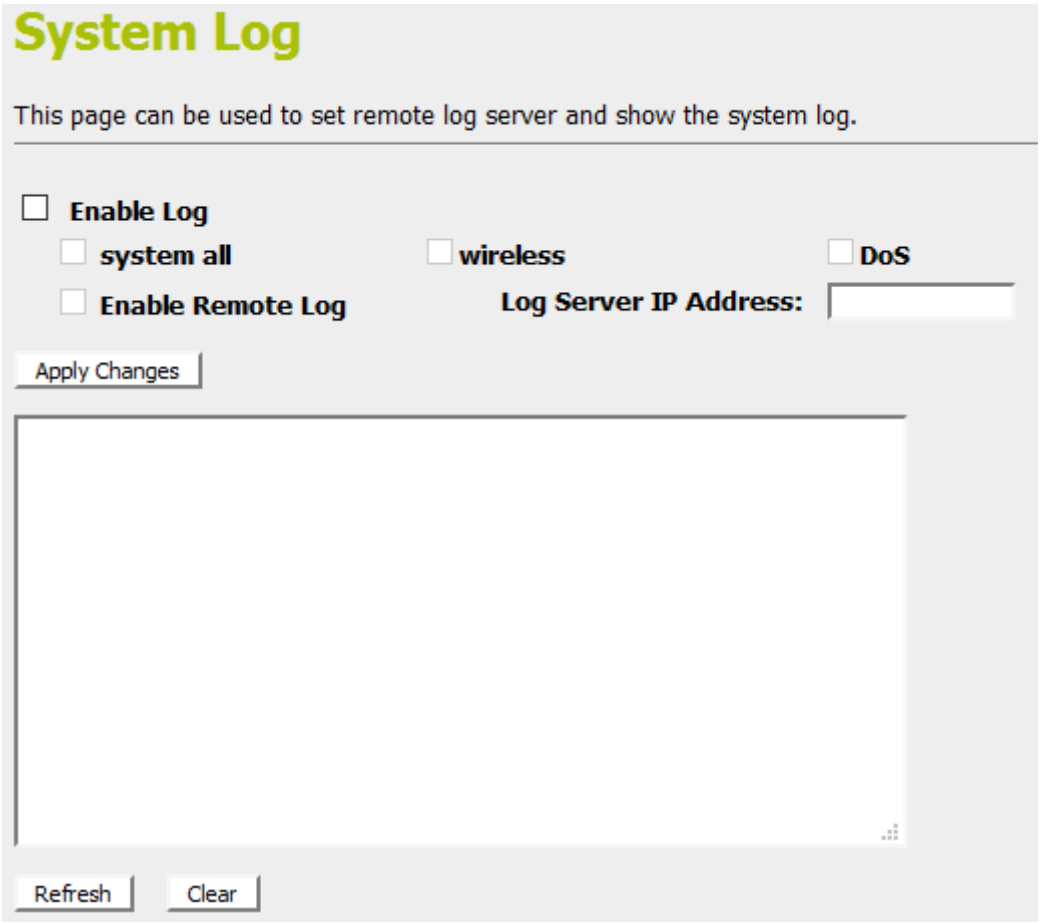
28 Log

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

System Log

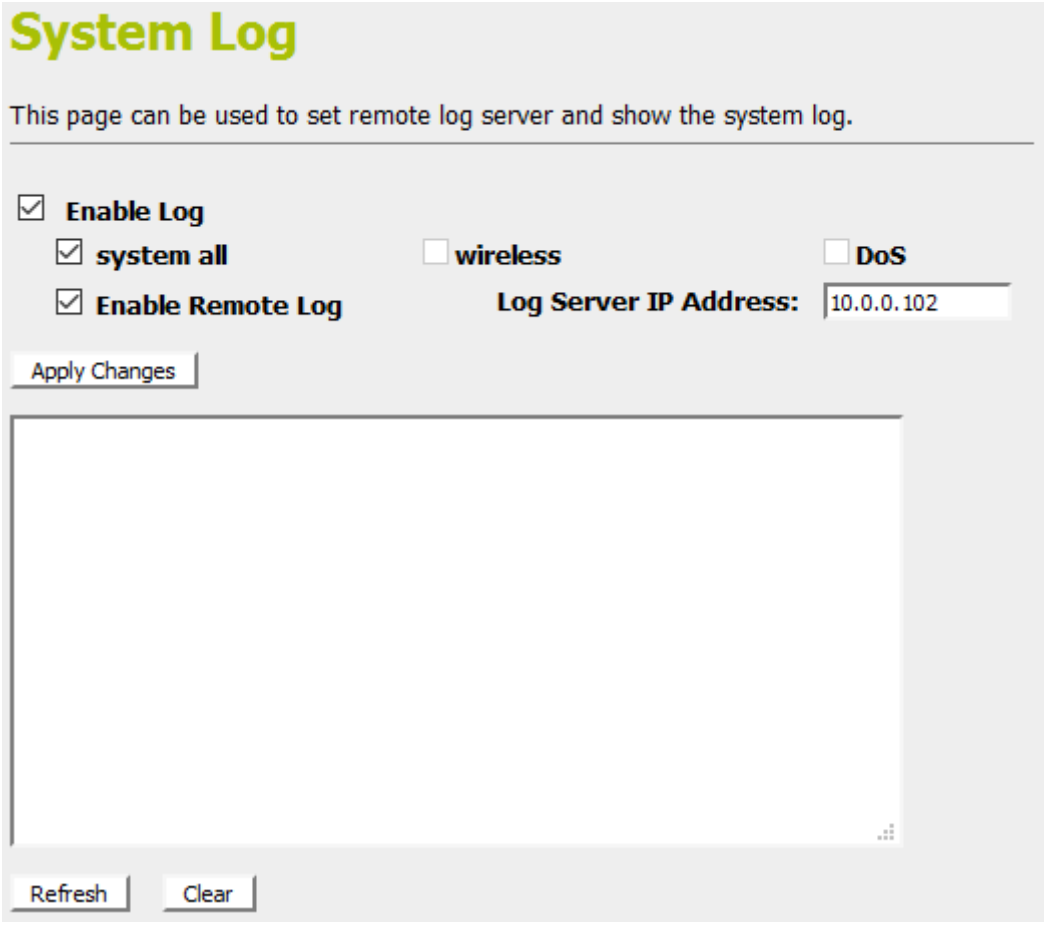
1. From the head menu, click on *Management*.

2. From the left-hand menu, click on *Log*. The following page is displayed:



Option	Description
Enable Log	**Enable/Disable the feature.** **Default: Disable**
system all	**All system logs will be recorded in the system log**
wireless	**The wireless logs will be recorded in the system log**
DoS	**The DoS logs will be recorded in the system log**
Enable Remote Log	**Enable: Send the system log to remote log server. To do this, make sure a secure syslog server is available. Default: Disable**
Log Server IP Address	**Enter the IP Address of remote log server.**

3. Check the option*Enable Log*.
4. Check the option *system all,wireless* or *DoS*.
5. Check the option*Enable Remote Log* if you
6. Enter the IP Address in the *Log Server IP Address* field.
7. Click *Save & Apply*.



8. Change setting successfully! Please wait 20 seconds….

29 Firmware Update

About firmware versions

Firmware is a software program. It is stored as read-only memory on your device.

Your device can check whether there are later firmware versions available. If there is a later version, you can download it via the Internet and install it on your device.

Note

If there is a firmware update available you are strongly advised to install it on your device to ensure that you take full advantage of any new feature developments.

Manually updating firmware

You can manually download the latest firmware version from provider's website to your PC's file directory.

1. Once you have downloaded the latest firmware version to your From the head menu, click on *Management*.

2. From the left-hand menu, click on *Upgrade Firmware*. The following page is displayed:
3. Click on the *Browse…* button.

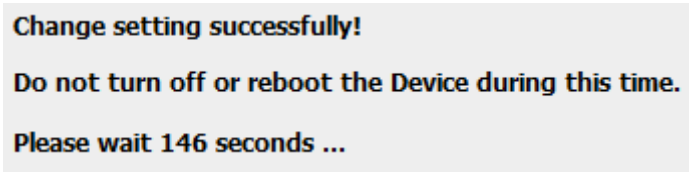
Figure 9: Manual Update Installation section

(Note that if you are using certain browsers (such as *Opera 7*) the *Browse* button is labeled *Choose*.)

Use the *Choose file* box to navigate to the relevant directory where the firmware version is saved.

4. Once you have selected the file to be installed, click *Open*. The file's directory path is displayed in the *New Firmware Image:* text box.
5. Click *Upload*. The device checks that the selected file contains an updated version of firmware. A status screen pops up, please wait for a while…….

6. Firmware update has been update complete. The following page is displayed:



30 Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously.

Besides, you could reset the current configuration to factory default.

If you do make changes to the default configuration but then wish to revert back to the original factory configuration, you can do so by resetting the device to factory defaults.

Save Settings to File

It allows you save current settings to a file.

1. From the left-hand *Management* menu, click on *Reset factory default*. The following page is displayed:

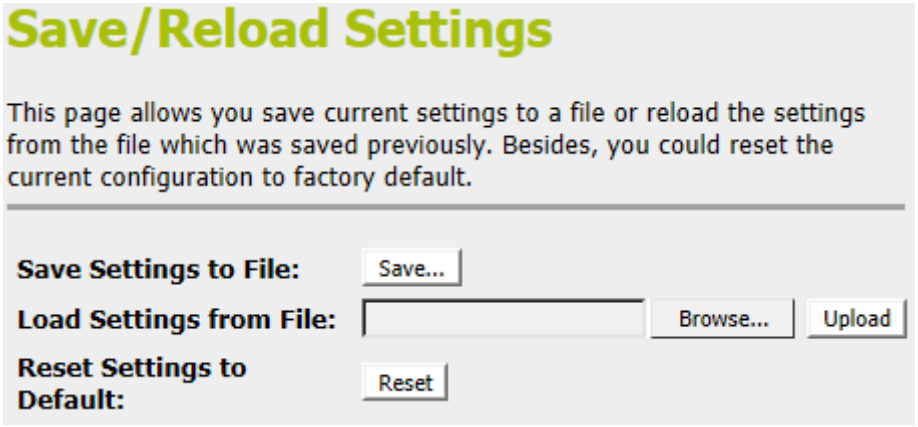
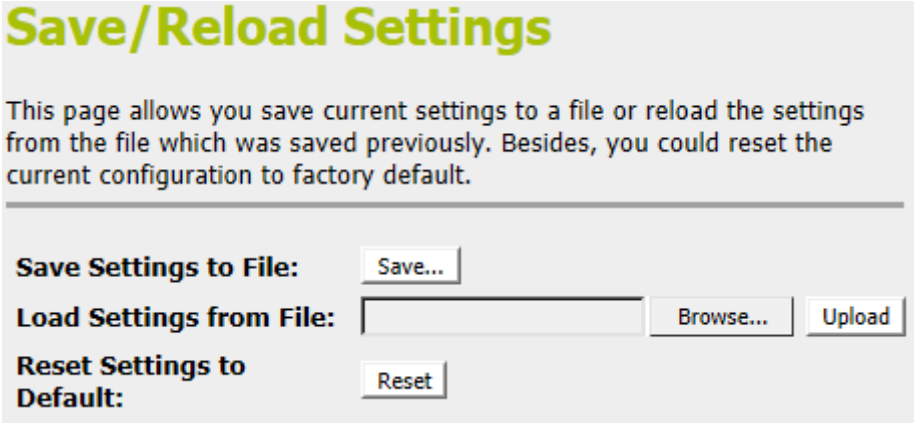


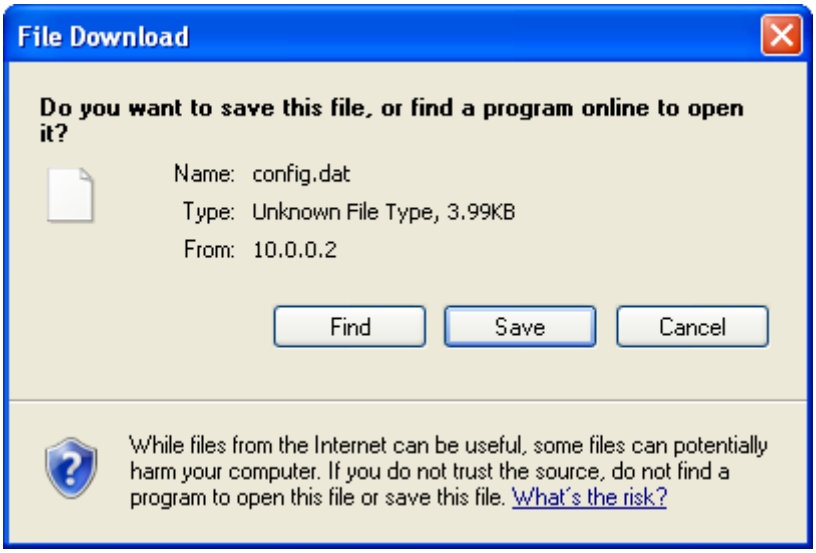
Figure 10: Reset to Defaults page

Option	Description
Save Settings to File	**Save the Settings to a File**
Load Settings from File	**Load Settings from a File**
Reset Settings to Default	**Reset Settings to Factory Default**

2. Click on *Save*….



3. If you are happy with this, click *Save* and then browse to where the file to be saved. Or click *Cancel* to cancel it.



Load Settings from File

It allows you to reload the settings from the file which was saved previously.

1. From the left-hand *Management* menu, click on *Reset factory default*. The following page is displayed:

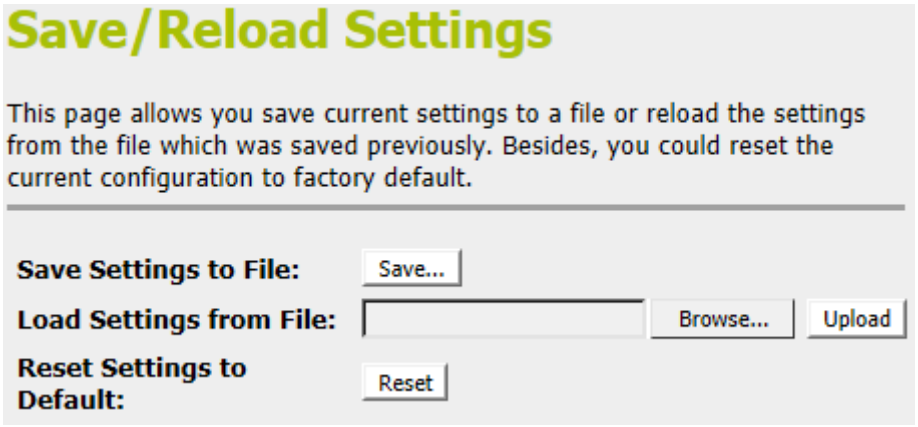
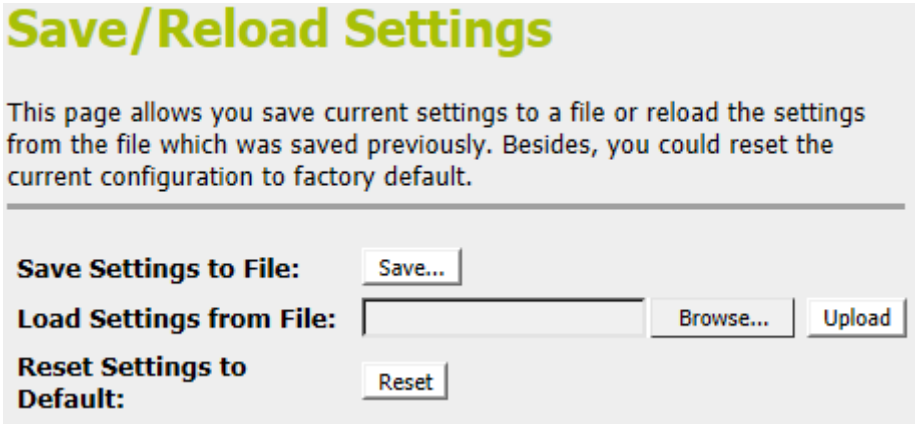
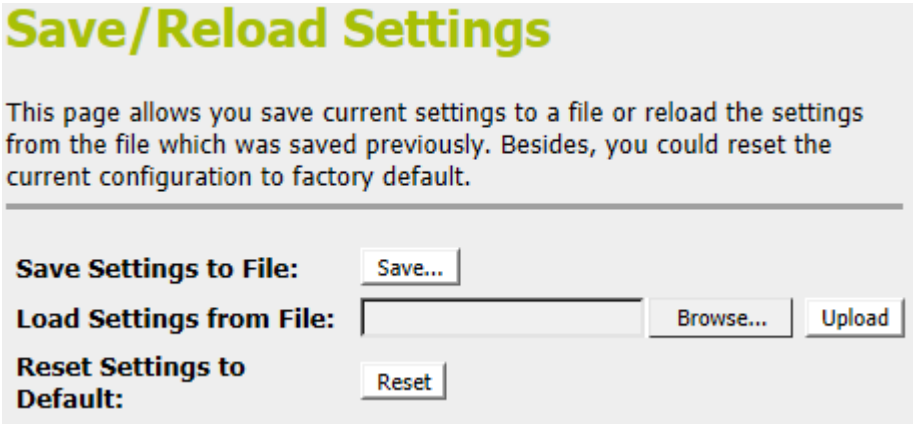


Figure 11: Reset to Defaults page

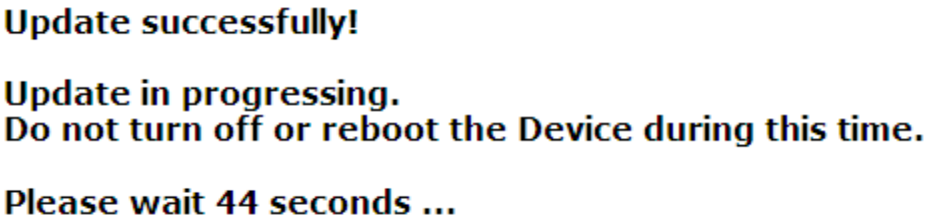
2. Click on *Browse*….to browse to where the config.dat is.



3. If you are happy with this, click *Upload* to start to load settings from file.



4. Once it finished loading settings form file, it'll show the message below.



Resetting to Defaults

If you do make changes to the default configuration but then wish to revert back to the original factory configuration, you can do so by resetting the device to factory defaults.

Note

If you reset your device to factory defaults, all previous configuration changes that you have made are overwritten by the factory default configuration.

Software Reset:

1. From the left-hand *Management* menu, click on *Reset factory default*. The following page is displayed:

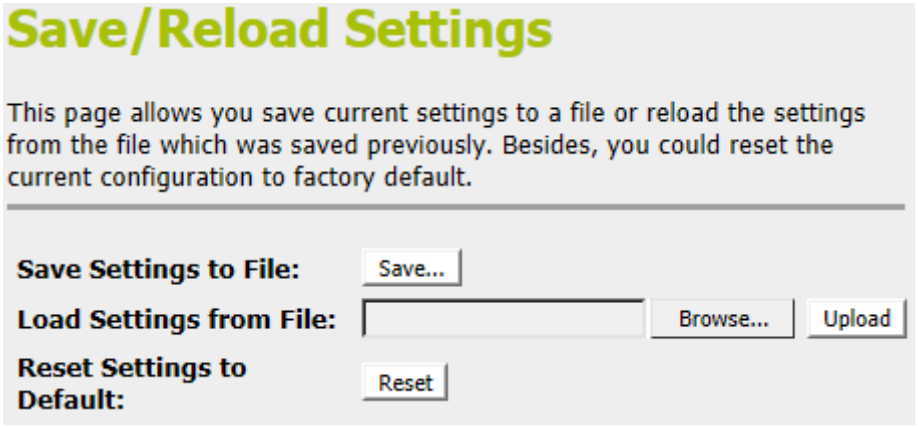
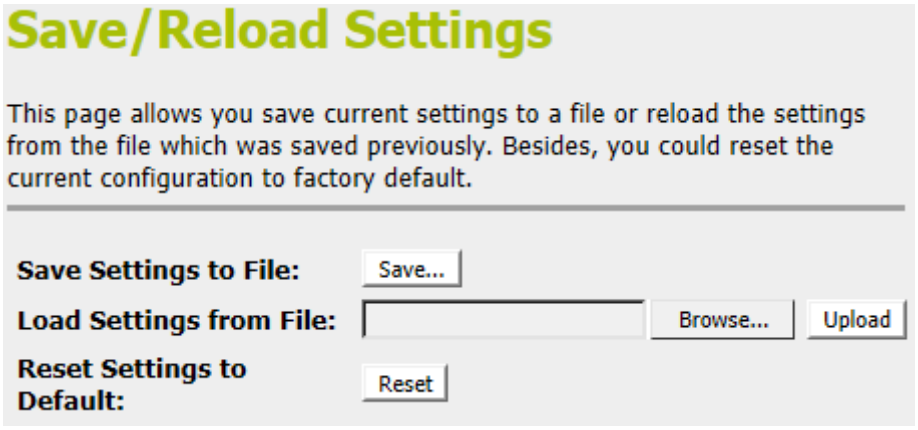
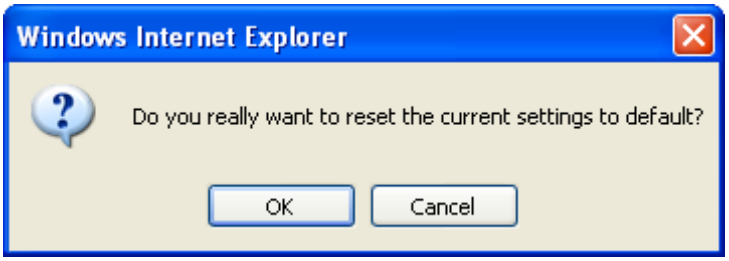


Figure 12: Reset to Defaults page

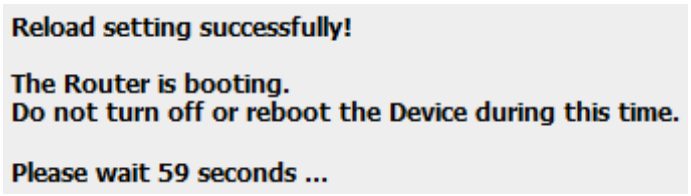
2. Click on *Reset to Default*.



3. This page reminds you that resetting to factory defaults cannot be undone – any changes that you have made to the basic settings will be replaced. If you are happy with this, click *OK*. Or click *Cancel* to cancel it.



4. Reload setting successfully! Please wait for a moment while rebooting ...



31 Password

You can restrict access to your device's web pages using password protection. With password protection enabled, users must enter a username and password before gaining access to the web pages.

By default, password protection is enabled on your device, and the username and password set are as follows:

Username: **admin**

Password: **administrator**

Setting your username and password

Note

Non-authorized users may try to access your system by guessing your username and password. We recommend that you change the default username and password to your own unique settings.

To change the default password:

1. From the left-hand *Management* menu, click on *Password*. The following page is displayed:

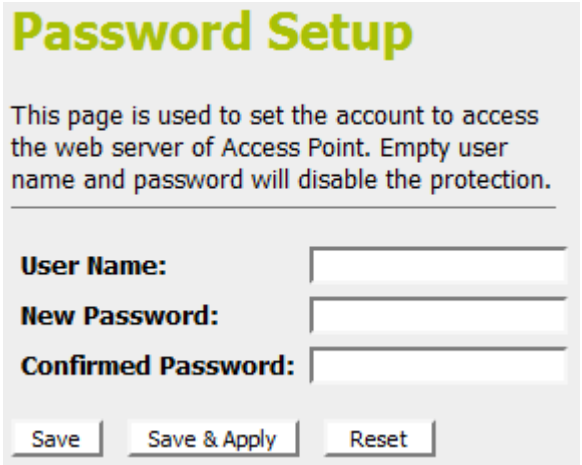


Figure 13: Currently Defined Administration Password: Setup page

2. This page displays the current username and password settings. Change your own unique password in the relevant boxes. They can be any combination of letters or numbers with a maximum of 30 characters. The default setting uses ***admin*** for the username and **administrator** for password.
3. If you are happy with these settings, click ***Save & Apply***You will see following page that the new user has been displayed on the Currently Defined Users. You need to login to the web pages using your new usernameand new password.

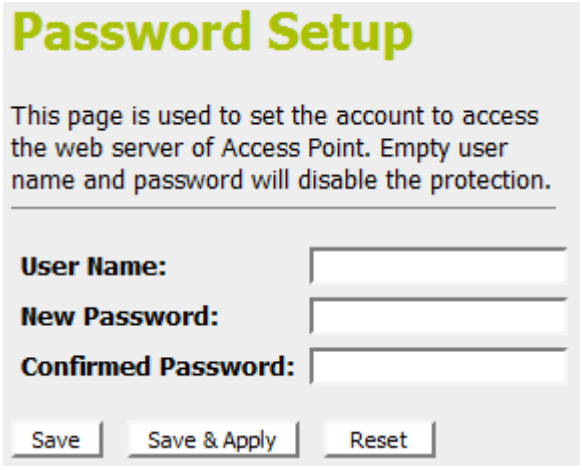
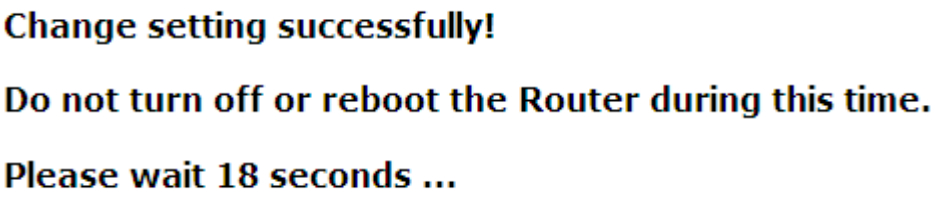


Figure 14: Administration Password

4. Change setting successfully.



5. Enter new *User name* and *Password*.
6. Click *Apply.*

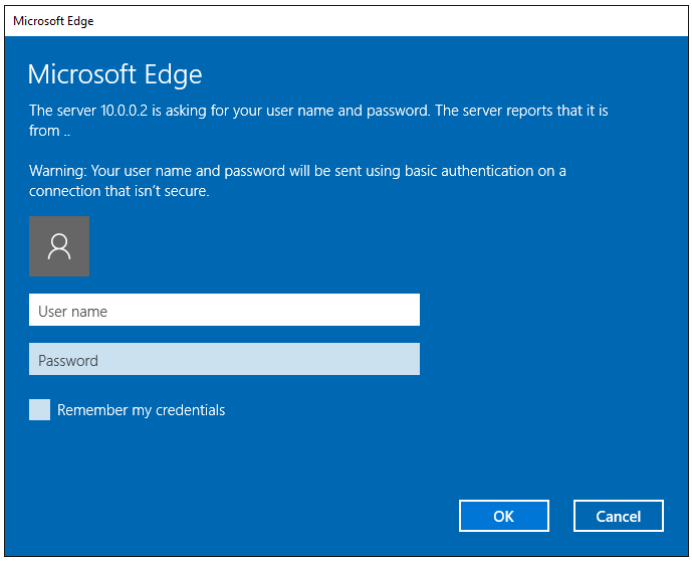


Figure 15: Login page

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 *10.0.0.2*. (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".

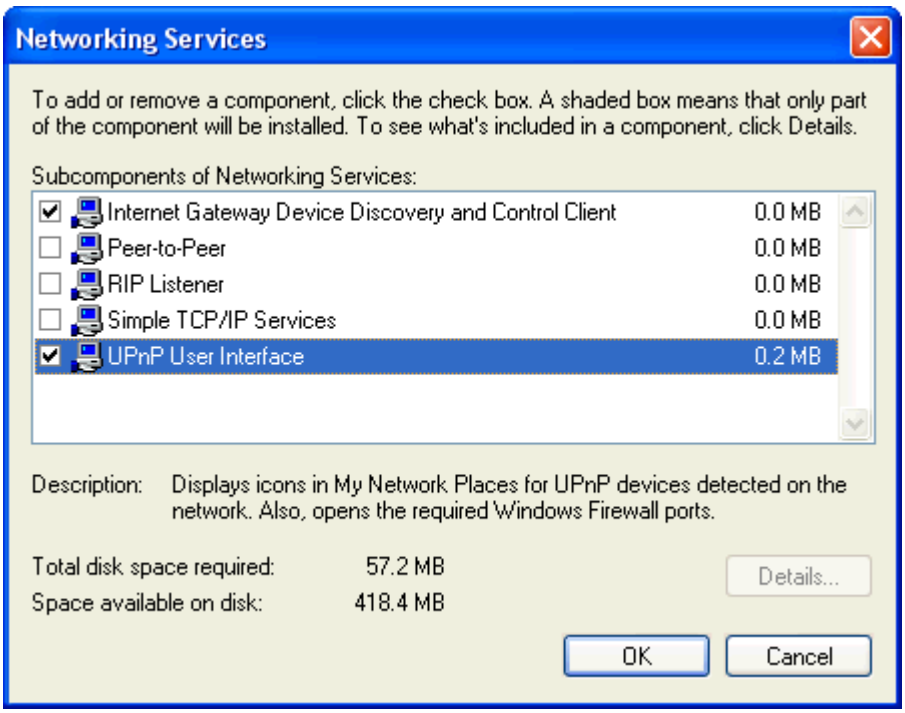
2. In the "Add or Remove Programs" dialog box, click the "Add / Remove Windows Components" button.

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:



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:

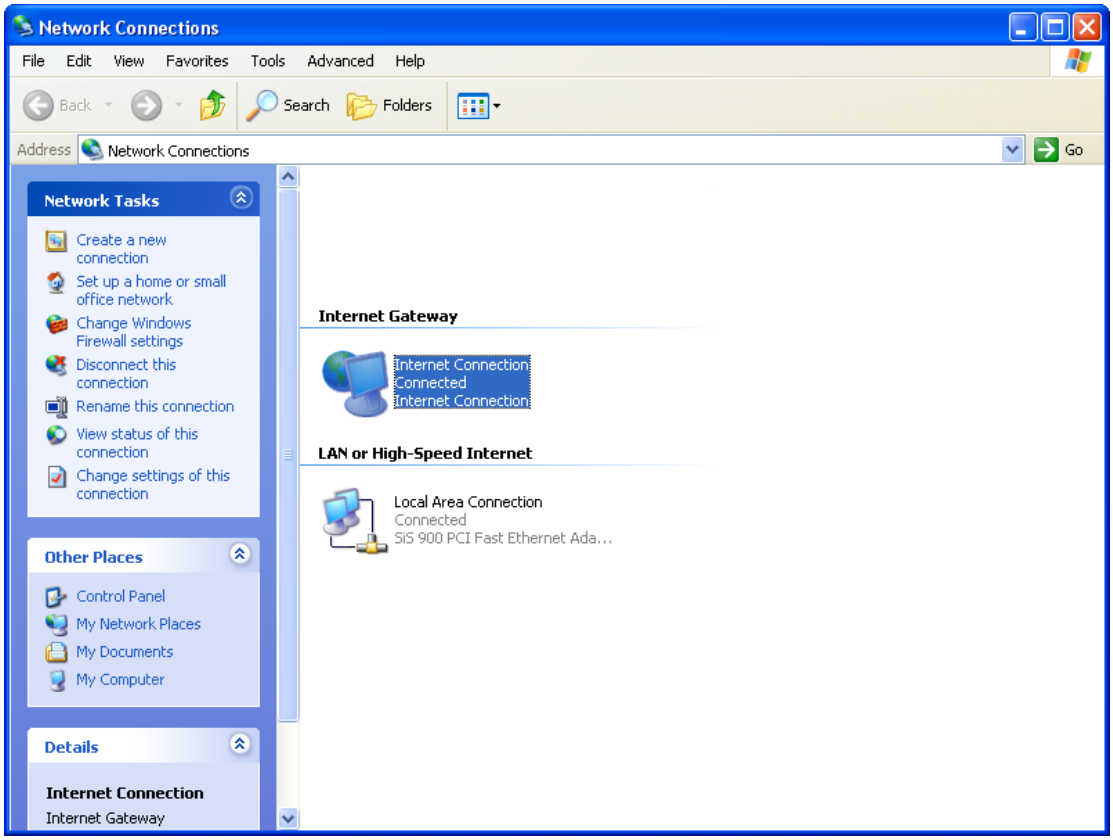
• "Internet Gateway Device discovery and Control Client".

• "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:



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 10.0.0.2). 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 “administrator“ 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 10.0.0.2). 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.

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 10.0.0.2

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:

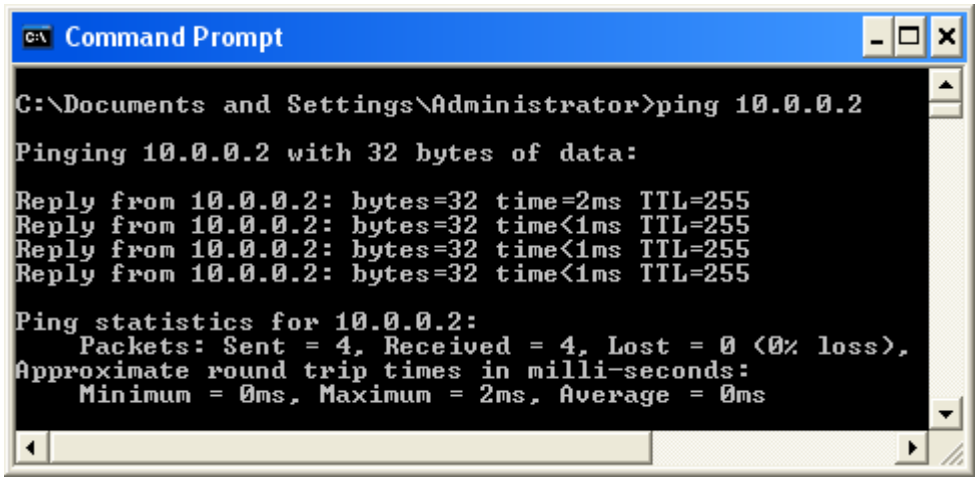


Figure 16: Using the ping Utility

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 10.0.0.2) 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:

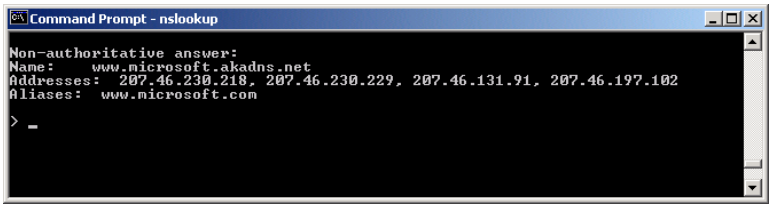


Figure 17: Using the nslookup Utility

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 LICENSE STATEMENT / GPL CODE STATEMENT

This product resp. the here (http://global.level1.com/downloads.php?action=init) for downloading offered software includes software code developed by third parties, including software code subject to the GNU General Public License Version 2 (“GPLv2”) and GNU Lesser General Public License 2.1 („LGPLv2.1“).

WRITTEN OFFER FOR GPL/LGPL SOURCE CODE

We will provide everyone upon request the applicable GPLv2 and LGPLv2.1 source code files via CDROM or similar storage medium for a nominal cost to cover shipping and media charges as allowed under the GPLv2 and LGPLv2.1. This offer is valid for 3 years. GPLv2 and LGPLv2 inquiries: Please direct all GPL and LGPL inquiries to the following address:

Digital Data Communications GmbH

Zeche-Norm-Str. 25

44319 Dortmund

Deutschland

Phone: +49 231 9075 - 0

Fax: +49 231 9075 - 184

Email: support@level1.com

Web: www.level1.com

NO WARRANTY

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN

WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

```
51 Franklin Street, Fifth Floor, Boston, MA  02110-
1301, USA

Everyone is permitted to copy and distribute verbatim
copies
of this license document, but changing it is not
allowed.
```

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this

service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but

does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

we use this doubled UL to get the sub-sections indented, while making the bullets as unobvious as possible.

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than

your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include

anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited

to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the

sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be

guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
one line to give the program's name and an idea of
what it does.
Copyright (C) yyyy  name of author

This program is free software; you can redistribute
it and/or
modify it under the terms of the GNU General Public
License
as published by the Free Software Foundation; either
version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will
be useful,
but WITHOUT ANY WARRANTY; without even the implied
warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
See the
GNU General Public License for more details.
```

```
You should have received a copy of the GNU General
Public License
along with this program; if not, write to the Free
Software
Foundation, Inc., 51 Franklin Street, Fifth Floor,
Boston, MA  02110-1301, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of
author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for
details
type `show w'.  This is free software, and you are
welcome
to redistribute it under certain conditions; type
`show c'
for details.
```

The hypothetical commands `` `show w' `` and `` `show c' `` should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `` `show w' `` and `` `show c' ``; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright

disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright
interest in the program `Gnomovision'
(which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

Notification of Compliance

Europe - EU Declaration of Conformity

For complete DoC please visit

http://global.level1.com/downloads.php?action=init

GPL License Agreement

GPL may be included in this product, to view the GPL license agreement goes to

http://download.level1.com/level1/gpl/GPL.pdf

For GNU General Public License (GPL) related information, please visit http://global.level1.com/downloads.php?action=init.