MC-421

WLAN Router

user's manual

MODECOM

MC-421
WLAN Router

Contents:

Introduction

Congratulations on becoming the owner of the Wireless Gateway. 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 Wireless Gateway, 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
- IOP (Inter-Operability) with major soft-switch vendors
- SIP signaling supporting
- Supports remote software upgrades
- Plug & Play, Auto Configuration / Auto Provisioning
- User-friendly configuration program accessed via a web browser
- User-friendly configuration program accessed via EasySetup program

The Wireless Gateway 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 Wireless Gateway and a co-located PC or other Ethernet-based device.

Device Requirements

In order to use the Wireless Gateway, 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 (10Base-T/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 Wireless Gateway 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	*Provides clarifying or non-essential information on the current topic.*
WARNING	*Provides clarifying or non-essential information on the current topic.*

Parameters that you need to configure the Wireless Gateway

Following table is the parameters that you need to configure the Wireless Gateway.

If you cannot get the Internet/WAN access of your own network, it's difficult to configure the Wireless Gateway correctly and have it work properly.

Parameters that you need to configure the Wireless Gateway			
	Internet/WAN Access of your own Network		
	DHCP Client	PPPoE Client	Static IP
Obtain an IP Address automatically	X	N/A	N/A
Username	N/A	1234	N/A
Password	N/A	1234	N/A
IP Address	N/A	N/A	192.168.10.110
Subnet Mask	N/A	N/A	255.255.255.0
Gateway	N/A	N/A	192.168.10.100
DNS Server IP	N/A	N/A	192.168.10.100

Note:

Username / Password which was given by Telecom or by your Internet Service Provider (ISP).

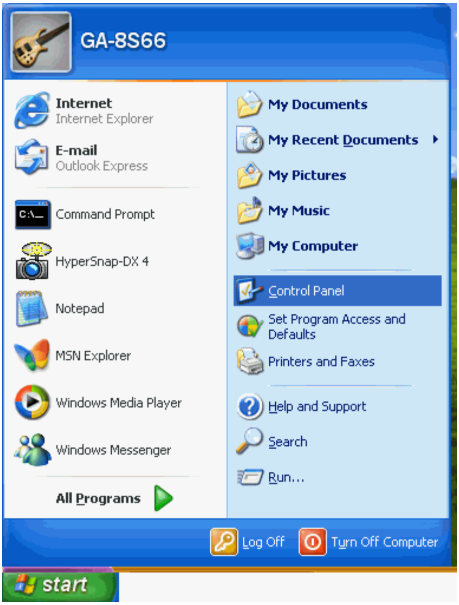
IP Address / Subnet Mask / Gateway / DNS Server IP which was given by your network administrator or by Telecom or by your Internet Service Provider (ISP).

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

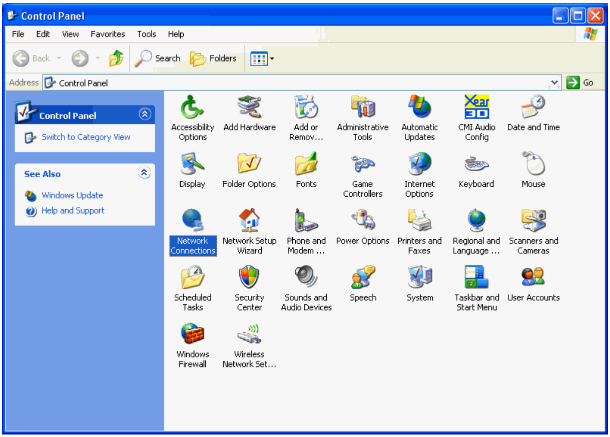
Now you could check what the Internet/WAN access of your network is to know how to configure the WAN port of Wireless Gateway.

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

Click Start -> Control Panel



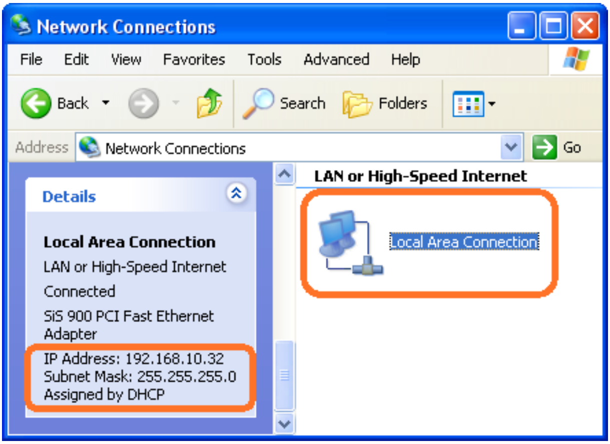
Double click Network Connections



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.

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

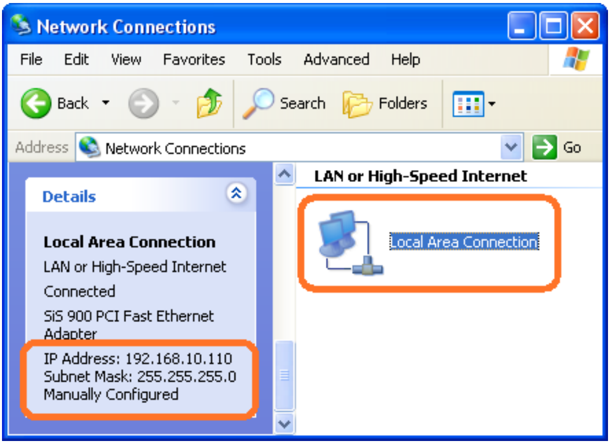


Local Area Connection
LAN or High-Speed Internet
Connected
SiS 900 PCI Fast Ethernet Adapter
IP Address: 192.168.10.32
Subnet Mask: 255.255.255.0
Assigned by DHCP

Internet/WAN access is the Static IP

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

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



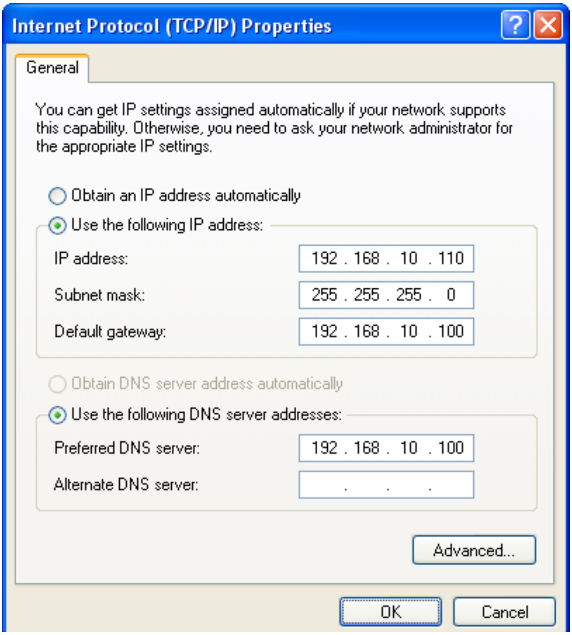
Local Area Connection
LAN or High-Speed Internet
Connected
SiS 900 PCI Fast Ethernet Adapter
IP Address: 192.168.10.110
Subnet Mask: 255.255.255.0
Manually Configured

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 Protocol (TCP/IP) Properties

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 10 . 110

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 10 . 100

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 10 . 100

Alternate DNS server: . . .

Internet/WAN access is the PPPoE client

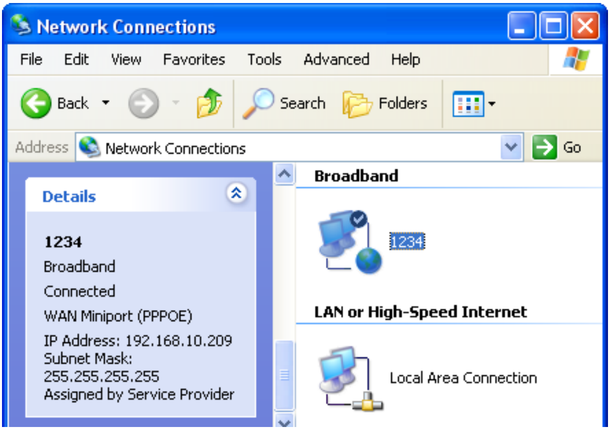
If you can see any Broadband Adapter in the Network Connections, your Internet/WAN access is PPPoE Client.

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



Network Connections

Details

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

Broadband

1234

LAN or High-Speed Internet

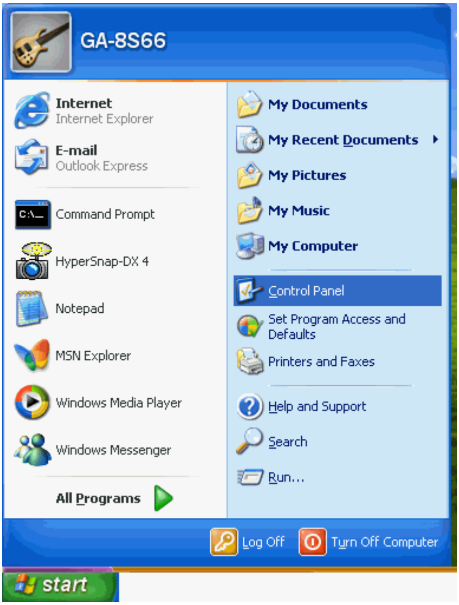
Local Area Connection

Configure the Obtain an IP Address automatically for LAN Card

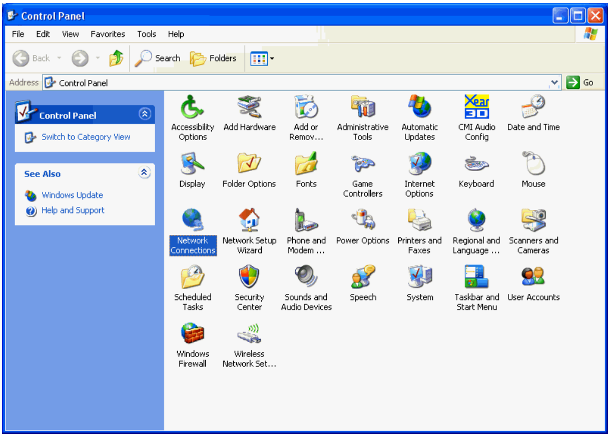
To configure the Wireless Gateway by Easy Setup utility or Web page, please follow steps below to configure your LAN Card to obtain an IP Address automatically (DHCP Client).

If your LAN Card is configured to obtain an IP Address automatically (DHCP Client) already, just skip this chapter.

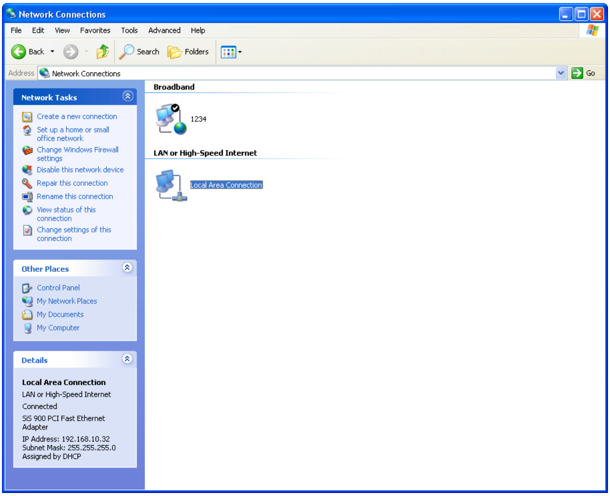
Click Start -> Control Panel



Double click Network Connections

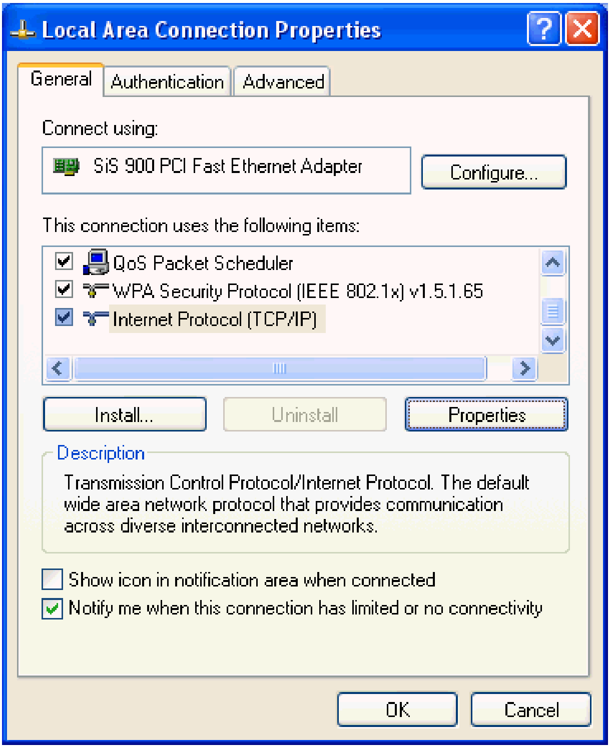


Right click Local Area Connection and then click Properties


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections Go
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
Other Places
Control Panel
My Network Places
My Documents
My Computer
Details
Broadband
1234
LAN or High-Speed Internet
Local Area Connection

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

Click Internet Protocol [TCP/IP] and then click Properties



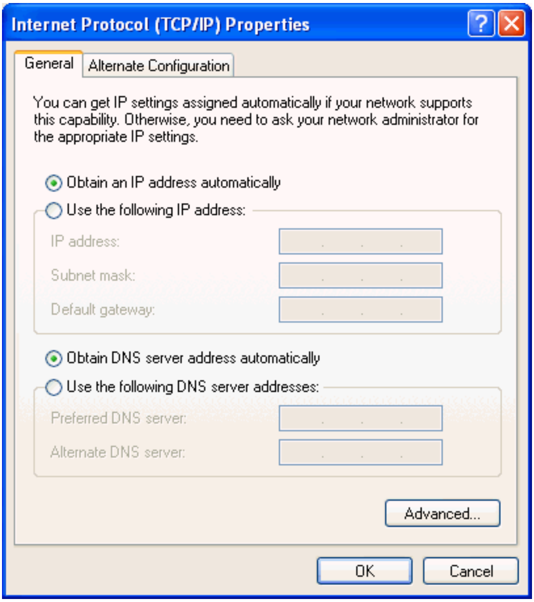
Connect using:
SiS 900 PCI Fast Ethernet Adapter

This connection uses the following items:
☑ QoS Packet Scheduler
☑ WPA Security Protocol (IEEE 802.1x) v1.5.1.65
☑ Internet Protocol (TCP/IP)

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

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

Select Obtain and IP Address automatically and then click OK



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

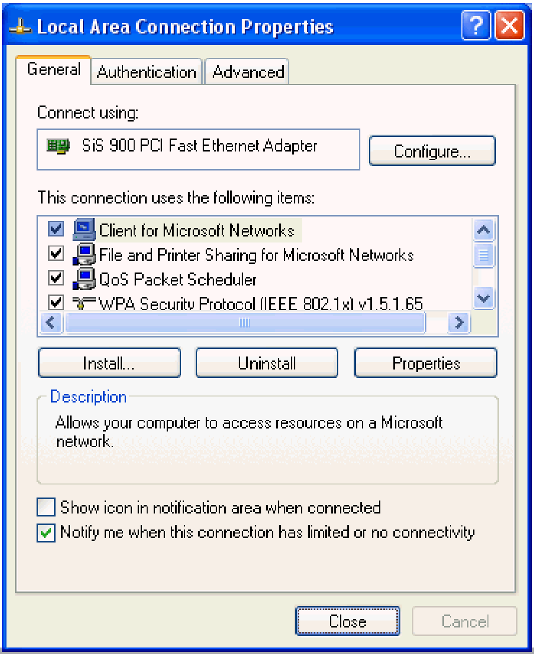
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

Click Close

Now you've already configured the LAN to obtain an IP Address automatically (DHCP Client), just follow reset steps to finish the installation of Wireless Gateway.



Local Area Connection Properties

General | Authentication | Advanced

Connect using:
SiS 900 PCI Fast Ethernet Adapter

This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ WPA Security Protocol (IEEE 802.1x) v1.5.1.65

Description
Allows your computer to access resources on a Microsoft network.

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

Getting to know the device

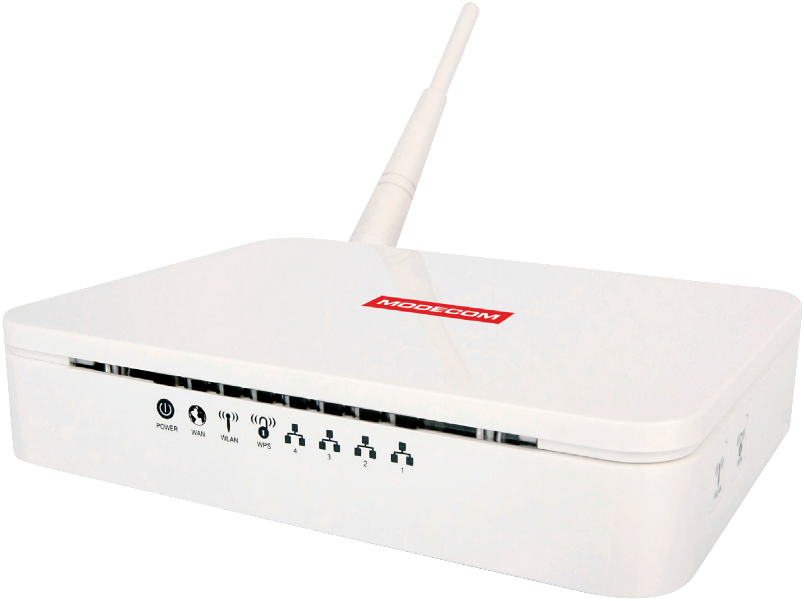
Parts Check

In addition to this document, your package should arrive containing the following:

1. Wireless Gateway
2. Ethernet cable
3. CD-ROM containing the online manual
4. QIG
5. Power Adapter

Front Panel

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

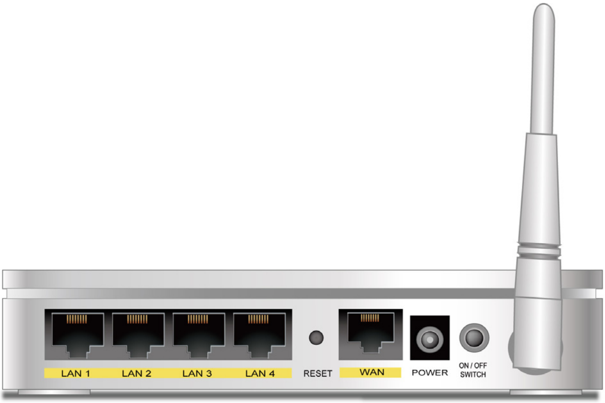


Front Panel and LEDs

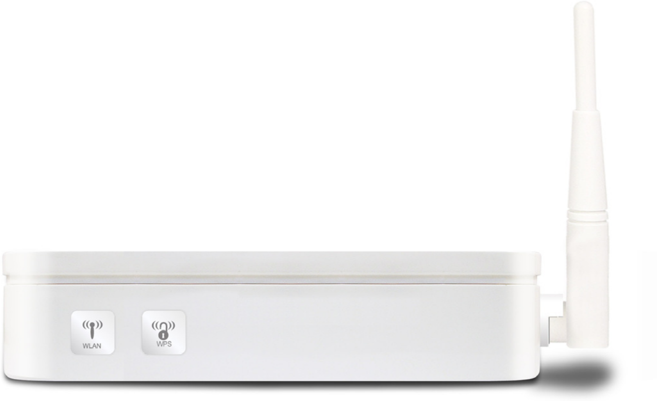
Label	Color	Function
POWER	green	On: device is powered on Off: device is powered off
WLAN	green	On: WLAN link established and active Blink: Valid Wireless packet being transferred
WPS	green	Off: WPS link isn't established and active Blink: Valid WPS packet being transferred
WAN	green	On: WAN link established 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

Rear and Right Panel

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



Rear Panel Connections



Right Panel Connections

Label	Function
ANETENNA	ANETENNA
ON/OFF SWITCH	Power on/off the device
POWER	Connects to the supplied power cable
LAN 4/3/2/1	Connects the device via Ethernet to up to four PCs on your LAN
WAN	Connects the device via Ethernet to xDSL / Cable Modem
RESET	Pressing this button for 3 seconds to restores the factory default configuration on your device

Label	Function
WLAN	Press this button for 5 seconds to Disable or Enable Wireless LAN.
WPS	Press this button for 3 seconds to Enable WPS function.

Connecting your device

This chapter provides basic instructions for connecting the Wireless Gateway 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.

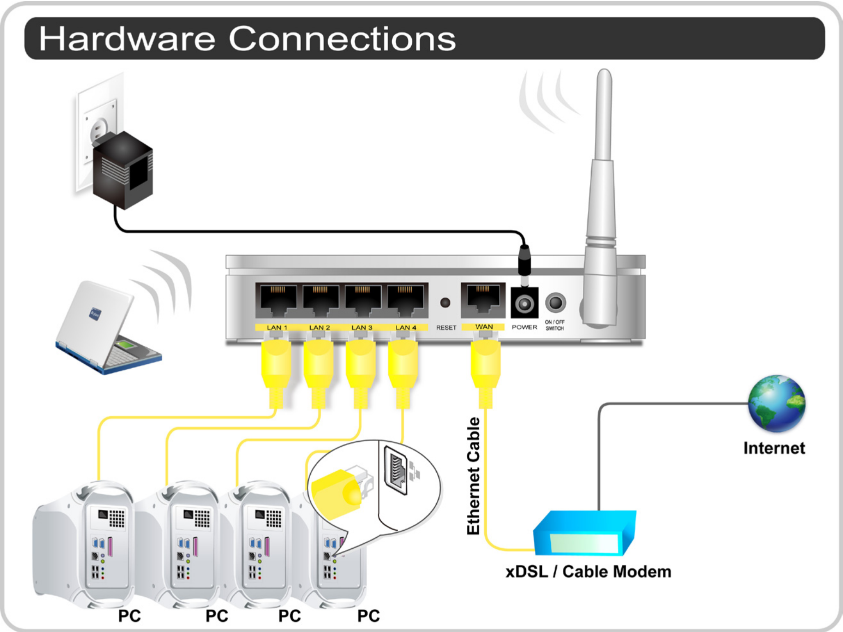
Connecting the Hardware

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 Wireless Gateway.

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.



Overview of Hardware Connections

Step 1. Connect the Ethernet cable to WAN Port

Plug one end of the RJ-45 Ethernet cable into the WAN port and plug the other end into the Ethernet port of the Internet service device, such as the cable modem or xDSL modem. Then connect the cable modem or xDSL modem to the modem port of the splitter using a RJ-11 telephone line.

Step 2. Connect the Ethernet cable to LAN Port

Connect either a LAN hub or a single Ethernet computer directly to the device via Ethernet cable(s).
Note that the cables do not need to be crossover cables.

Step 3. Attach the power connector

Connect the power adapter to the Power connector on the back of the device and plug the adapter into a wall outlet or power strip. Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

Step 4. Configure your Ethernet PCs

You must also configure the Internet properties on your Ethernet PCs. See Configuring Ethernet PCs.

Step 5. Install a Wireless card and connect Wireless PCs

You can attach a Wireless LAN that enables Wireless PCs to access the Internet via your device.
You must configure your Wireless computer(s) in order to access your device. For complete instructions, see Configuring Wireless PCs.

Next step

After setting up and configuring the device and PCs, you can log on to the device by following the instructions in Getting Started with the Web pages. The chapter includes a section called Testing your Setup, which enables you to verify that the device is working properly.

Easy Setup

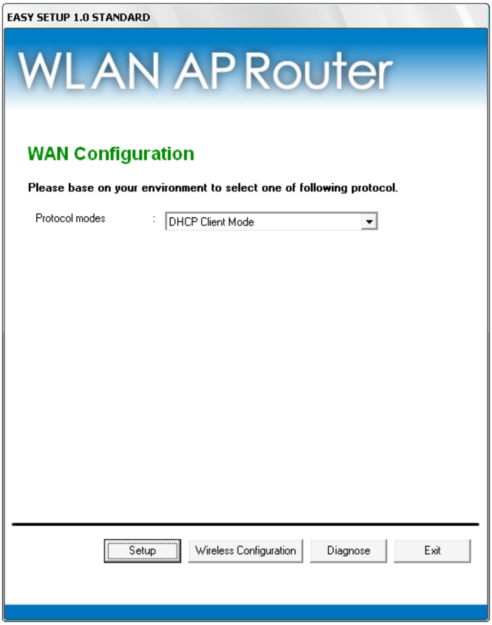
For easy configuration, insert the CD into your CD-ROM drive.
The CD should auto-start and then click "Easy Configuration". If it does not start, click on Start -> Run and type in CD:\fscommand\vbpES.exe (where CD is the drive letter of your CD-ROM drive.)

WAN Configuration:

There are Three options of Protocol Modes on WAN Configuration: DHCP Client, PPPoE Client and Fixed IP Mode.

DHCP Client

The default Internet access is: DHCP Client Mode
From the Protocol modes drop-down list, select DHCP Client Mode setting.
Click Setup, it will start to configure the router for a while. Follow the instructions of the Easy Setup utility which will guide you to complete the configuration.



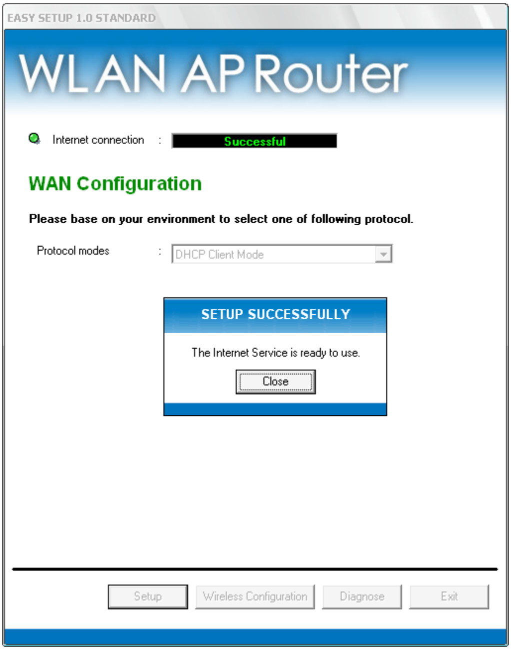
WAN Configuration

Please base on your environment to select one of following protocol.

Protocol modes : DHCP Client Mode

Easy setup configuration completed.

Now you are ready to Surf the Internet!!!



Internet connection : Successful

WAN Configuration

Please base on your environment to select one of following protocol.

Protocol modes : DHCP Client Mode

SETUP SUCCESSFULLY

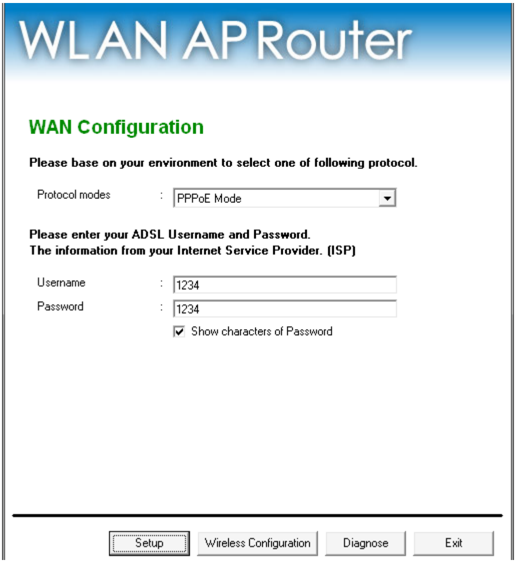
The Internet Service is ready to use.

PPPoE Client

From the Protocol modes drop-down list, select PPPoE Client Mode setting.

Enter PPPoE Username and Password.

Click Setup, it will start to configure the router for a while. Follow the instructions of the Easy Setup utility which will guide you to complete the configuration.



WLAN AP Router

WAN Configuration

Please base on your environment to select one of following protocol.

Protocol modes : PPPoE Mode

Please enter your ADSL Username and Password.
The information from your Internet Service Provider. (ISP)

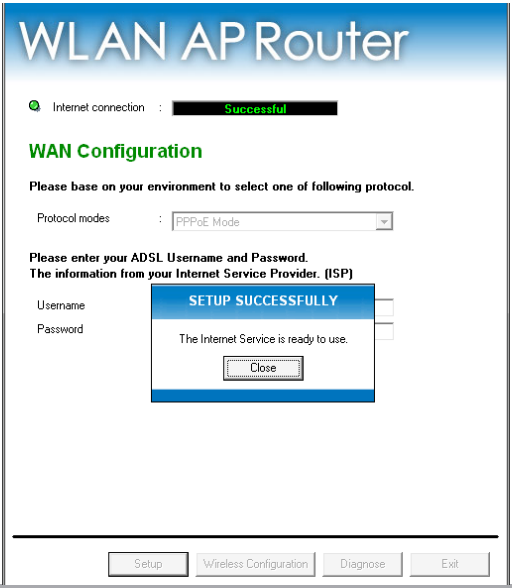
Username : 1234

Password : 1234

☑ Show characters of Password

Easy setup configuration completed.

Now you are ready to Surf the Internet!!!



WLAN AP Router

Internet connection : Successful

WAN Configuration

Please base on your environment to select one of following protocol.

Protocol modes : PPPoE Mode

Please enter your ADSL Username and Password.
The information from your Internet Service Provider. (ISP)

Username

Password

SETUP SUCCESSFULLY

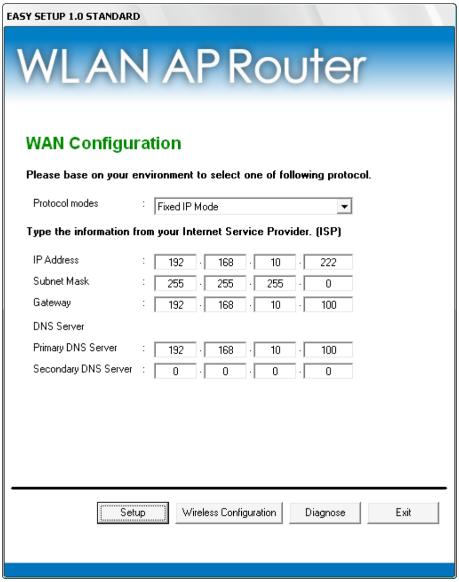
The Internet Service is ready to use.

Fixed IP

From the Protocol modes drop-down list, select Fixed IP Mode setting.

Enter IP Address, Subnet Mask, Gateway, Primary DNS Server and Secondary DNS Server.

Click Setup, it will start to configure the router for a while. Follow the instructions of the Easy Setup utility which will guide you to complete the configuration.



EASY SETUP 1.0 STANDARD

WLAN AP Router

WAN Configuration

Please base on your environment to select one of following protocol.

Protocol modes : Fixed IP Mode

Type the information from your Internet Service Provider. (ISP)

IP Address : 192 . 168 . 10 . 222

Subnet Mask : 255 . 255 . 255 . 0

Gateway : 192 . 168 . 10 . 100

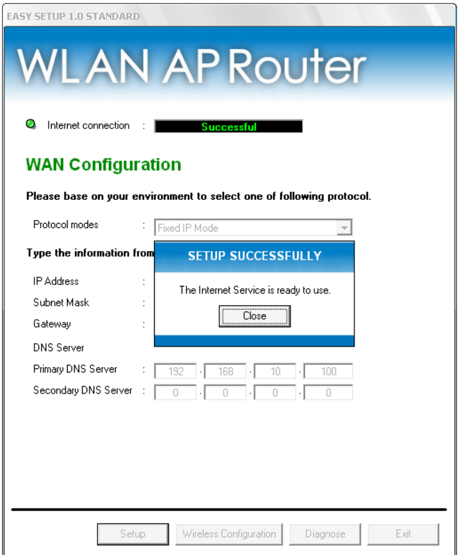
DNS Server

Primary DNS Server : 192 . 168 . 10 . 100

Secondary DNS Server : 0 . 0 . 0 . 0

Easy setup configuration completed.

Now you are ready to Surf the Internet!!!



EASY SETUP 1.0 STANDARD

WLAN AP Router

Internet connection : Successful

WAN Configuration

Please base on your environment to select one of following protocol.

Protocol modes : Fixed IP Mode

Type the information from

IP Address :

Subnet Mask :

Gateway :

DNS Server

Primary DNS Server : 192 . 168 . 10 . 100

Secondary DNS Server : 0 . 0 . 0 . 0

SETUP SUCCESSFULLY

The Internet Service is ready to use.

Getting Started with the Web pages

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

Accessing the Web pages

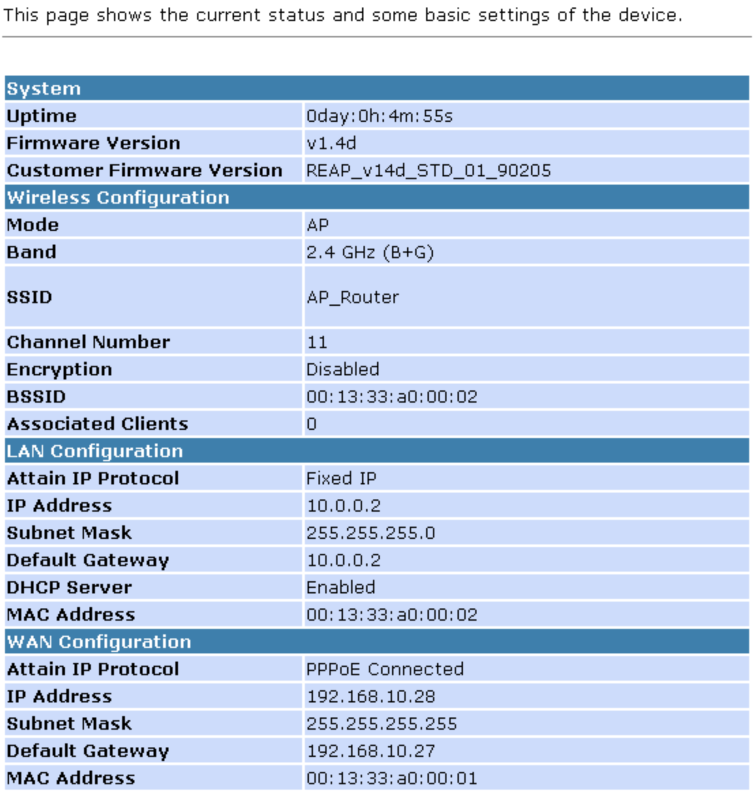
To access the Web pages, you need the following:

A PC or laptop connected to the LAN port on the device.

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

http://10.0.0.2

The Status homepage for the web pages is displayed:



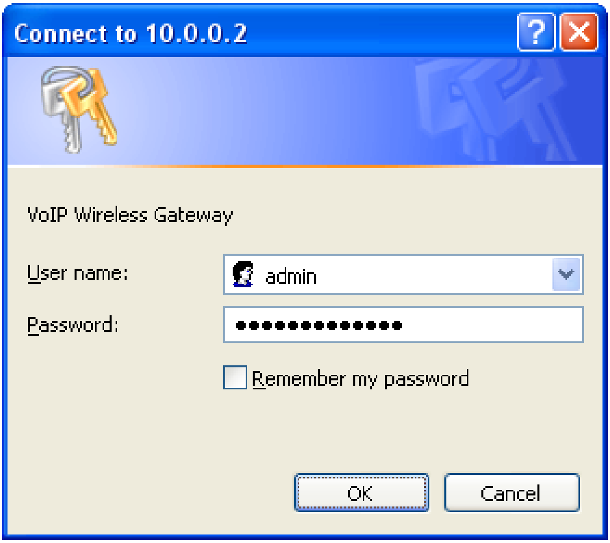
This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:4m:55s
Firmware Version	v1.4d
Customer Firmware Version	REAP_v14d_STD_01_90205
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	AP_Router
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:a0:00:02
Associated Clients	0
LAN 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	00:13:33:a0:00:02
WAN Configuration	
Attain IP Protocol	PPPoE Connected
IP Address	192.168.10.28
Subnet Mask	255.255.255.255
Default Gateway	192.168.10.27
MAC Address	00:13:33:a0:00:01

Homepage

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

A login screen is displayed:



Connect to 10.0.0.2

VoIP Wireless Gateway

User name: admin

Password: ●●●●●●●●●●●●●●

□ Remember my password

Login screen

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

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

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.

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	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. 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 Wireless Gateway can provide a variety of services to your network. The device is preconfigured with default settings for use with a typical home or small office network.

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

⚠ WARNING

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

Option	Default Setting	Explanation/Instructions
WAN Port IP Address	DHCP Client	This is the temporary public IP address of the WAN port on the device. It is an unnumbered interface that is replaced as soon as your ISP assigns a 'real' IP address. See Network Settings -> WAN Interface.
LAN Port IP Address	Assigned static IP address: 10.0.0.2 Subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See Network Settings -> LAN Interface.
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 10.0.0.100 through 10.0.0.200	The Wireless Gateway 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.

Quick Setup

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

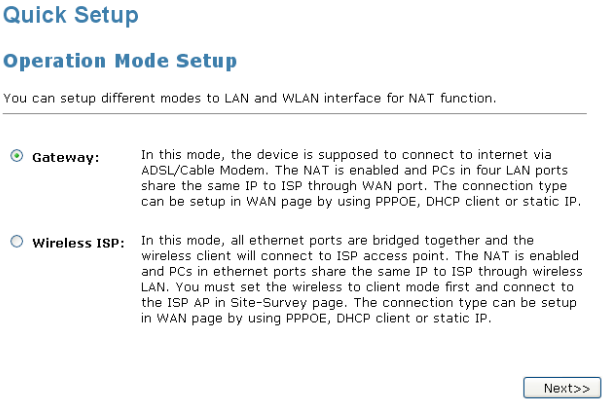
details of the device's Internet access settings

details of the device's VoIP settings

details of the device's Wireless settings

To display this page:

From the left-hand menu, click on Quick Setup. The following page is displayed:



Quick Setup

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 or static IP.

○ **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.

Quick Setup page

Operation Mode Setup

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

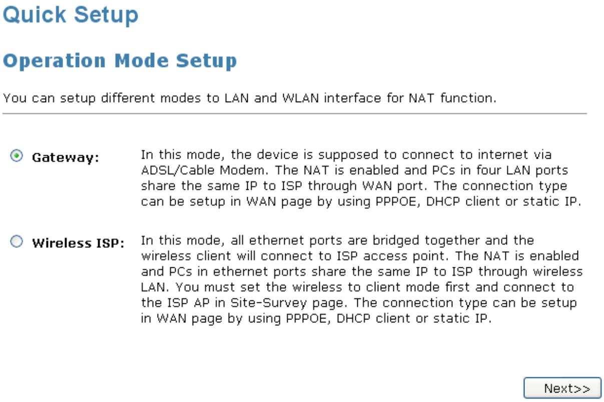
Gateway

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 or static IP.

To change the Operation Mode:

From the left-hand menu, click on Quick Setup. The following page is displayed:

Click on the ratio of Gateway and then click on Next>>.



Quick Setup

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 or static IP.

○ 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.

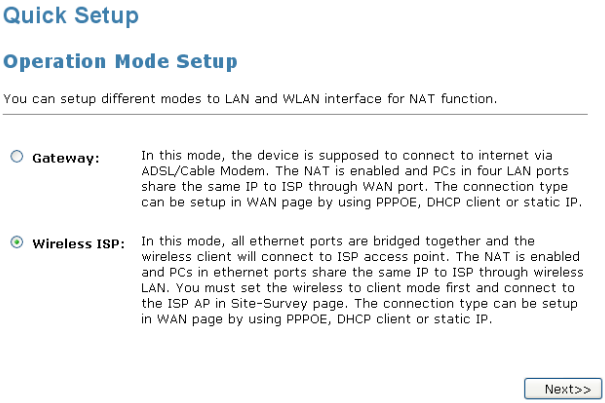
Wireless ISP

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:

From the left-hand menu, click on Quick Setup. The following page is displayed:

Click on the ratio of Wireless ISP and then click on Next>>.



Quick Setup

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 or static IP.

● 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.

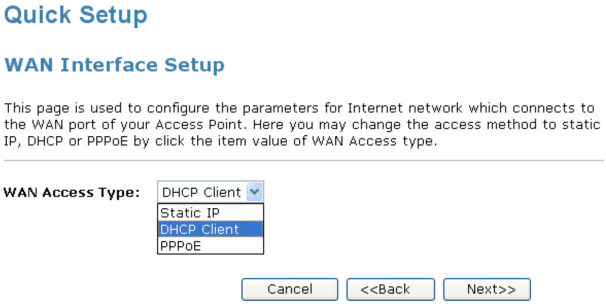
WAN Interface Setup

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, or PPPoE by click the item value of WAN Access type.

To change the WAN Access Type:

From the WAN Access Type drop-down list, select Static IP, DHCP Client, or PPPoE setting determined by your Network Administrator or ISP.

Click Next>>.



Quick Setup

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 or PPPoE by click the item value of WAN Access type.

WAN Access Type: DHCP Client

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.

From the WAN Access Type drop-down list, select Static IP setting determined by your Network Administrator or ISP.

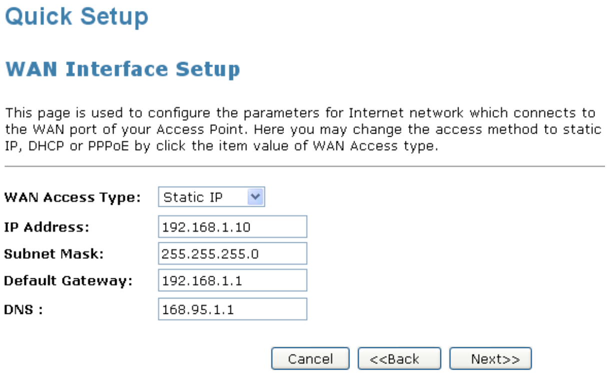
Enter IP Address for example 192.168.1.10.

Enter Subnet Mask for example 255.255.255.0.

Enter Default Gateway for example 192.168.1.1.

Enter DNS for example 168.95.1.1.

Click Next>>.



Quick Setup

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 or PPPoE by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

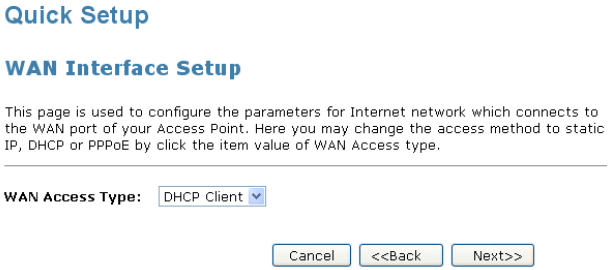
DNS : 168.95.1.1

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 static IP.

From the WAN Access Type drop-down list, select DHCP Client setting determined by your Network Administrator or ISP.

Click Next>>.



Quick Setup

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 or PPPoE by click the item value of WAN Access type.

WAN Access Type: DHCP Client

PPPoE

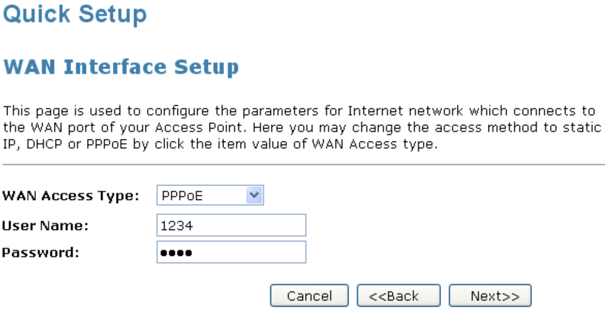
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using static IP.

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

Enter User Name for example 1234.

Enter Password for example 1234.

Click Next>>.



Quick Setup

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 or PPPoE by click the item value of WAN Access type.

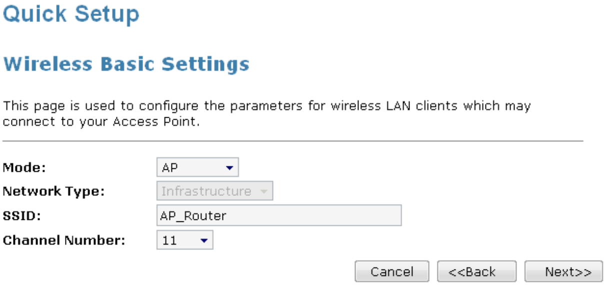
WAN Access Type: PPPoE

User Name: 1234

Password: ●●●●

Wireless Basic Setup

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



Quick Setup

Wireless Basic Settings

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

Mode: AP

Network Type: Infrastructure

SSID: AP_Router

Channel Number: 11

AP (Access Point)

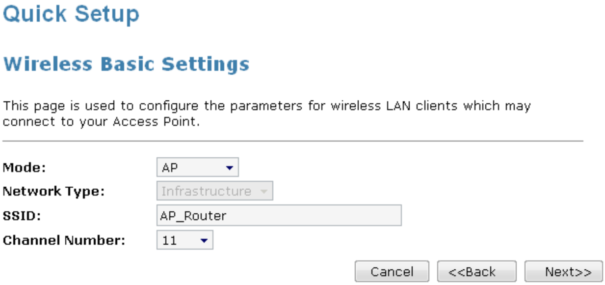
Access Point is used to configure the parameters for wireless LAN clients who may connect to your Access Point.

From the Mode drop-down list, select AP setting.

Enter SSID for example AP_Router.

From the Channel Number drop-down list, select a Channel.

Click Next>>.



Quick Setup

Wireless Basic Settings

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

Mode: AP

Network Type: Infrastructure

SSID: AP_Router

Channel Number: 11

WDS (Wireless Distribution System)

WDS stands for Wireless Distribution System. It enables the access points (APs) to be connected wirelessly. Integrated Access Device can also provide you services of WDS.

Note

Integrated Access Device 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 the network. Your exact steps (and the verbiage used) will vary from vendor to vendor. Generally, you'll see some settings like the following:

Main WDS station:

One of your WDS stations is the main base station for the WDS network. This AP is connected directly to your Internet connection, or connected to your router via a wired connection. The main station is the bridge to your Internet connection that all wireless traffic eventually 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 main base station and relays the data to the wireless clients associated to the repeater station (and vice versa for data coming from the clients). If you have more than two APs, remote APs may be repeaters, or they may be relays that provide an intermediate stopping point for data if the repeater is too far away from the main station to communicate.

When you configure your main or base WDS station, take note of the channel you're set to and the ESSID or network name of your network. If your AP has any kind of channel auto configuration function that changes channels based on network conditions, be sure to disable this feature. If your main WDS station is also your network's router, make sure it's set up to distribute IP addresses 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 Base Station — that's the wording Apple uses for their AirPort Extreme products). When you turn on this functionality, the configuration software may ask you to identify the remote repeater(s). Have the MAC addresses of those repeaters handy in case you need them.

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

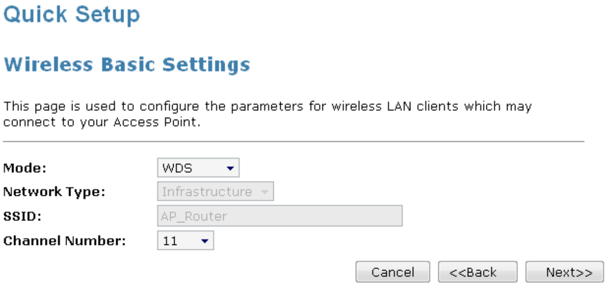
- You need to assign any other WDS stations to the same channel that your main base station is using. This is counterintuitive to many folks who have had the 802.11b/g "use channels 1, 6, and 11 and keep your APs on different channels" mantra driven into their heads for a long time!
- You set the ESSID of the remote location(s) using either a unique name or by using the same ESSID as you use for your main base station. (Whoa, our heads just exploded!) Using the same ESSID (a "roaming" network) is pretty cool. You associate with one AP one time and then your PC or Mac can associate with any AP on your WDS network without you having to do anything — it's more seamless this way. But remember, you don't have to do this — you can give each AP a unique ESSID and just configure your computer to associate with them according to your preference.
- Make sure you turn off any routing or DHCP functionality in the remote repeater stations. All of this functionality should be performed in the main base station or the network's main router.

WDS (Wireless Distribution System) only

From the Mode drop-down list, select WDS setting.

From the Channel Number drop-down list, select a Channel.

Click Next>>.



Quick Setup

Wireless Basic Settings

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

Mode:	WDS
Network Type:	Infrastructure
SSID:	AP_Router
Channel Number:	11

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

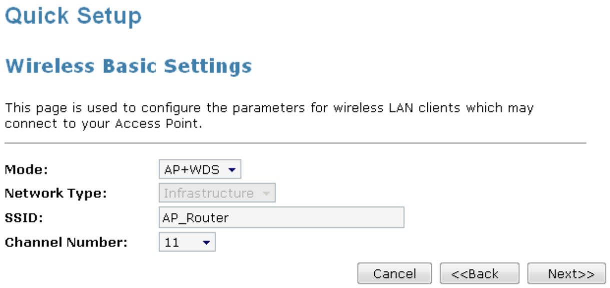
Access Point is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

From the Mode drop-down list, select AP+WDS setting.

Enter SSID for example VoIP_Wireless.

From the Channel Number drop-down list, select a Channel.

Click Next>>.



Quick Setup

Wireless Basic Settings

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

Mode: AP+WDS

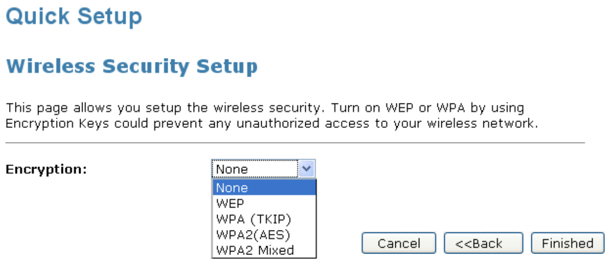
Network Type: Infrastructure

SSID: AP_Router

Channel Number: 11

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.



Quick Setup

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.

Encryption: None

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 WEP 64bit 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 WPA1 - Wi-Fi Protected Access 1 (TKIP) Passphrase encryption, follow the instructions in Configuring WPA (TKIP) Passphrase security.
- If you want to use WPA1 - Wi-Fi Protected Access 1 (TKIP) HEX (64 characters) encryption, follow the instructions in Configuring WPA (TKIP) HEX (64 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 WPA2 Mixed- Wi-Fi Protected Access 2 (Mixed) Passphrase encryption, follow the instructions in Configuring WPA2 (Mixed) Passphrase security.
- If you want to use WPA2 Mixed- Wi-Fi Protected Access 2 (Mixed) HEX (64 characters) encryption, follow the instructions in Configuring WPA2 (Mixed) HEX (64 characters) security.

Configuring WEP 64bit ASCII (5 characters) security

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

From the Encryption drop-down list, select WEP setting.

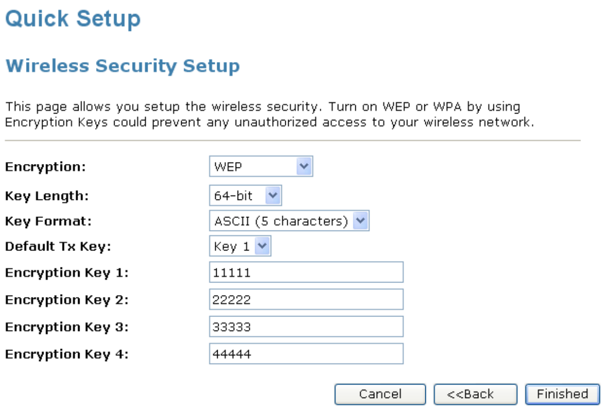
From the Key Length drop-down list, select 64-bit setting.

From the Key Format drop-down list, select ASCII (5 characters) setting.

From the Default Tx Key drop-down list, select Key 1, Key 2, Key 3 or Key 4 setting.

Type the Default Tx Key to Key 1, Key 2, Key 3, or Key 4. The Default Tx Key is realated to Encryption Key 1, Encryption Key 2, Encryption Key 3 and Encryption Key 4.

Click Finished.



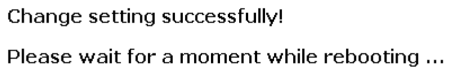
Quick Setup

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.

Encryption:	WEP
Key Length:	64-bit
Key Format:	ASCII (5 characters)
Default Tx Key:	Key 1
Encryption Key 1:	11111
Encryption Key 2:	22222
Encryption Key 3:	33333
Encryption Key 4:	44444

Change setting successfully! Please wait for a moment while rebooting.



Change setting successfully!

Please wait for a moment while rebooting ...

Configuring WEP 64bit Hex (10 characters) security

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

From the Encryption drop-down list, select WEP setting.

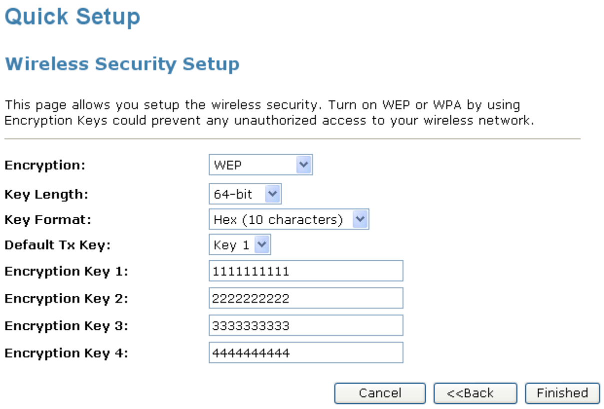
From the Key Length drop-down list, select 64-bit setting.

From the Key Format drop-down list, select Hex (10 characters) setting.

From the Default Tx Key drop-down list, select Key 1, Key 2, Key 3 or Key 4 setting.

Type the Default Tx Key to Key 1, Key 2, Key 3, or Key 4. The Default Tx Key is realated to Encryption Key 1, Encryption Key 2, Encryption Key 3 and Encryption Key 4.

Click Finished.



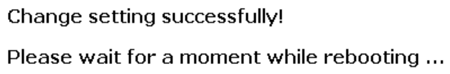
Quick Setup

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.

Encryption:	WEP
Key Length:	64-bit
Key Format:	Hex (10 characters)
Default Tx Key:	Key 1
Encryption Key 1:	1111111111
Encryption Key 2:	2222222222
Encryption Key 3:	3333333333
Encryption Key 4:	4444444444

Change setting successfully! Please wait for a moment while rebooting.



Change setting successfully!

Please wait for a moment while rebooting ...

Configuring WEP 128bit ASCII (13 characters) security

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

From the Encryption drop-down list, select WEP setting.

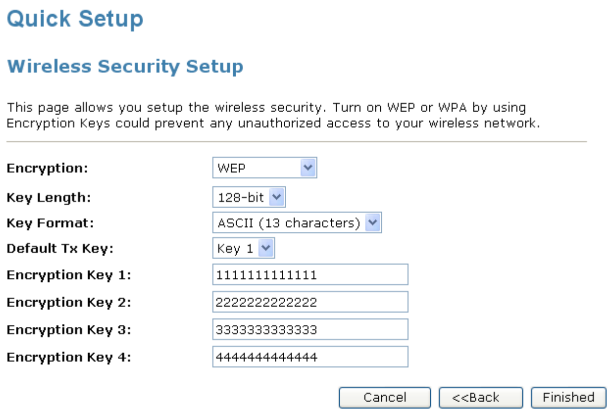
From the Key Length drop-down list, select 128-bit setting.

From the Key Format drop-down list, select ASCII (13 characters) setting.

From the Default Tx Key drop-down list, select Key 1, Key 2, Key 3 or Key 4 setting.

Type the Default Tx Key to Key 1, Key 2, Key 3, or Key 4. The Default Tx Key is realated to Encryption Key 1, Encryption Key 2, Encryption Key 3 and Encryption Key 4.

Click Finished.



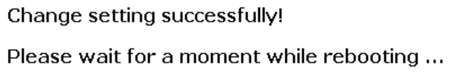
Quick Setup

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.

Encryption:	WEP
Key Length:	128-bit
Key Format:	ASCII (13 characters)
Default Tx Key:	Key 1
Encryption Key 1:	1111111111111
Encryption Key 2:	2222222222222
Encryption Key 3:	3333333333333
Encryption Key 4:	4444444444444

Change setting successfully! Please wait for a moment while rebooting.



Change setting successfully!

Please wait for a moment while rebooting ...

Configuring WEP 128bit Hex (26 characters) security

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

From the Encryption drop-down list, select WEP setting.

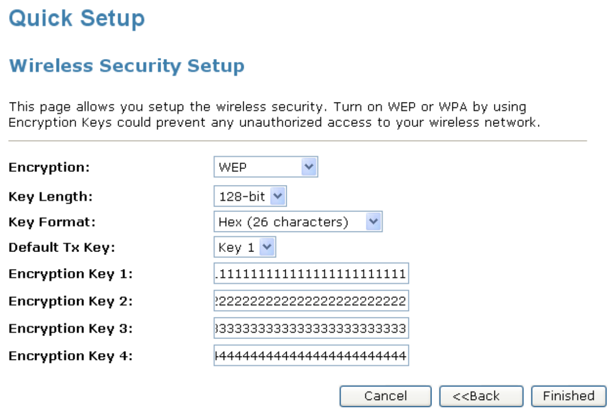
From the Key Length drop-down list, select 128-bit setting.

From the Key Format drop-down list, select Hex (26 characters) setting.

From the Default Tx Key drop-down list, select Key 1, Key 2, Key 3 or Key 4 setting.

Type the Default Tx Key to Key 1, Key 2, Key 3, or Key 4. The Default Tx Key is realated to Encryption Key 1, Encryption Key 2, Encryption Key 3 and Encryption Key 4.

Click Finished.



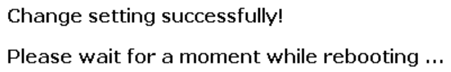
Quick Setup

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.

Encryption:	WEP
Key Length:	128-bit
Key Format:	Hex (26 characters)
Default Tx Key:	Key 1
Encryption Key 1:	.1111111111111111111111111
Encryption Key 2:	2222222222222222222222222
Encryption Key 3:	3333333333333333333333333
Encryption Key 4:	4444444444444444444444444

Change setting successfully! Please wait for a moment while rebooting.



Change setting successfully!

Please wait for a moment while rebooting ...

Configuring WPA (TKIP) Passphrase security

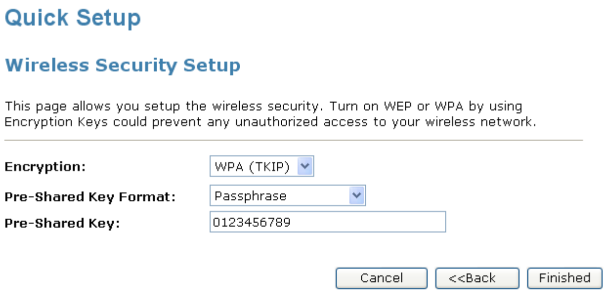
The example set in this section is for WPA (TKIP) Passphrase encryption.

From the Encryption drop-down list, select WPA (TKIP) setting.

From the Pre-Shared Key Format drop-down list, select Passphrase setting.

Type the Pre-Shared Key.

Click Finished.



Quick Setup

Wireless Security Setup

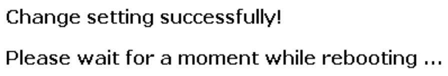
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA (TKIP)

Pre-Shared Key Format: Passphrase

Pre-Shared Key: 0123456789

Change setting successfully! Please wait for a moment while rebooting.



Change setting successfully!

Please wait for a moment while rebooting ...

Configuring WPA (TKIP) HEX (64 characters) security

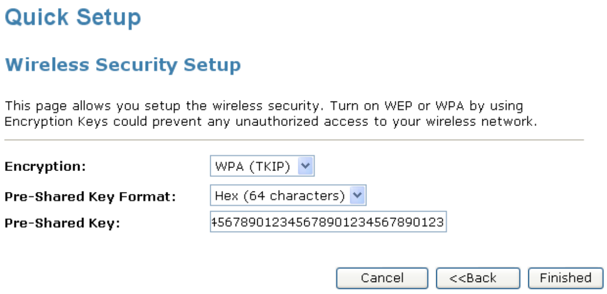
The example set in this section is for WPA (TKIP) HEX (64 characters) encryption.

From the Encryption drop-down list, select WPA (TKIP) setting.

From the Pre-Shared Key Format drop-down list, select HEX (64 characters) setting.

Type the Pre-Shared Key.

Click Finished.



Quick Setup

Wireless Security Setup

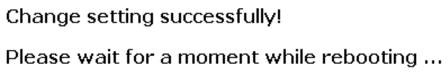
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA (TKIP)

Pre-Shared Key Format: Hex (64 characters)

Pre-Shared Key: 456789012345678901234567890123

Change setting successfully! Please wait for a moment while rebooting.



Change setting successfully!

Please wait for a moment while rebooting ...

Configuring WPA2 (AES) Passphrase security

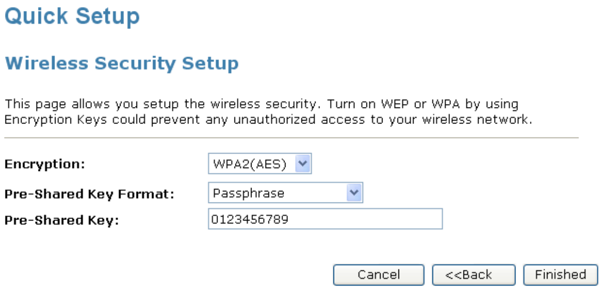
The example set in this section is for WPA2 (AES) Passphrase encryption.

From the Encryption drop-down list, select WPA2 (AES) setting.

From the Pre-Shared Key Format drop-down list, select Passphrase setting.

Type the Pre-Shared Key.

Click Finished.



Quick Setup

Wireless Security Setup

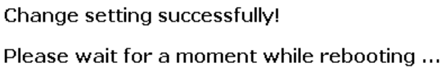
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA2(AES)

Pre-Shared Key Format: Passphrase

Pre-Shared Key: 0123456789

Change setting successfully! Please wait for a moment while rebooting.



Change setting successfully!

Please wait for a moment while rebooting ...

Configuring WPA2 (AES) HEX (64 characters) security

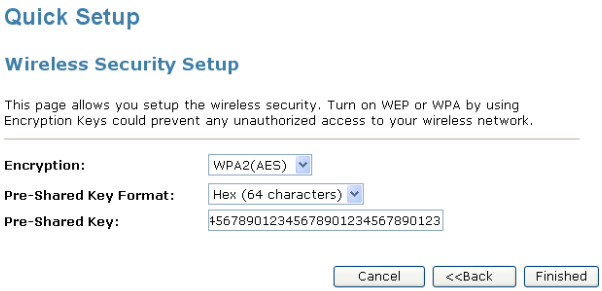
The example set in this section is for WPA2 (AES) HEX (64 characters) encryption.

From the Encryption drop-down list, select WPA2 (AES) setting.

From the Pre-Shared Key Format drop-down list, select HEX (64 characters) setting.

Type the Pre-Shared Key.

Click Finished.



Quick Setup

Wireless Security Setup

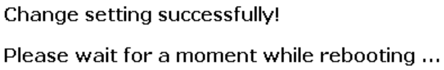
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA2(AES)

Pre-Shared Key Format: Hex (64 characters)

Pre-Shared Key: 456789012345678901234567890123

Change setting successfully! Please wait for a moment while rebooting.



Change setting successfully!

Please wait for a moment while rebooting ...

Configuring WPA2 (Mixed) Passphrase security

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

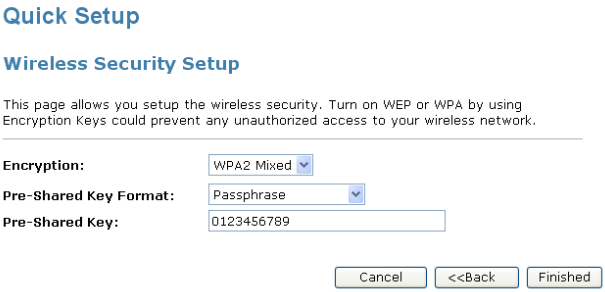
The WPA2 (Mixed) Passphrase encryption supports both WPA (TKIP) and WPA2 (AES).

From the Encryption drop-down list, select WPA2 (Mixed) setting.

From the Pre-Shared Key Format drop-down list, select Passphrase setting.

Type the Pre-Shared Key.

Click Finished.



Quick Setup

Wireless Security Setup

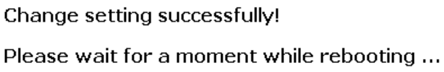
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA2 Mixed

Pre-Shared Key Format: Passphrase

Pre-Shared Key: 0123456789

Change setting successfully! Please wait for a moment while rebooting.



Change setting successfully!

Please wait for a moment while rebooting ...

Configuring WPA2 (Mixed) HEX (64 characters) security

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

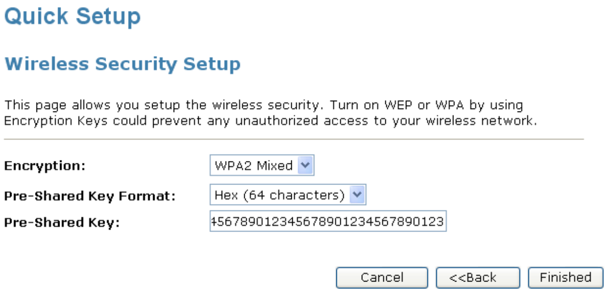
The WPA2 (Mixed) HEX (64 characters) encryption supports both WPA (TKIP) and WPA2 (AES).

From the Encryption drop-down list, select WPA2 (Mixed) setting.

From the Pre-Shared Key Format drop-down list, select HEX (64 characters) setting.

Type the Pre-Shared Key.

Click Finished.



Quick Setup

Wireless Security Setup

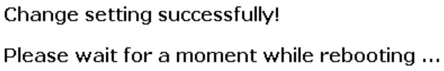
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA2 Mixed

Pre-Shared Key Format: Hex (64 characters)

Pre-Shared Key: 456789012345678901234567890123

Change setting successfully! Please wait for a moment while rebooting.



Change setting successfully!

Please wait for a moment while rebooting ...

Operation Mode

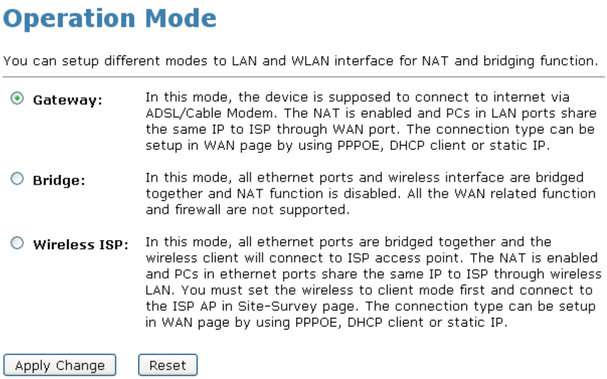
This chapter describes how to configure the way that your device connects to the Internet. There are Three options of Operation Mode: Gateway, Bridge and Wireless ISP.

Setting Operation Mode

To change the Operation Mode:

From the left-hand Operation Mode menu. The following page is displayed:

Click on the ratio of Gateway, Bridge or Wireless ISP and then click on Apply to active it.



Operation Mode

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

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

○ **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.

○ **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.

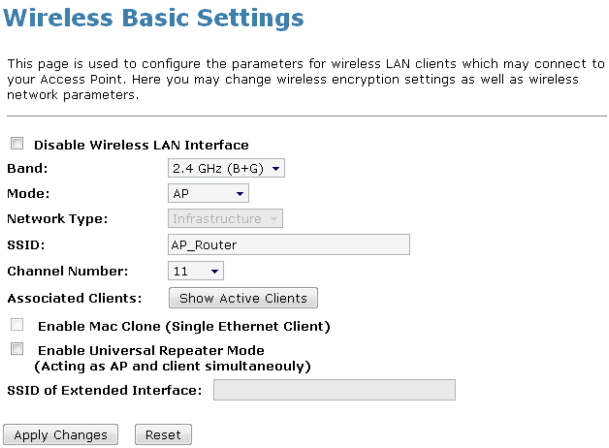
Wireless Network

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 Network Basic Settings page:

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



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ **Disable Wireless LAN Interface**

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: AP_Router

Channel Number: 11

Associated Clients: Show Active Clients

□ **Enable Mac Clone (Single Ethernet Client)**

□ **Enable Universal Repeater Mode (Acting as AP and client simultaneouly)**

SSID of Extended Interface:

Wireless Network page

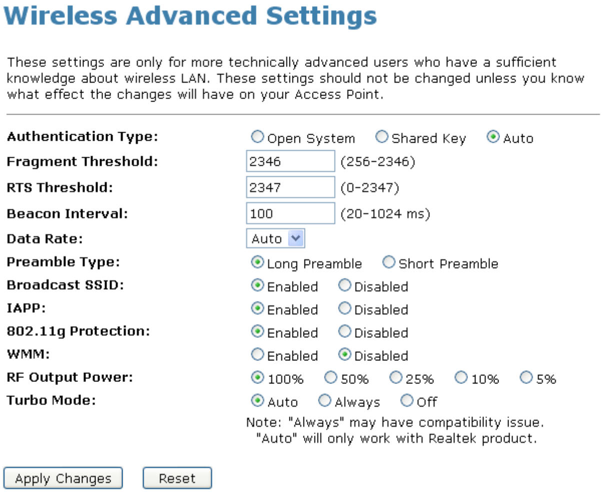
Field	Description
Disable Wireless LAN Interface	Enable/Disable the Wireless LAN Interface. Default: Disable
Band	Specify the WLAN Mode to 802.11b/g Mixed mode, 802.11b mode or 802.11g mode
Mode	Configure the Wireless LAN Interface to AP, Client, WDS or WDS + AP mode
Network Type	Configure the Network Type to Infrastructure or Ad hoc.

Field	Description
Disable Wireless LAN Interface	Enable/Disable the Wireless LAN Interface. Default: Disable
Band	Specify the WLAN Mode to 802.11b/g Mixed mode, 802.11b mode or 802.11g mode
Mode	Configure the Wireless LAN Interface to AP, Client, WDS or WDS + AP 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 Number	Choose a Channel Number from the pull-down menu.
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 Network Advanced Settings page:

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



Wireless 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.

Authentication Type: ○ Open System ○ Shared Key ● Auto

Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024 ms)

Data Rate: Auto

Preamble Type: ● Long Preamble ○ Short Preamble

Broadcast SSID: ● Enabled ○ Disabled

IAPP: ● Enabled ○ Disabled

802.11g Protection: ● Enabled ○ Disabled

WMM: ○ Enabled ● Disabled

RF Output Power: ● 100% ○ 50% ○ 25% ○ 10% ○ 5%

Turbo Mode: ● Auto ○ Always ○ Off

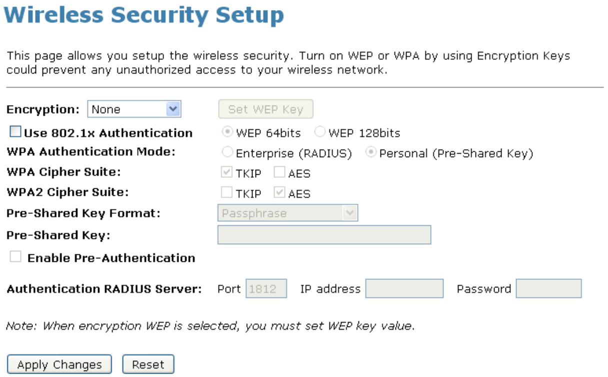
Note: "Always" may have compatibility issue.
"Auto" will only work with Realtek product.

Field	**Description**
Authentication Type	Configure the Authentication Type to Open System, Shared Key or Auto
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.
Data Rate	Select the Data Rate from the drop-down list
Preamble Type	Specify the Preamble type is short preamble or long preamble
Broadcast SSID	Broadcast or Hide SSID to your Network. Default: Enabled
IAPP	Disable or Enable IAPP
802.11g Protection	A protection mechanism prevents collisions among 802.11g nodes.
WMM	Enable/disable the Wi-Fi Multimedia (WMM) support.
RF Output Power	TX Power measurement.
Turbo Mode	Configure the Turbo Mode to Auto, Always or Off Note: „Always" may have compatibility issue. „Auto" will only work with Realtek product.

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 Network Security page:

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



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.

Encryption: None | Set WEP Key

□ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

Note: When encryption WEP is selected, you must set WEP key value.

Field	Description
Encryption	Configure the Encryption to None, WEP, WPA , WPA2 or WPA Mixed
Set WEP Key	Configure the WEP Key
Use 802.1x Authentication	Use 802.1x Authentication by WEP 64bits or WEP 128bits
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 TKIP and/or AES
WPA2 Cipher Suite	Configure the WPA2 Cipher Suite to TKIP and/or AES
Pre-Shared Key Format	Configure the Pre-Shared Key Format to Passphrase or HEX (64 characters)

Field	Description
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

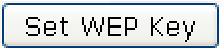
WEP + Encryption Key

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.

From the Encryption drop-down list, select WEP setting.

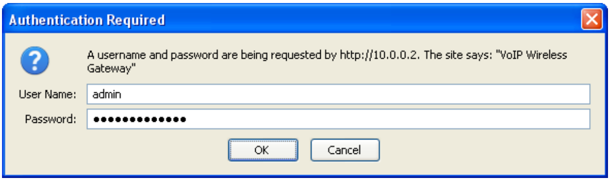
Encryption: WEP

Click Set WEP Key button.



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

User Name:	admin
Password:	administrator


Authentication Required

A username and password are being requested by http://10.0.0.2. The site says: "VoIP Wireless Gateway"

User Name: admin

Password: ••••••••••••••

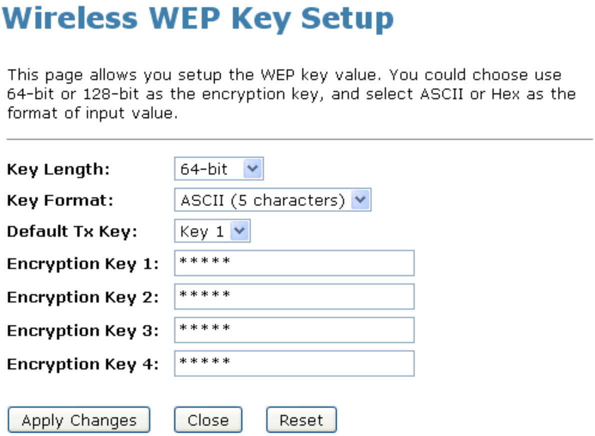
From the Key Length drop-down list, select 64-bit or 128-bit setting.

From the Key Format drop-down list, select ASCII (5 characters), Hex (10 characters), ASCII (13 characters) or Hex (26 characters) setting.

From the Default Tx Key drop-down list, select a key is used for encryption.

Enter the Encryption Key value depending on selected ASCII or Hexadecimal.

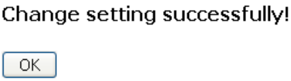
Click Apply Changes button.


Wireless WEP Key Setup

This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

Key Length:	64-bit
Key Format:	ASCII (5 characters)
Default Tx Key:	Key 1
Encryption Key 1:	*****
Encryption Key 2:	*****
Encryption Key 3:	*****
Encryption Key 4:	*****

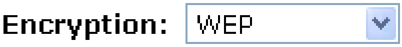
Change setting successfully! Click on OK button to confirm and return.


Change setting successfully!

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.

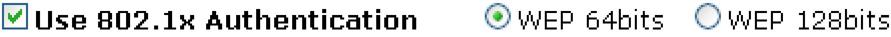
From the Encryption drop-down list, select WEP setting.



Encryption: WEP

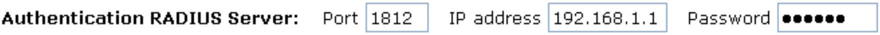
Check the option of Use 802.1x Authentication.

Click on the ratio of WEP 64bits or WEP 128bits.



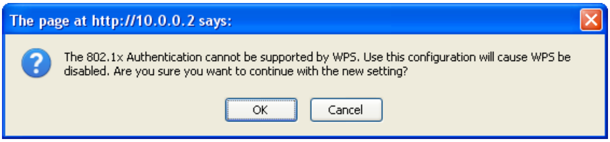
☑ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

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



Authentication RADIUS Server: Port 1812 IP address 192.168.1.1 Password ●●●●●●

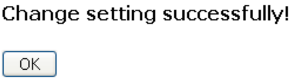
Click OK button.



The page at http://10.0.0.2 says:

The 802.1x Authentication cannot be supported by WPS. Use this configuration will cause WPS be disabled. Are you sure you want to continue with the new setting?

Change setting successfully! Click on OK button to confirm and return.



Change setting successfully!

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

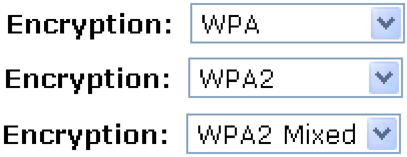
Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless (Wi-Fi)

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.

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

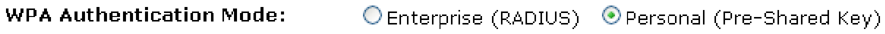


Encryption: WPA

Encryption: WPA2

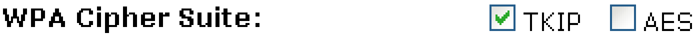
Encryption: WPA2 Mixed

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



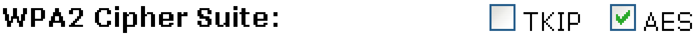
WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

Check the option of TKIP and/or AES in WPA Cipher Suite if your Encryption is WPA:



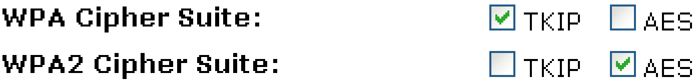
WPA Cipher Suite: ☑ TKIP □ AES

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



WPA2 Cipher Suite: □ TKIP ☑ AES

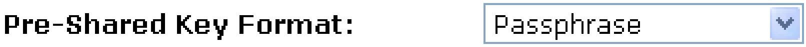
Check the option of TKIP and/or AES in WPA/WPA2 Cipher Suite if your Encryption is WPA2 Mixed:



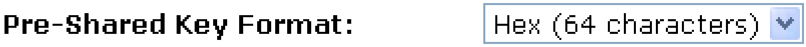
WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP ☑ AES

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

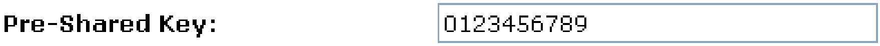


Pre-Shared Key Format: Passphrase



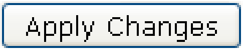
Pre-Shared Key Format: Hex (64 characters)

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

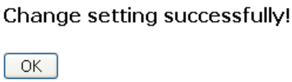


Pre-Shared Key: 0123456789

Click on Apply Changes button to confirm and return.



Change setting successfully! Click on OK button to confirm and return.



Change setting successfully!

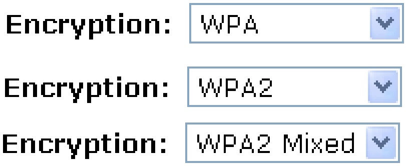
WPA/WPA2/WPA2 Mixed + Enterprise (RADIUS)

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.

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

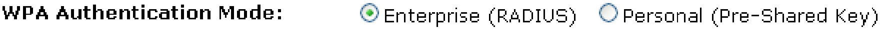


Encryption: WPA

Encryption: WPA2

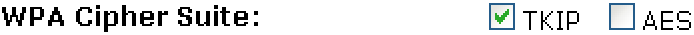
Encryption: WPA2 Mixed

Click on the ratio of Enterprise (RADIUS).



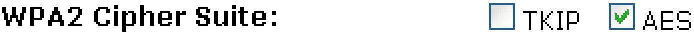
WPA Authentication Mode: ● Enterprise (RADIUS) ○ Personal (Pre-Shared Key)

Check the option of TKIP and/or AES in WPA Cipher Suite if your Encryption is WPA:



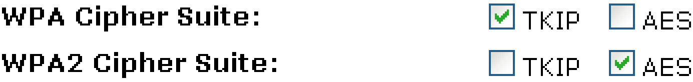
WPA Cipher Suite: ☑ TKIP □ AES

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



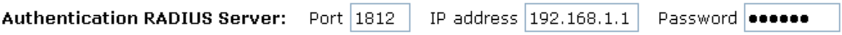
WPA2 Cipher Suite: □ TKIP ☑ AES

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



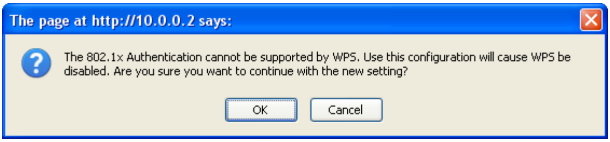
WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP ☑ AES



Authentication RADIUS Server: Port 1812 IP address 192.168.1.1 Password ●●●●●●

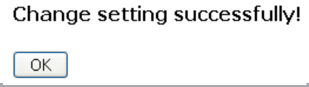
Click OK button.



The page at http://10.0.0.2 says:

The 802.1x Authentication cannot be supported by WPS. Use this configuration will cause WPS be disabled. Are you sure you want to continue with the new setting?

Change setting successfully! Click on OK button to confirm and return.



Change setting successfully!

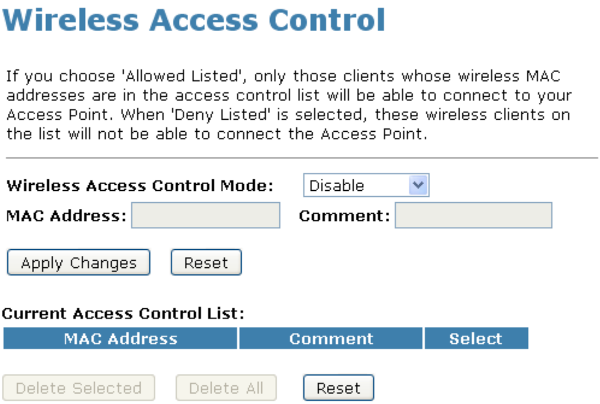
Access Control

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 Network Access Control page:

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



Wireless Access Control

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.

Wireless Access Control Mode: Disable

MAC Address:

Comment:

Current Access Control List:

MAC Address	Comment	Select

Allow Listed

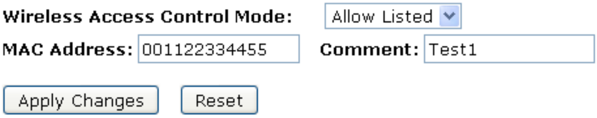
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point.

From the Wireless Access Control Mode drop-down list, select Allowed Listed setting.

Enter the MAC Address.

Enter the Comment.

Click Apply Changes button.

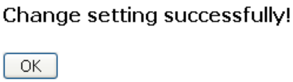


Wireless Access Control Mode: Allow Listed

MAC Address: 001122334455

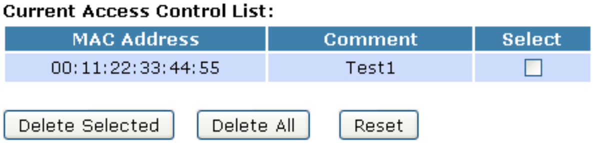
Comment: Test1

Change setting successfully! Click on OK button to confirm and return.



Change setting successfully!

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



Current Access Control List:

MAC Address	Comment	Select
00:11:22:33:44:55	Test1	□

Deny Listed

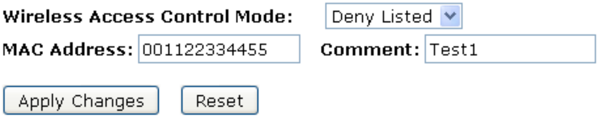
When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

From the Wireless Access Control Mode drop-down list, select Deny Listed setting.

Enter the MAC Address.

Enter the Comment.

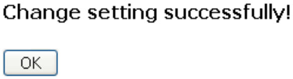
Click Apply Changes button.



Wireless Access Control Mode: Deny Listed

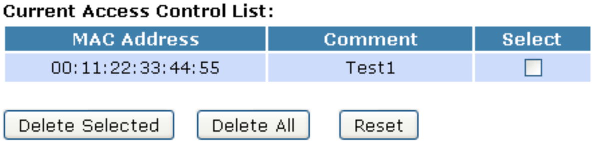
MAC Address: 001122334455 Comment: Test1

Change setting successfully! Click on OK button to confirm and return.



Change setting successfully!

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



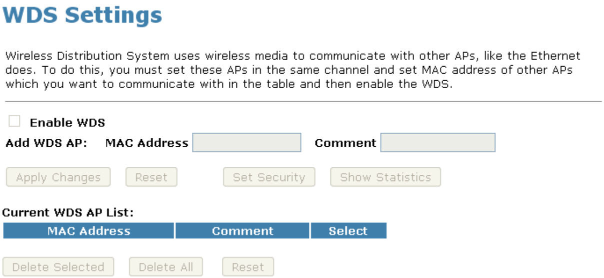
Current Access Control List:

MAC Address	Comment	Select
00:11:22:33:44:55	Test1	□

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 Network WDS settings page:

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



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.

□ Enable WDS

Add WDS AP: MAC Address Comment

Current WDS AP List:

MAC Address	Comment	Select

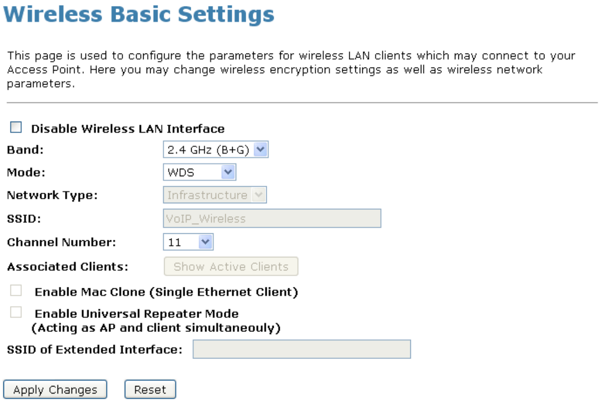
Configure WDS (Wireless Distribution System) only

From the left-hand Wireless menu, click on Basic Settings.

From the Mode drop-down list, select WDS.

From the Channel Number drop-down list, select a Channel.

Click Apply Changes button.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ **Disable Wireless LAN Interface**

Band: 2.4 GHz (B+G)

Mode: WDS

Network Type: Infrastructure

SSID: VoIP_Wireless

Channel Number: 11

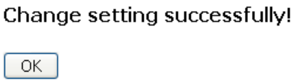
Associated Clients: Show Active Clients

☐ **Enable Mac Clone (Single Ethernet Client)**

☐ **Enable Universal Repeater Mode (Acting as AP and client simultaneouly)**

SSID of Extended Interface:

Change setting successfully! Click on OK button to confirm and return.



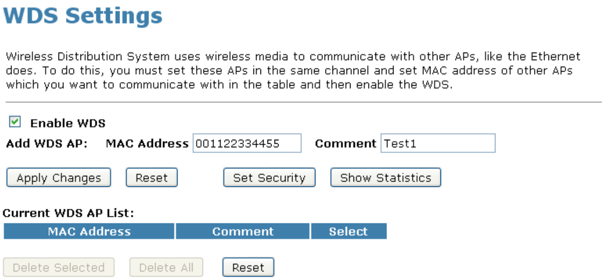
Change setting successfully!

From the left-hand Wireless menu, click on WDS settings.

Check on the option Enable WDS.

Enter the MAC Address.

Enter the Comment.



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.

☑ **Enable WDS**

Add WDS AP: **MAC Address** 001122334455 **Comment** Test1

Current WDS AP List:

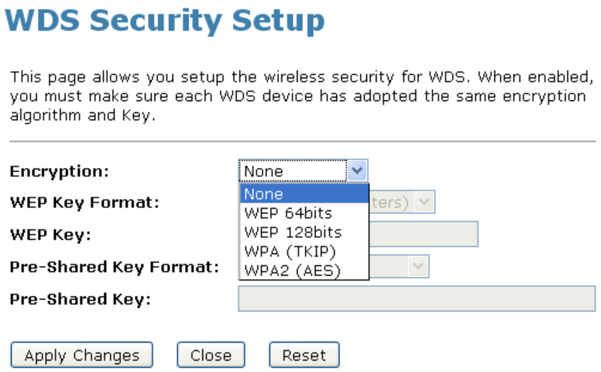
MAC Address	Comment	Select

Click the Set Security.

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.

Configure each field with the Encryption that you selected.

Click Apply Changes button.



WDS Security Setup

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.

Encryption: None

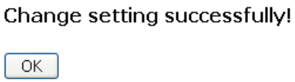
WEP Key Format:

WEP Key:

Pre-Shared Key Format:

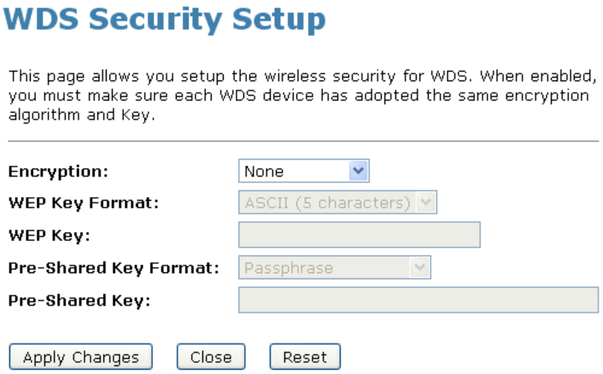
Pre-Shared Key:

Change setting successfully! Click on OK button to confirm and return.



Change setting successfully!

Click Close button to close and exit the WDS Security Setup.



WDS Security Setup

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.

Encryption: None

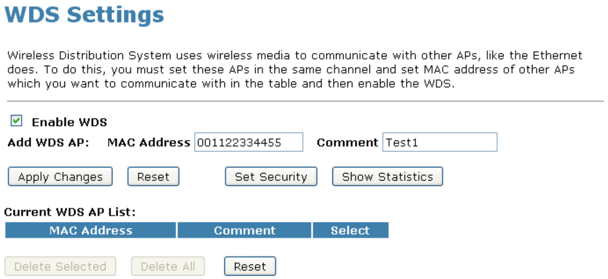
WEP Key Format: ASCII (5 characters)

WEP Key:

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Click Apply Changes button.



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.

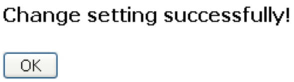
☑ Enable WDS

Add WDS AP: MAC Address 001122334455 Comment Test1

Current WDS AP List:

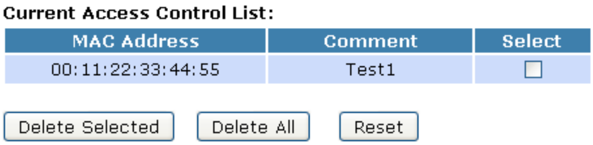
MAC Address	Comment	Select

Change setting successfully! Click on OK button to confirm and return.



Change setting successfully!

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



Current Access Control List:

MAC Address	Comment	Select
00:11:22:33:44:55	Test1	□

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

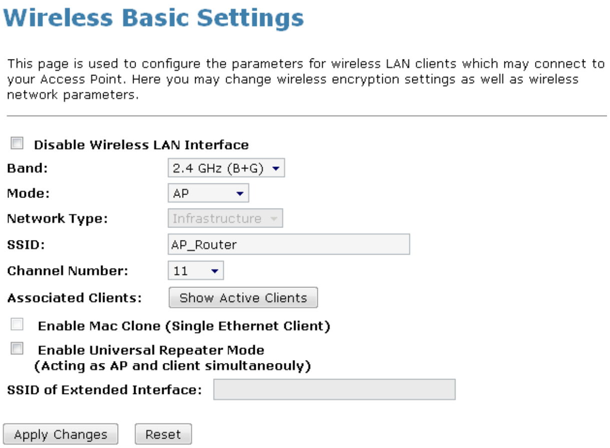
From the left-hand Wireless menu, click on Basic Settings.

From the Mode drop-down list, select AP+WDS.

Enter SSID for example AP_Router.

From the Channel Number drop-down list, select a Channel.

Click Apply Changes button.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: AP_Router

Channel Number: 11

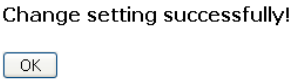
Associated Clients: Show Active Clients

□ Enable Mac Clone (Single Ethernet Client)

□ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

Change setting successfully! Click on OK button to confirm and return.



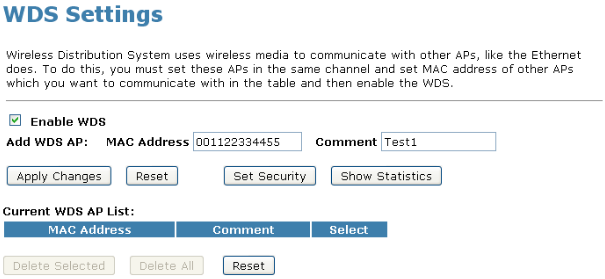
Change setting successfully!

From the left-hand Wireless menu, click on WDS settings.

Check on the option Enable WDS.

Enter the MAC Address.

Enter the Comment.



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.

☑ Enable WDS

Add WDS AP: MAC Address 001122334455 Comment Test1

Current WDS AP List:

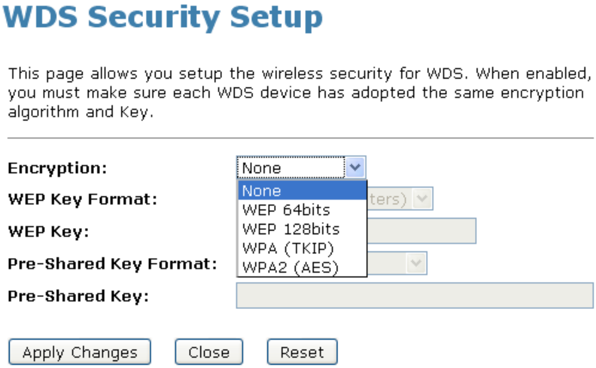
MAC Address	Comment	Select

Click the Set Security.

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.

Configure each field with the Encryption that you selected.

Click Apply Changes button.



WDS Security Setup

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.

Encryption: None

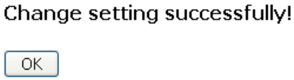
WEP Key Format:

WEP Key:

Pre-Shared Key Format:

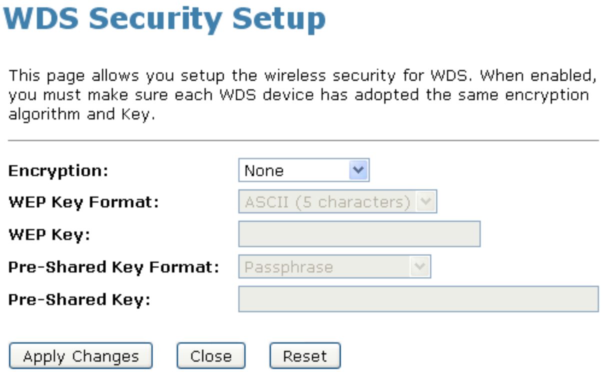
Pre-Shared Key:

Change setting successfully! Click on OK button to confirm and return.



Change setting successfully!

Click Close button to close and exit the WDS Security Setup.



WDS Security Setup

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.

Encryption: None

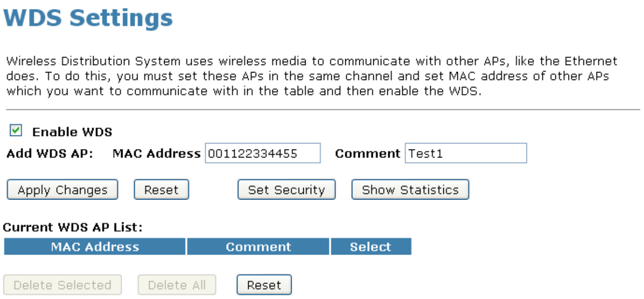
WEP Key Format: ASCII (5 characters)

WEP Key:

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Click Apply Changes button.



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.

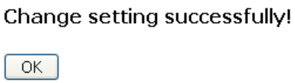
☑ Enable WDS

Add WDS AP: MAC Address 001122334455 Comment Test1

Current WDS AP List:

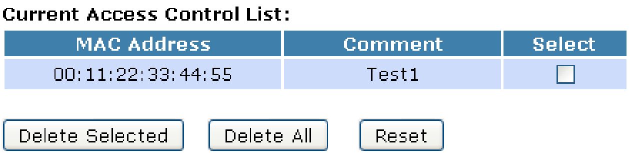
MAC Address	Comment	Select

Change setting successfully! Click on OK button to confirm and return.



Change setting successfully!

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



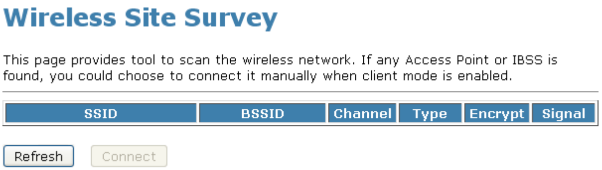
Current Access Control List:

MAC Address	Comment	Select
00:11:22:33:44:55	Test1	□

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 Network WDS settings page:

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



Wireless Site Survey

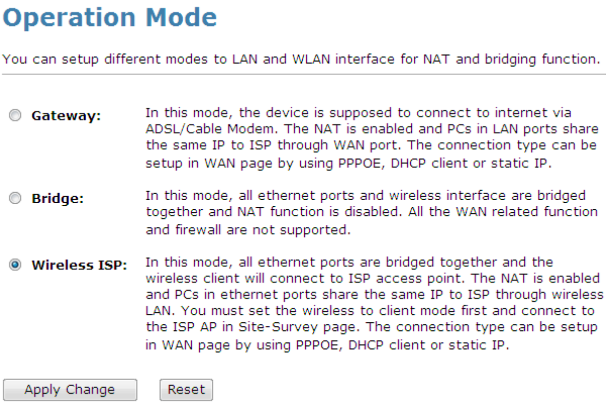
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal

Configure Wireless ISP + Wireless client + Site Survey

From the left-hand Operation Mode menu, click on Wireless ISP Settings.

Click Apply Changes button.



Operation Mode

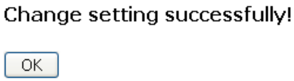
You can setup different modes to LAN and WLAN interface for NAT and bridging function.

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

○ **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.

● **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.

Change setting successfully! Click on OK button to confirm and return.



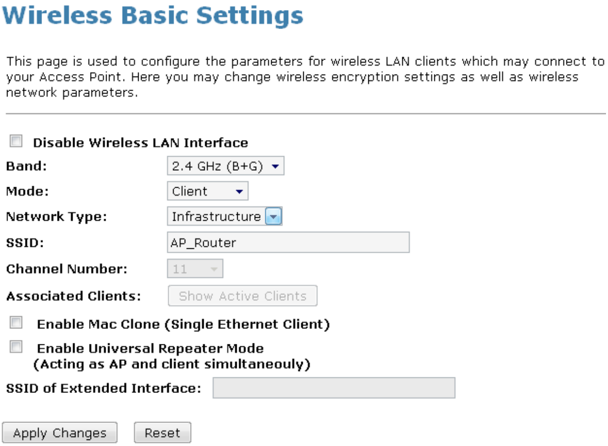
Change setting successfully!

From the left-hand Wireless menu, click on Basic Settings.

From the Mode drop-down list, select Client.

Enter SSID of the AP that you want to connect to for example AP_Router. If you don't know what the SSID of the AP that you want to connect to, please skip this step.

Click Apply Changes button.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ **Disable Wireless LAN Interface**

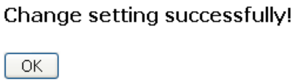
Band:	2.4 GHz (B+G)
Mode:	Client
Network Type:	Infrastructure
SSID:	AP_Router
Channel Number:	11
Associated Clients:	Show Active Clients

□ **Enable Mac Clone (Single Ethernet Client)**

□ **Enable Universal Repeater Mode (Acting as AP and client simultaneouly)**

SSID of Extended Interface:

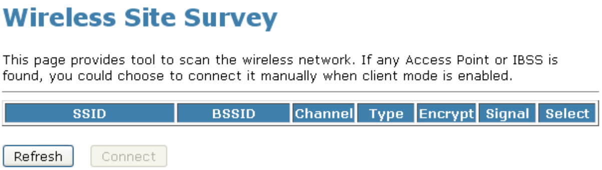
Change setting successfully! Click on OK button to confirm and return.



Change setting successfully!

From the left-hand Wireless menu, click on Site Survey.

Click Refresh button.

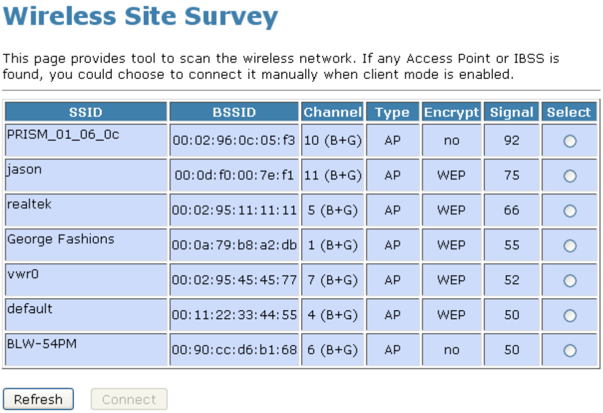


Wireless Site Survey

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.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select

Now you could see the APs that scanned by the Wireless Gateway were listed below.



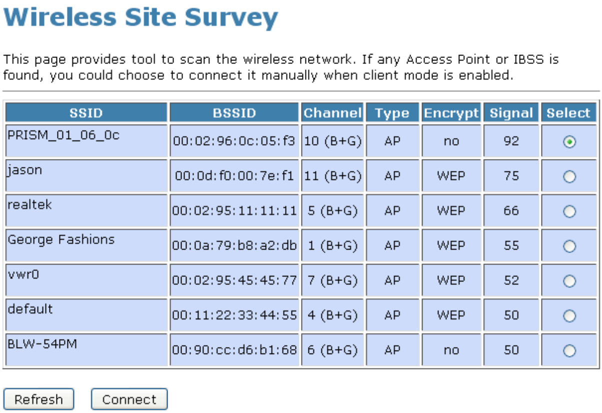
Wireless Site Survey

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.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
PRISM_01_06_0c	00:02:96:0c:05:f3	10 (B+G)	AP	no	92	○
jason	00:0d:f0:00:7e:f1	11 (B+G)	AP	WEP	75	○
realtek	00:02:95:11:11:11	5 (B+G)	AP	WEP	66	○
George Fashions	00:0a:79:b8:a2:db	1 (B+G)	AP	WEP	55	○
vwr0	00:02:95:45:45:77	7 (B+G)	AP	WEP	52	○
default	00:11:22:33:44:55	4 (B+G)	AP	WEP	50	○
BLW-54PM	00:90:cc:d6:b1:68	6 (B+G)	AP	no	50	○

Click on the ratio of AP's SSID under the item Select that you want the Wireless Gateway to connect to.

Click Connect button.

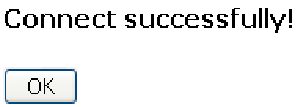


Wireless Site Survey

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.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
PRISM_01_06_0c	00:02:96:0c:05:f3	10 (B+G)	AP	no	92	●
jason	00:0d:f0:00:7e:f1	11 (B+G)	AP	WEP	75	○
realtek	00:02:95:11:11:11	5 (B+G)	AP	WEP	66	○
George Fashions	00:0a:79:b8:a2:db	1 (B+G)	AP	WEP	55	○
vwr0	00:02:95:45:45:77	7 (B+G)	AP	WEP	52	○
default	00:11:22:33:44:55	4 (B+G)	AP	WEP	50	○
BLW-54PM	00:90:cc:d6:b1:68	6 (B+G)	AP	no	50	○

Connect successfully! Click on OK button to confirm and return.

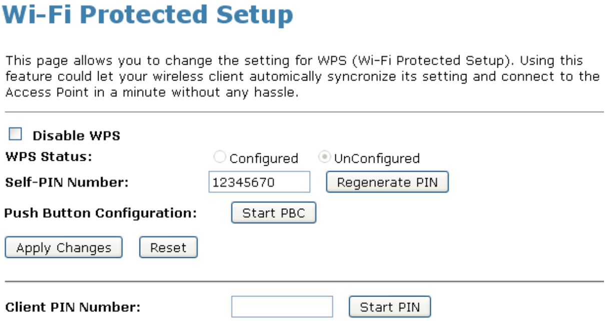


Connect successfully!

WPS

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

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



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

☐ Disable WPS

WPS Status: ○ Configured ● UnConfigured

Self-PIN Number: 12345670

Push Button Configuration:

Client PIN Number:

Field	Description
Disable WPS	Checking this box and clicking "Apply Changes" 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 " Apply Changes". Moreover, if users want to make their own PIN, they could enter four digit PIN without checksum and then click " Apply Changes". However, this would not be recommended since the registrar side needs to be supported with four digit PIN.
Push Button Configuration	Clicking this button will invoke the PBC method of WPS. It is only used when AP acts as a registrar.

Field	Description
Apply Changes	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

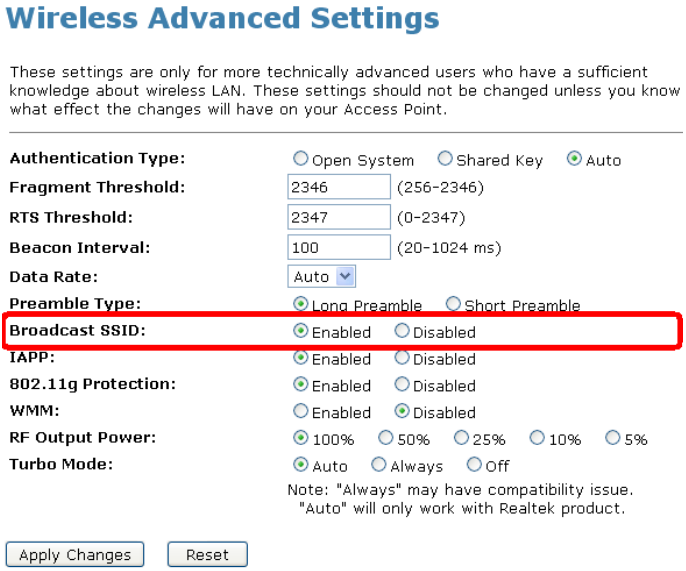
In Infrastructure-Client mode, Wireless Gateway only supports enrollee's role. If users click "Start PIN", click "Start PBC", or press the physical button on Wireless Gateway, it will start to seek WPS AP. Once users apply the same method on registrar side, Wireless Gateway will receive the wireless 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 Advanced Settings page

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



Wireless 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.

Authentication Type:	○ Open System ○ Shared Key ● Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Data Rate:	Auto
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enabled ○ Disabled
IAPP:	● Enabled ○ Disabled
802.11g Protection:	● Enabled ○ Disabled
WMM:	○ Enabled ● Disabled
RF Output Power:	● 100% ○ 50% ○ 25% ○ 10% ○ 5%
Turbo Mode:	● Auto ○ Always ○ Off

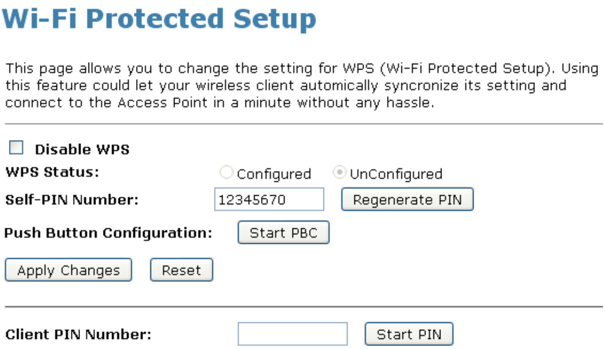
Note: "Always" may have compatibility issue.
"Auto" will only work with Realtek product.

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.

From the left-hand Wireless -> WPS menu. The following page is displayed:

Make sure AP is in un-configured state.



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

□ Disable WPS

WPS Status: ○ Configured ● UnConfigured

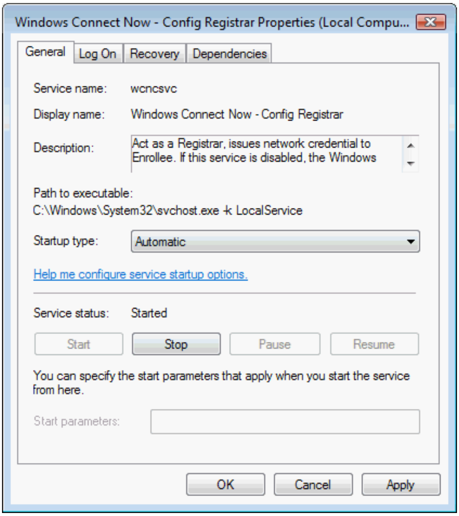
Self-PIN Number: 12345670

Push Button Configuration:

Client PIN Number:

Plug the Ethernet cable into AP's LAN port and make sure the IP connection is valid with Vista.

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".



Windows Connect Now - Config Registrar Properties (Local Compu...

Service name: wcncsvc

Display name: Windows Connect Now - Config Registrar

Description: Act as a Registrar, issues network credential to Enrollee. If this service is disabled, the Windows

Path to executable:
C:\Windows\System32\svchost.exe -k LocalService

Startup type: Automatic

Help me configure service startup options.

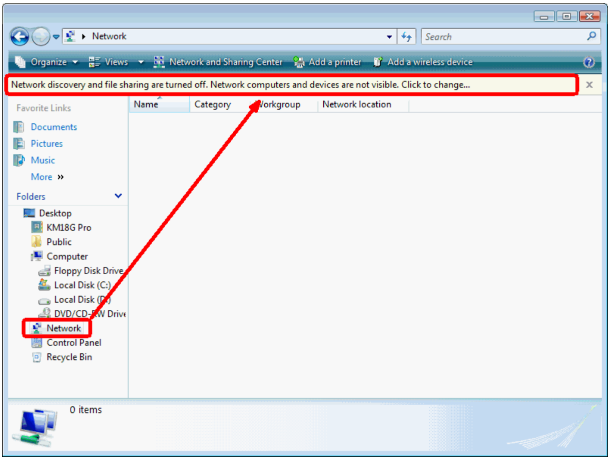
Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

If the previous steps are done, open Windows Explorer. Go to the Network section.

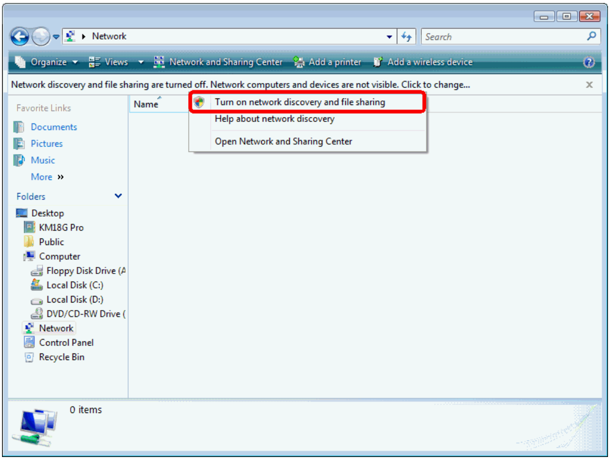
Click on "Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to Change…"



Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to change...

0 items

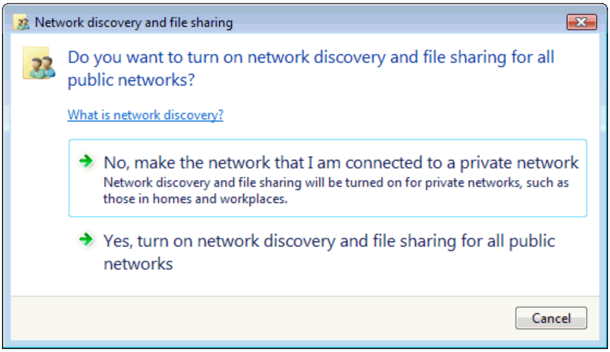
Click on “Turn on network discovery and file sharing“



Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to change...

0 items

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



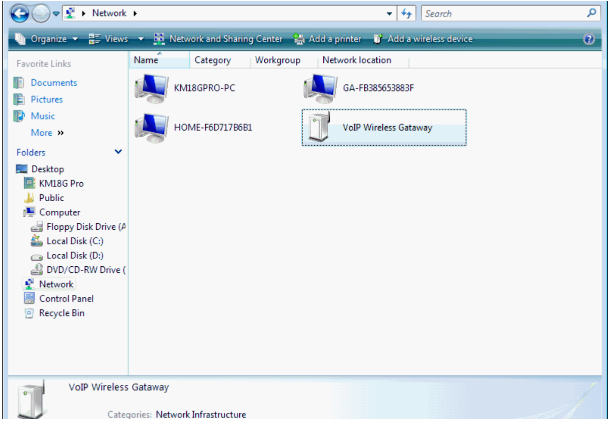
Do you want to turn on network discovery and file sharing for all public networks?

What is network discovery?

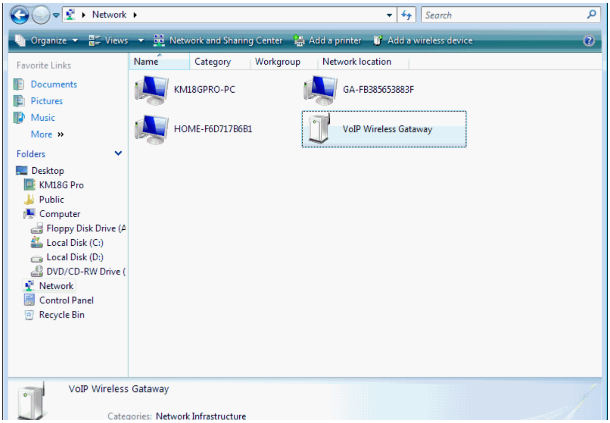
No, make the network that I am connected to a private network
Network discovery and file sharing will be turned on for private networks, such as those in homes and workplaces.

Yes, turn on network discovery and file sharing for all public networks

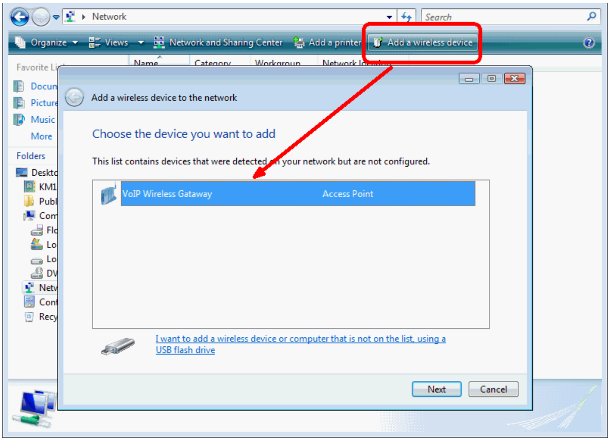
AP's icon will show up. Double click on it.



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



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



Add a wireless device to the network

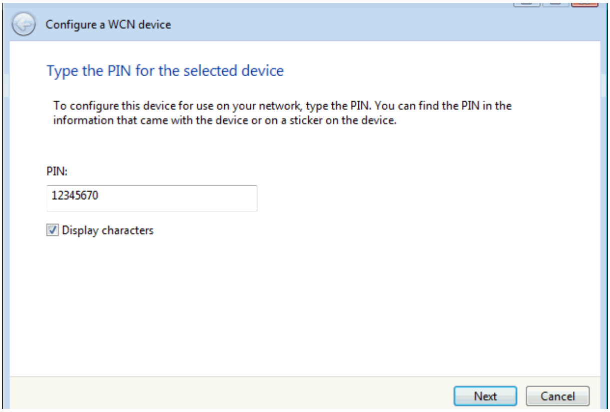
Choose the device you want to add

This list contains devices that were detected on your network but are not configured.

VoIP Wireless Gataway	Access Point

I want to add a wireless device or computer that is not on the list, using a USB flash drive

Enter AP's Self-PIN Number and click "next".



Configure a WCN device

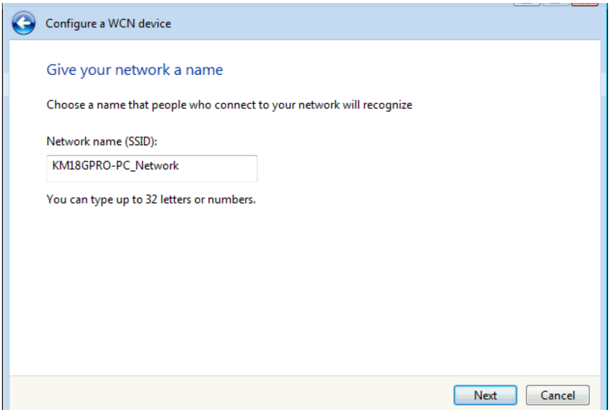
Type the PIN for the selected device

To configure this device for use on your network, type the PIN. You can find the PIN in the information that came with the device or on a sticker on the device.

PIN: 12345670

☑ Display characters

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



Configure a WCN device

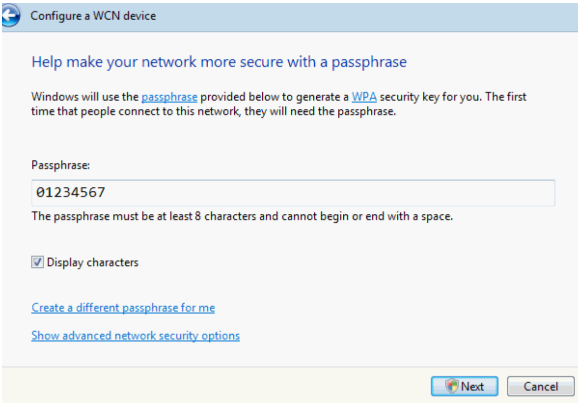
Give your network a name

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

Network name (SSID): KM18GPRO-PC_Network

You can type up to 32 letters or numbers.

Enter the Passphrase and then click Next.



Configure a WCN device

Help make your network more secure with a passphrase

Windows will use the passphrase provided below to generate a WPA security key for you. The first time that people connect to this network, they will need the passphrase.

Passphrase: 01234567

The passphrase must be at least 8 characters and cannot begin or end with a space.

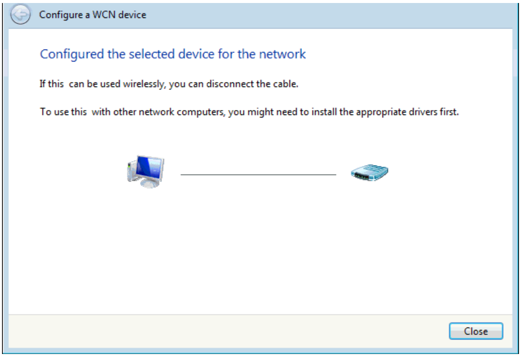
☑ Display characters

Create a different passphrase for me

Show advanced network security options

A User Account Control screen pops up, click Continue.

AP is successfully configured by WCN.



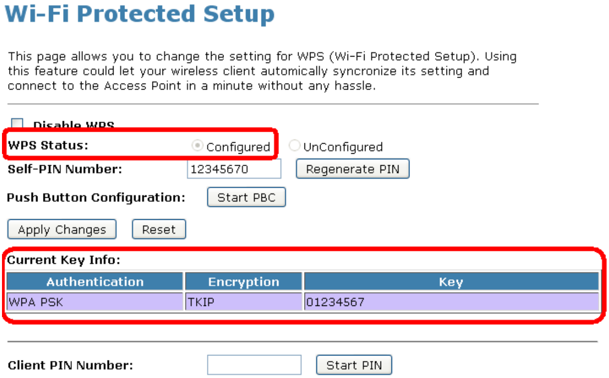
Configure a WCN device

Configured the selected device for the network

If this can be used wirelessly, you can disconnect the cable.

To use this with other network computers, you might need to install the appropriate drivers first.

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".



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

□ Disable WPS

WPS Status: ● Configured ○ UnConfigured

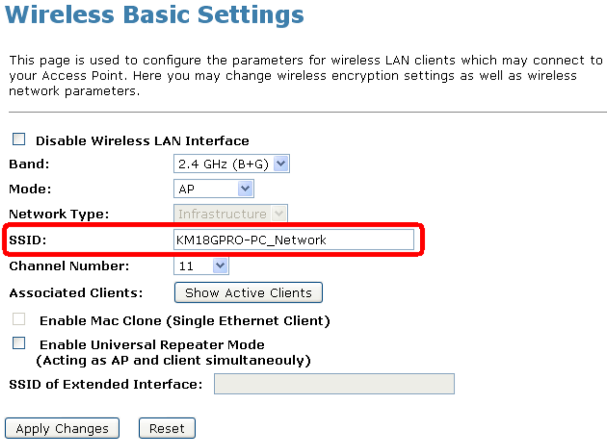
Self-PIN Number: 12345670

Current Key Info:

Authentication	Encryption	Key
WPA PSK	TKIP	01234567

Client PIN Number:

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



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: KM18GPRO-PC_Network

Channel Number: 11

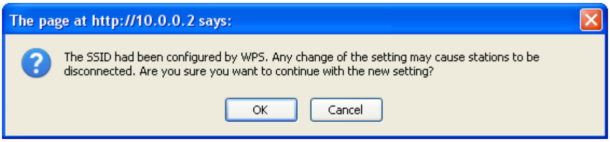
Associated Clients:

□ Enable Mac Clone (Single Ethernet Client)

□ Enable Universal Repeater Mode
(Acting as AP and client simultaneouly)

SSID of Extended Interface:

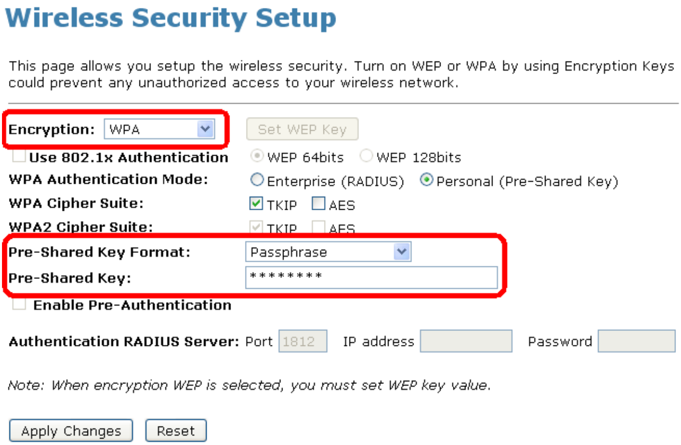
If users try to modify the SSID at this moment, there will be a warning message popping up that informs the risk of this action. The reason is that users may not know whether the SSID is already given to a station. Changing the SSID will result in the link between AP and stations to be broken. If users insist on this action, AP will take their decision.



The page at http://10.0.0.2 says:

The SSID had been configured by WPS. Any change of the setting may cause stations to be disconnected. Are you sure you want to continue with the new setting?

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.



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.

Encryption: WPA

□ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: ☑ TKIP □ AES

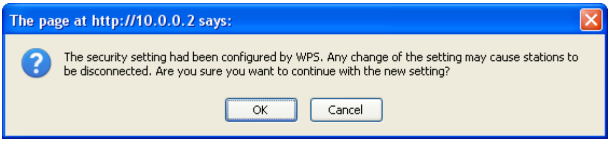
Pre-Shared Key Format: Passphrase

Pre-Shared Key: ********

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

Note: When encryption WEP is selected, you must set WEP key value.



The page at http://10.0.0.2 says:

The security setting had been configured by WPS. Any change of the setting may cause stations to be disconnected. Are you sure you want to continue with the new setting?

Operations of AP - AP being a registrar

AP mode

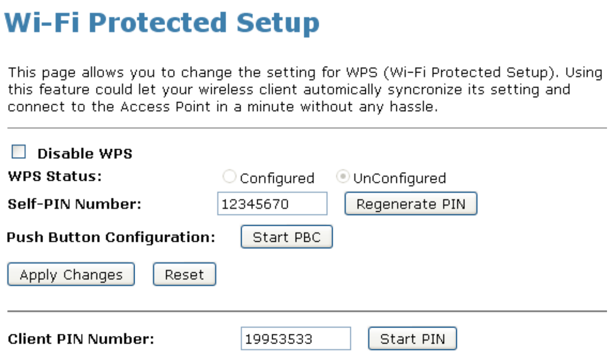
Whenever users enter station's PIN into AP's Wi-Fi Protected Setup page and click "Start PIN", AP will become a registrar. Users must start the PIN method on the station side within two minutes.

From the left-hand Wireless -> WPS menu. The following page is displayed:

Make sure AP is in un-configured state.

Enter the Client PIN Number.

Click Start PIN.



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

☐ **Disable WPS**

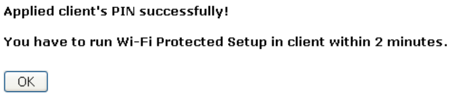
WPS Status: ○ Configured ● UnConfigured

Self-PIN Number: 12345670

Push Button Configuration:

Client PIN Number: 19953533

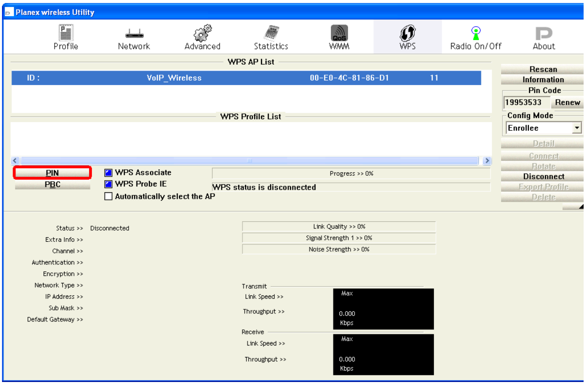
Users must start the PIN method on the station side within two minutes.



Applied client's PIN successfully!

You have to run Wi-Fi Protected Setup in client within 2 minutes.

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



Planex wireless Utility

WPS AP List

ID : VoIP_Wireless 00-E0-4C-81-86-D1 11

WPS Profile List

Pin Code: 19953533

Config Mode: Enrollee

☑ WPS Associate
☑ WPS Probe IE
☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

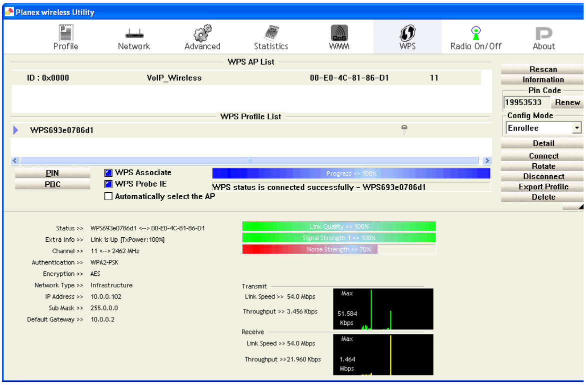
Status >> Disconnected
Extra Info >>
Channel >>
Authentication >>
Encryption >>
Network Type >>
IP Address >>
Sub Mask >>
Default Gateway >>

Link Quality >> 0%
Signal Strength 1 >> 0%
Noise Strength >> 0%

Transmit
Link Speed >>
Throughput >> 0.000 Kbps

Receive
Link Speed >>
Throughput >> 0.000 Kbps

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



Planex wireless Utility

WPS AP List

ID : 0x0000 VoIP_Wireless 00-E0-4C-81-86-D1 11

WPS Profile List

WPS693e0786d1

Pin Code: 19953533

Config Mode: Enrollee

☑ WPS Associate
☑ WPS Probe IE
☐ Automatically select the AP

Progress >> 100%

WPS status is connected successfully - WPS693e0786d1

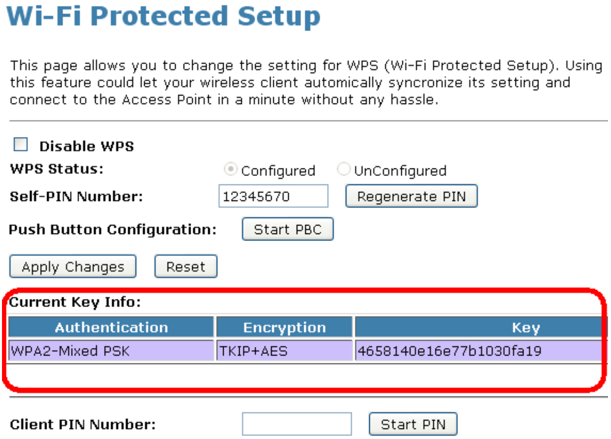
Status >> WPS693e0786d1 <--> 00-E0-4C-81-86-D1
Extra Info >> Link is Up [TxPower:100%]
Channel >> 11 <--> 2462 MHz
Authentication >> WPA2-PSK
Encryption >> AES
Network Type >> Infrastructure
IP Address >> 10.0.0.102
Sub Mask >> 255.0.0.0
Default Gateway >> 10.0.0.2

Link Quality >> 100%
Signal Strength 1 >> 100%
Noise Strength >> 70%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 3.456 Kbps
51.584 Kbps

Receive
Link Speed >> 54.0 Mbps
Throughput >>21.960 Kbps
1.464 Mbps

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.



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

□ **Disable WPS**

WPS Status: ● Configured ○ UnConfigured

Self-PIN Number: 12345670 [Regenerate PIN]

Push Button Configuration: [Start PBC]

[Apply Changes] [Reset]

Current Key Info:

Authentication	Encryption	Key
WPA2-Mixed PSK	TKIP+AES	4658140e16e77b1030fa19

Client PIN Number: [Start PIN]

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

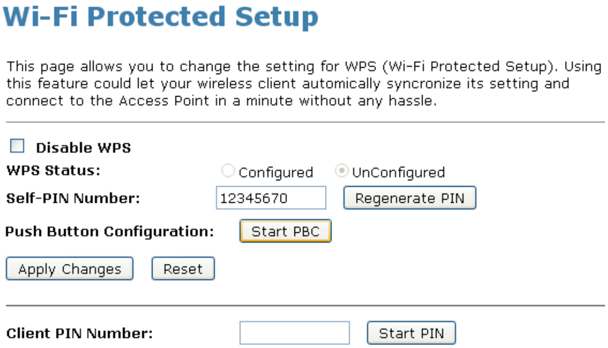
Wireless Gateway supports a virtual button "Start PBC" on the Wi-Fi Protected Setup page for Push Button method. If users push a virtual button "Start PBC", AP will initiate a WPS session and wait for any station to join. At this moment, AP will detect whether there is more than one station that starts 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.

From the left-hand Wireless -> WPS menu. The following page is displayed:

Make sure AP is in un-configured state.

Click Start PBC.



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

□ **Disable WPS**

WPS Status: ○ Configured ● UnConfigured

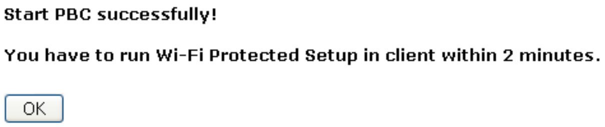
Self-PIN Number: 12345670 [Regenerate PIN]

Push Button Configuration: [Start PBC]

[Apply Changes] [Reset]

Client PIN Number: [Start PIN]

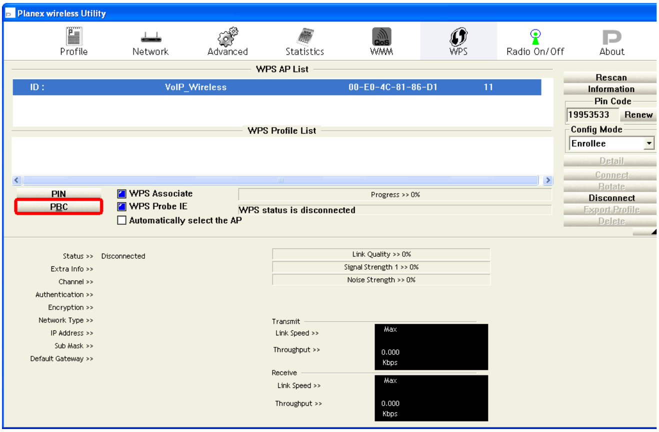
Users must start the PBC method on the station side within two minutes.



Start PBC successfully!

You have to run Wi-Fi Protected Setup in client within 2 minutes.

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



WPS AP List

ID : VoIP_Wireless 00-E0-4C-81-86-D1 11

WPS Profile List

Pin Code: 19953533

Config Mode: Enrollee

☑ WPS Associate
☑ WPS Probe IE
□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

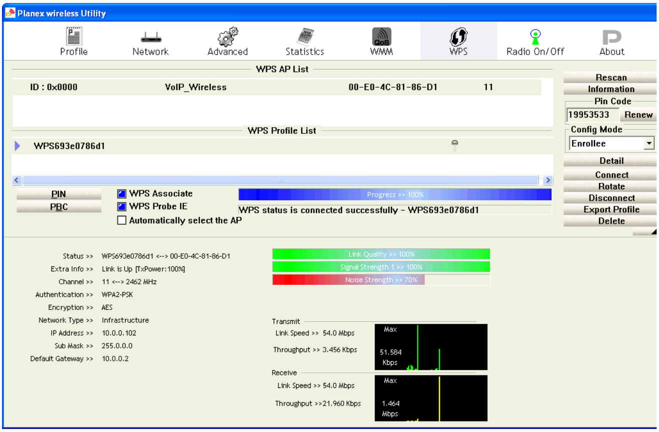
Status >> Disconnected
Extra Info >>
Channel >>
Authentication >>
Encryption >>
Network Type >>
IP Address >>
Sub Mask >>
Default Gateway >>

Link Quality >> 0%
Signal Strength 1 >> 0%
Noise Strength >> 0%

Transmit
Link Speed >>
Throughput >>
Max 0.000 Kbps

Receive
Link Speed >>
Throughput >>
Max 0.000 Kbps

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



WPS AP List

ID : 0x0000 VoIP_Wireless 00-E0-4C-81-86-D1 11

WPS Profile List

WPS693e0786d1

Pin Code: 19953533

Config Mode: Enrollee

☑ WPS Associate
☑ WPS Probe IE
□ Automatically select the AP

Progress >> 100%

WPS status is connected successfully - WPS693e0786d1

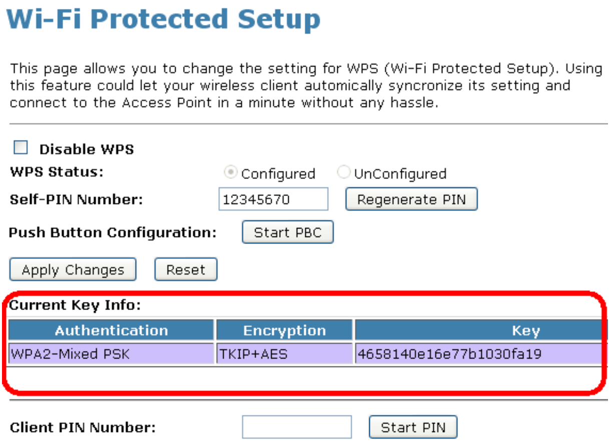
Status >> WPS693e0786d1 <--> 00-E0-4C-81-86-D1
Extra Info >> Link is Up [TxPower:100%]
Channel >> 11 <--> 2462 MHz
Authentication >> WPA2-PSK
Encryption >> AES
Network Type >> Infrastructure
IP Address >> 10.0.0.102
Sub Mask >> 255.0.0.0
Default Gateway >> 10.0.0.2

Link Quality >> 100%
Signal Strength 1 >> 100%
Noise Strength >> 70%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 3.456 Kbps
Max 51.584 Kbps

Receive
Link Speed >> 54.0 Mbps
Throughput >>21.960 Kbps
Max 1.464 Mbps

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.



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

□ **Disable WPS**

WPS Status: ● Configured ○ UnConfigured

Self-PIN Number: 12345670

Push Button Configuration:

Current Key Info:

Authentication	Encryption	Key
WPA2-Mixed PSK	TKIP+AES	4658140e16e77b1030fa19

Client PIN Number:

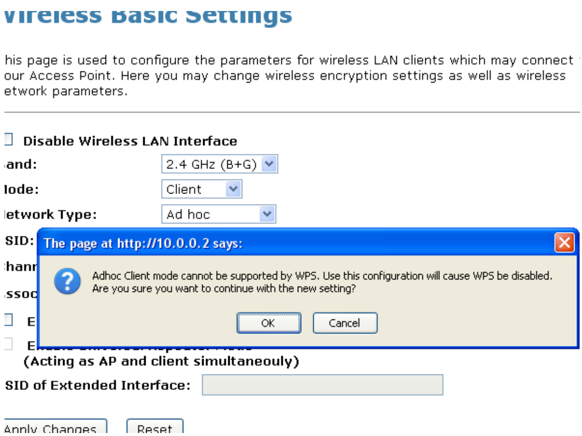
Other pages such as Wireless Basic Settings page and Wireless Security Setup page will also be updated appropriately as described in previous sections. In this case, AP is in un-configured state before the station initiates the WPS handshake. According to the WPS spec, AP will create a wireless profile 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.

Warning pop-up windows of AP

When users try to operate on AP not appropriately, AP will give a warning message to them. All kinds of pop-up windows will be demonstrated in this section.

Un-supported mode in WPS

If users select any mode that is not supported with WPS, there will be a pop-up warning window as the following. If users click "Yes", WPS will be disabled.



vireless Basic Settings

his page is used to configure the parameters for wireless LAN clients which may connect our Access Point. Here you may change wireless encryption settings as well as wireless etwork parameters.

□ **Disable Wireless LAN Interface**

and: 2.4 GHz (B+G)

lode: Client

letwork Type: Ad hoc

SID:

hanr

sso

□ **E**

□ **E**

(Acting as AP and client simultaneouly)

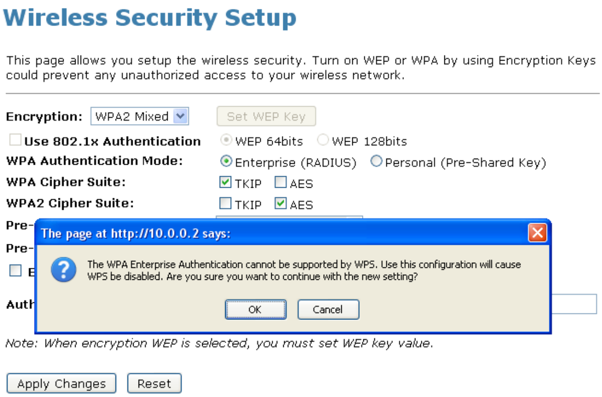
SID of Extended Interface:

The page at http://10.0.0.2 says:

Adhoc Client mode cannot be supported by WPS. Use this configuration will cause WPS be disabled.
Are you sure you want to continue with the new setting?

Un-supported security in WPS

If users try to select an unsupported type of security such as RADIUS support, a warning message will be given. If users enforce this security, WPS will be disabled. Please see below.



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.

Encryption: WPA2 Mixed ▾ Set WEP Key

□ Use 802.1x Authentication ○ WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ● Enterprise (RADIUS) ○ Personal (Pre-Shared Key)

WPA Cipher Suite: ☑ TKIP □ AES

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-

Pre-

□ E

Auth

The page at http://10.0.0.2 says:

The WPA Enterprise Authentication cannot be supported by WPS. Use this configuration will cause WPS be disabled. Are you sure you want to continue with the new setting?

OK Cancel

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes Reset

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...

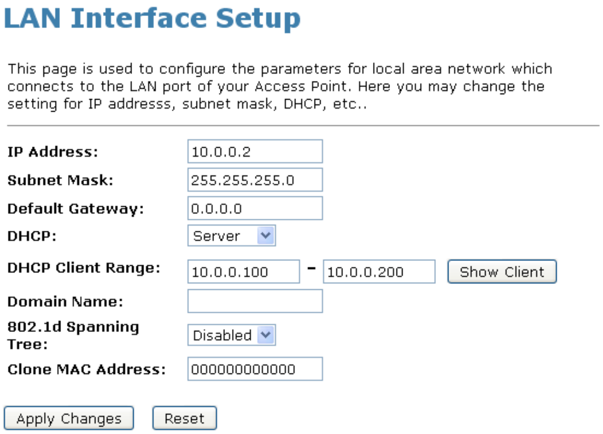
Note

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:

From the left-hand Network Settings -> LAN Interface menu. The following page is displayed:



LAN Interface Setup

This page is used 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 addresss, subnet mask, DHCP, etc..

IP Address:	10.0.0.2
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server ▾
DHCP Client Range:	10.0.0.100 - 10.0.0.200 Show Client
Domain Name:	
802.1d Spanning Tree:	Disabled ▾
Clone MAC Address:	000000000000

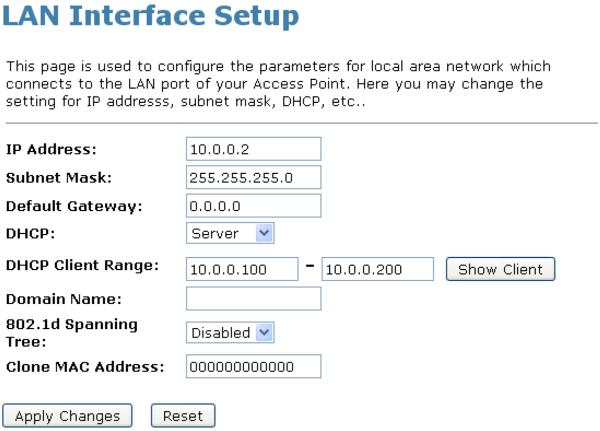
Apply Changes Reset

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
DHCP Client Range	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
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:

From the left-hand Network Settings -> LAN Interface menu. The following page is displayed:



LAN Interface Setup

This page is used 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 addresss, subnet mask, DHCP, etc..

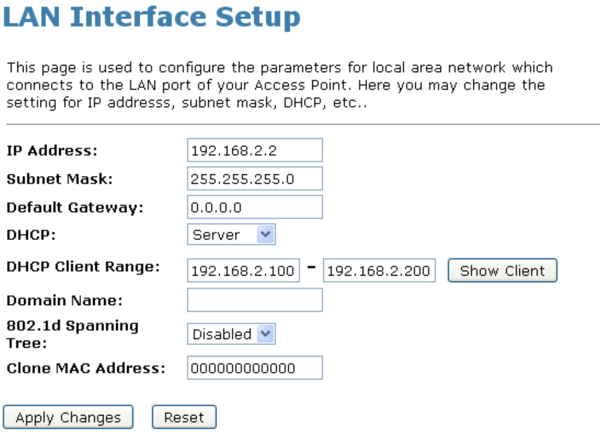
IP Address:	10.0.0.2
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	10.0.0.100 - 10.0.0.200
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Type IP Address and Change default LAN port IP address.

Click in the IP Address and Subnet Mask box and type a new IP Address and Subnet Mask.

Change the default DHCP Client Range.

Click Apply Changes.



LAN Interface Setup

This page is used 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 addresss, subnet mask, DHCP, etc..

IP Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DHCP: Server

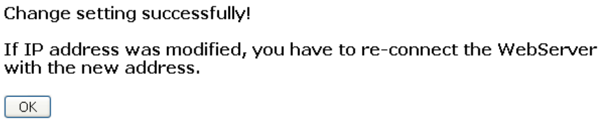
DHCP Client Range: 192.168.2.100 - 192.168.2.200

Domain Name:

802.1d Spanning Tree: Disabled

Clone MAC Address: 000000000000

The primary IP address is being changed to 192.168.2.2 netmask 255.255.255.0. Please go to http://192.168.2.2 to continue. Your browser communicates with the web server via the LAN connection, and changing the IP address may disrupt this.



Change setting successfully!

If IP address was modified, you have to re-connect the WebServer with the new address.

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.

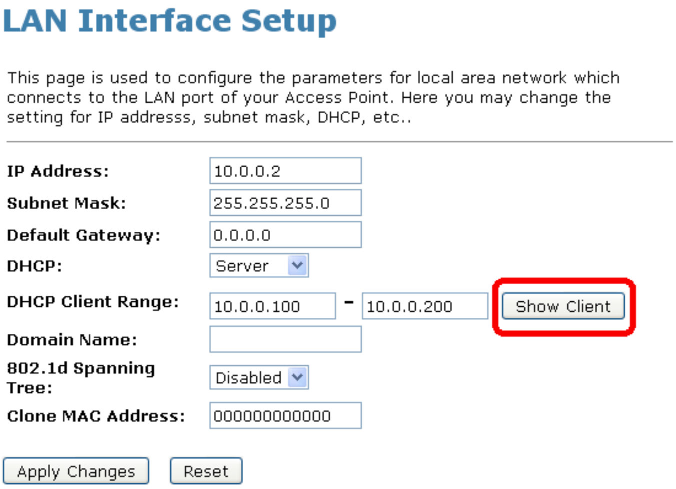
Note

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:

From the left-hand Network Settings -> LAN Interface menu. The following page is displayed:

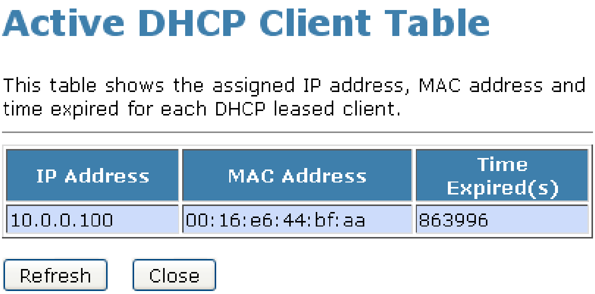


LAN Interface Setup

This page is used 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 addresss, subnet mask, DHCP, etc..

IP Address:	10.0.0.2
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	10.0.0.100 - 10.0.0.200
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

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



Active DHCP Client Table

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP Address	MAC Address	Time Expired(s)
10.0.0.100	00:16:e6:44:bf:aa	863996

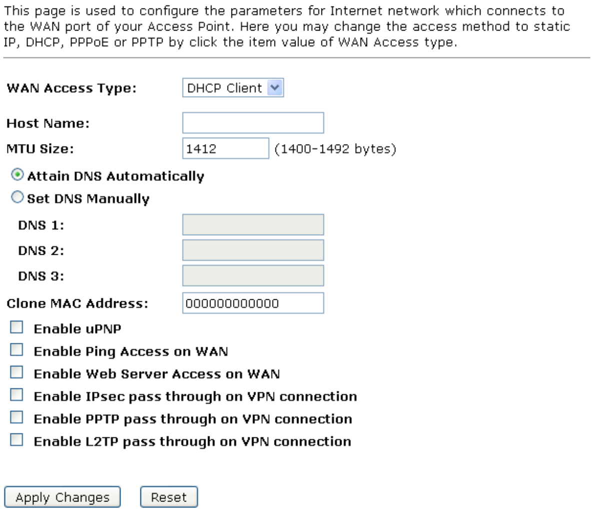
WAN Interface

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

From the left-hand Network Settings -> WAN Interface menu. The following page is displayed:



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 or PPTP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Host Name:

MTU Size: 1412 (1400-1492 bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

□ Enable Ping Access on WAN

□ Enable Web Server Access on WAN

□ Enable IPsec pass through on VPN connection

□ Enable PPTP pass through on VPN connection

□ Enable L2TP pass through on VPN connection

Option		Description
WAN Access Type	Static IP	Choose this option if you are a leased line user with a fixed IP ad-dress.
	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
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 se-rvice provider
Password		Password for PPPoE registration recognized by the Internet servi-ce 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
Clone MAC Address		Clone MAC lets the device identify itself as another computer or device

Option	Description
Enable uPNP	Enable or Disable uPNP
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.

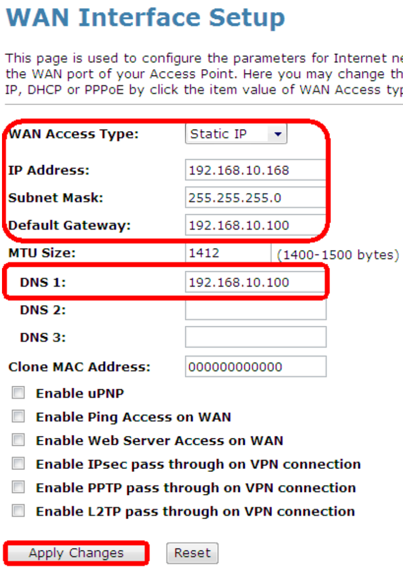
If your ISP wants you to connect to the Internet using Static IP, follow the instructions below.

From the left-hand Network Settings -> WAN Interface menu. The following page is displayed:

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

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

Click Apply Changes.



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 or PPPoE by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 192.168.10.168

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.100

MTU Size: 1412 (1400-1500 bytes)

DNS 1: 192.168.10.100

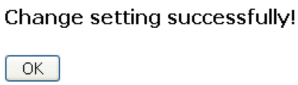
DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP
□ Enable Ping Access on WAN
□ Enable Web Server Access on WAN
□ Enable IPsec pass through on VPN connection
□ Enable PPTP pass through on VPN connection
□ Enable L2TP pass through on VPN connection

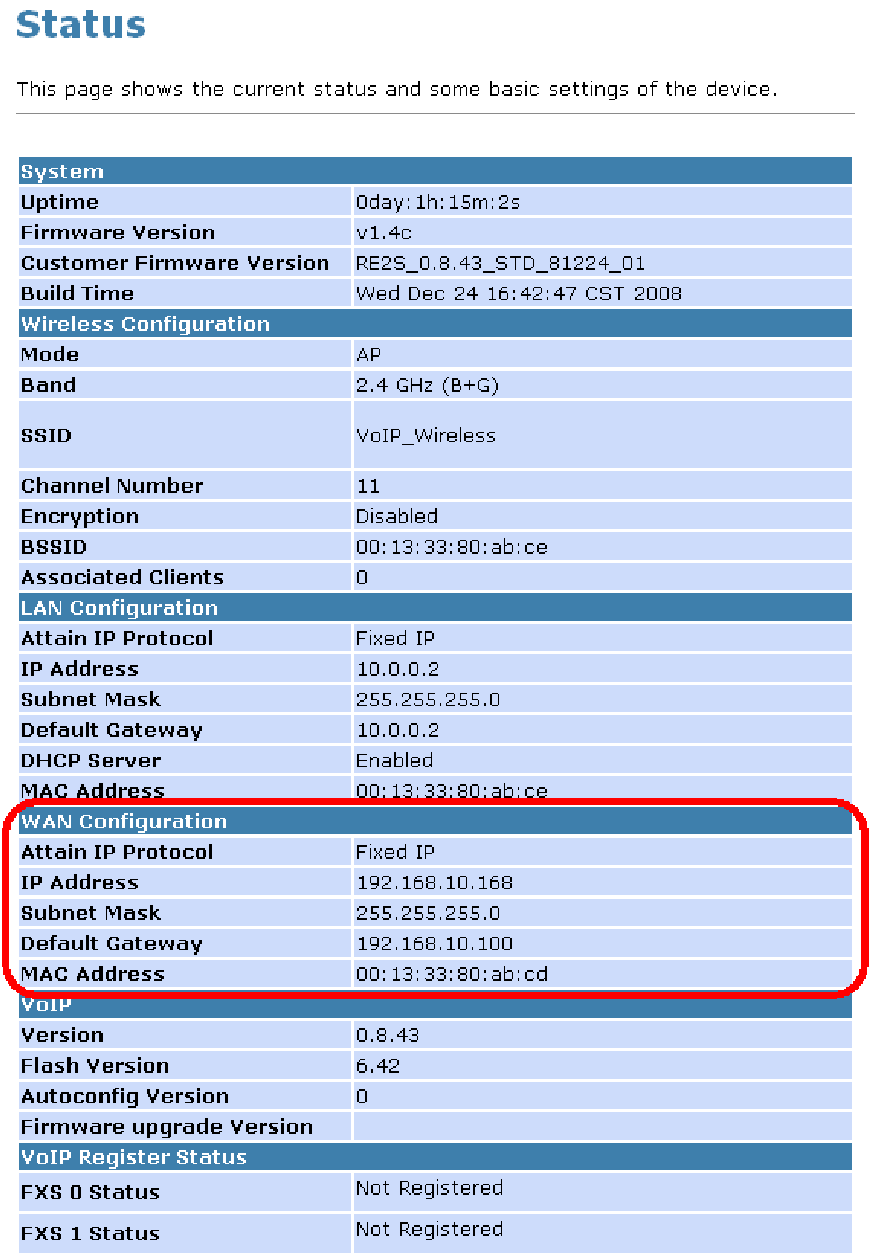
Click OK.



Change setting successfully!

From the left-hand Management -> Status menu. The following page is displayed:

If you could see the Attain IP Protocol is shown Fixed IP, you can have the Internet Access right now.



Status

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

System	
Uptime	0day:1h:15m:2s
Firmware Version	v1.4c
Customer Firmware Version	RE2S_0.8.43_STD_81224_01
Build Time	Wed Dec 24 16:42:47 CST 2008
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	VoIP_Wireless
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:80:ab:ce
Associated Clients	0
LAN 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	00:13:33:80:ab:ce
WAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.10.168
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.100
MAC Address	00:13:33:80:ab:cd
VoIP	
Version	0.8.43
Flash Version	6.42
Autoconfig Version	0
Firmware upgrade Version	
VoIP Register Status	
FXS 0 Status	Not Registered
FXS 1 Status	Not Registered

Configuring DHCP Client connection

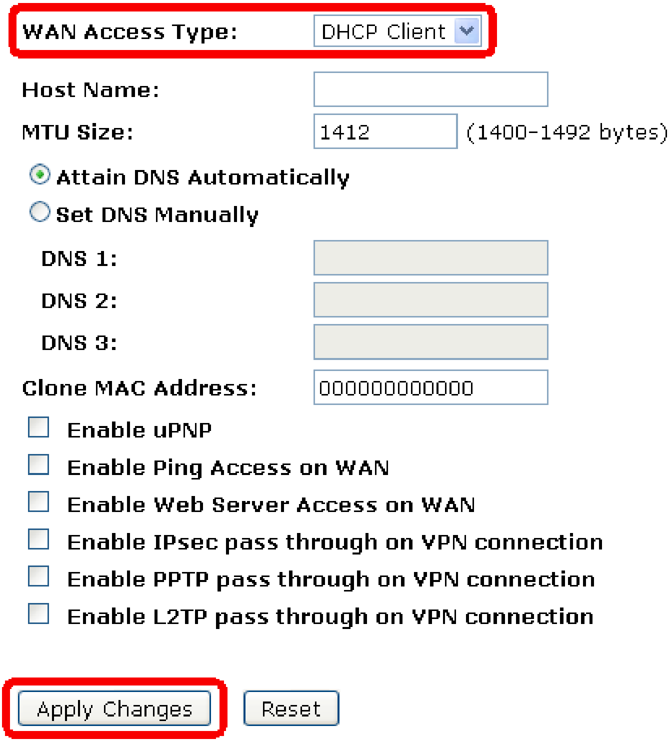
Dynamic Host Configuration Protocol (DHCP), Dynamic IP (Get WAN IP Address automatically). If you are connected to the Internet through a Cable modem line, then a dynamic IP will be assigned.

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

From the left-hand Network Settings -> WAN Interface menu. The following page is displayed:

From the WAN Access Type drop-down list, select DHCP Client setting.

Click Apply Changes.



WAN Access Type: DHCP Client

Host Name:

MTU Size: 1412 (1400-1492 bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

□ Enable Ping Access on WAN

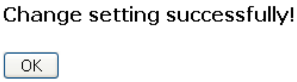
□ Enable Web Server Access on WAN

□ Enable IPsec pass through on VPN connection

□ Enable PPTP pass through on VPN connection

□ Enable L2TP pass through on VPN connection

Click OK.



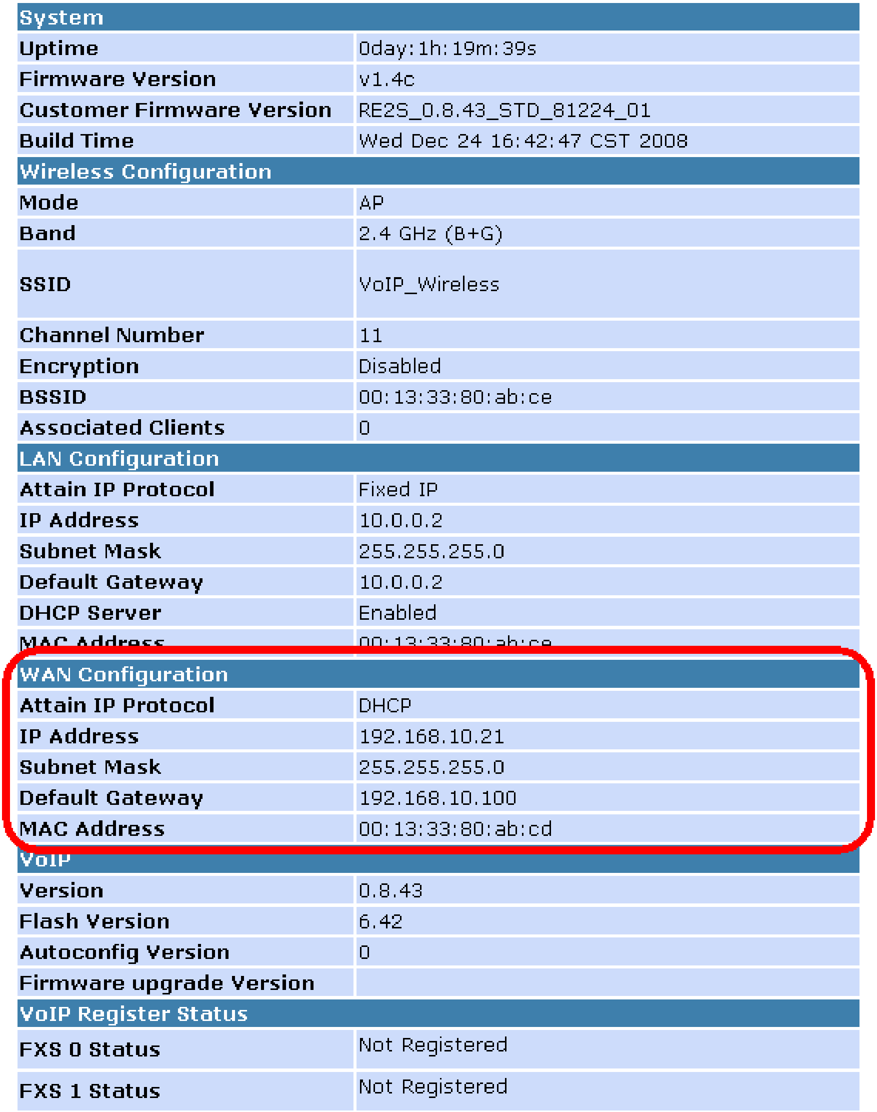
Change setting successfully!

From the left-hand Management -> Status menu. The following page is displayed:

If you could see the Attain IP Protocol is shown DHCP, you can have the Internet Access right now.

Status

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



System	
Uptime	0day:1h:19m:39s
Firmware Version	v1.4c
Customer Firmware Version	RE2S_0.8.43_STD_81224_01
Build Time	Wed Dec 24 16:42:47 CST 2008
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	VoIP_Wireless
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:80:ab:ce
Associated Clients	0
LAN 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	00:13:33:80:ab:ce
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.21
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.100
MAC Address	00:13:33:80:ab:cd
VoIP	
Version	0.8.43
Flash Version	6.42
Autoconfig Version	0
Firmware upgrade Version	
VoIP Register Status	
FXS 0 Status	Not Registered
FXS 1 Status	Not Registered

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.

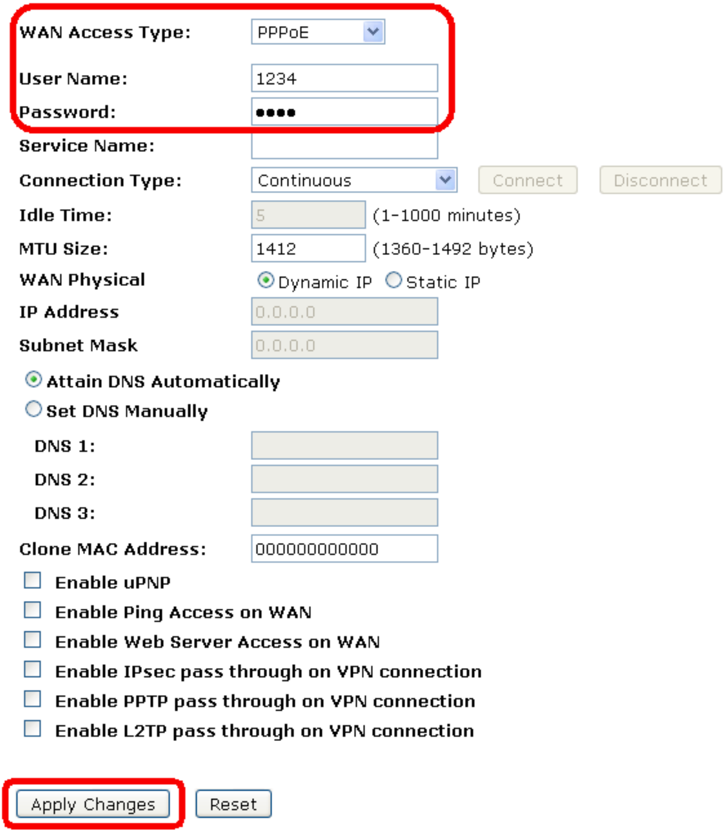
If your ISP wants you to connect to the Internet using PPP, follow the instructions below.

From the left-hand Network Settings -> WAN Interface menu. The following page is displayed:

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.

Click Apply Changes.



WAN Access Type: PPPoE

User Name: 1234

Password: ●●●●

Service Name:

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1412 (1360-1492 bytes)

WAN Physical ● Dynamic IP ○ Static IP

IP Address 0.0.0.0

Subnet Mask 0.0.0.0

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

□ Enable Ping Access on WAN

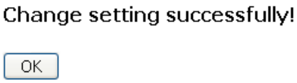
□ Enable Web Server Access on WAN

□ Enable IPsec pass through on VPN connection

□ Enable PPTP pass through on VPN connection

□ Enable L2TP pass through on VPN connection

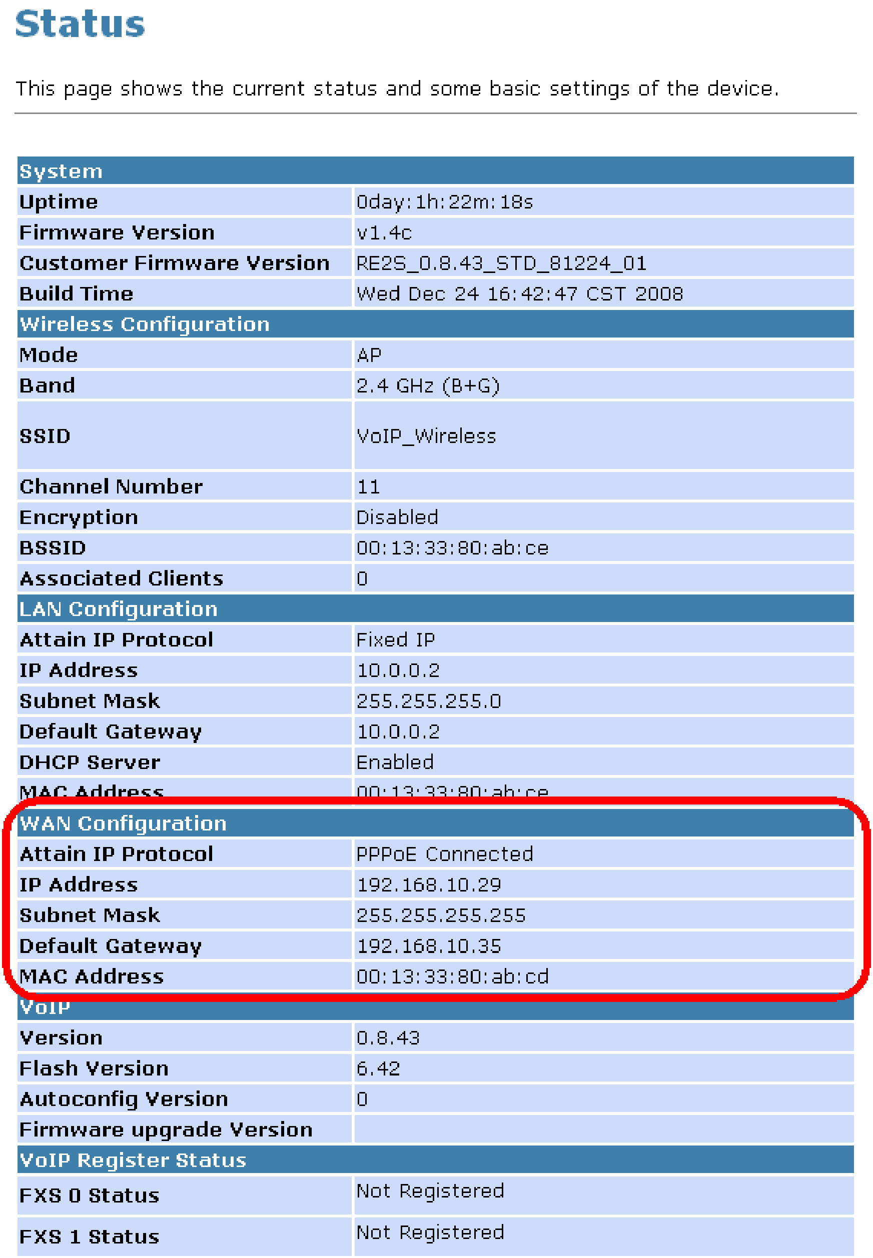
Click OK.



Change setting successfully!

From the left-hand Management -> Status menu. The following page is displayed:

If you could see the Attain IP Protocol is shown PPPoE Connected, you can have the Internet Access right now.



Status

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

System	
Uptime	0day:1h:22m:18s
Firmware Version	v1.4c
Customer Firmware Version	RE2S_0.8.43_STD_81224_01
Build Time	Wed Dec 24 16:42:47 CST 2008
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	VoIP_Wireless
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:80:ab:ce
Associated Clients	0
LAN 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	00:13:33:80:ab:ce
WAN Configuration	
Attain IP Protocol	PPPoE Connected
IP Address	192.168.10.29
Subnet Mask	255.255.255.255
Default Gateway	192.168.10.35
MAC Address	00:13:33:80:ab:cd
VoIP	
Version	0.8.43
Flash Version	6.42
Autoconfig Version	0
Firmware upgrade Version	
VoIP Register Status	
FXS 0 Status	Not Registered
FXS 1 Status	Not Registered

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.

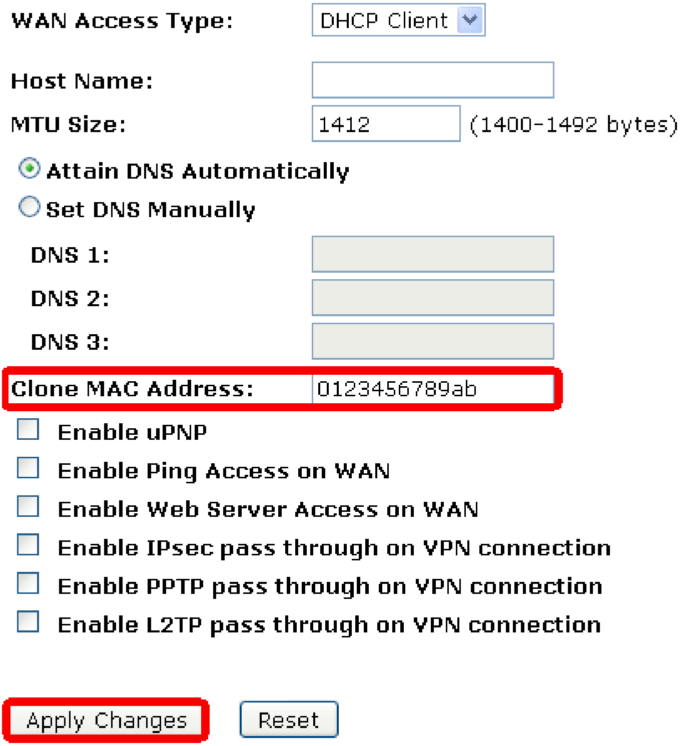
This page allows you to enable or disable Clone MAC Address option.

From the left-hand Network Settings -> WAN Interface menu. The following page is displayed:

Enter the MAC for example 0123456789ab that you want to be instead of in the Clone MAC Address field.

If you enter 12 digits of 0 in the Clone MAC Address field, it'll disable Clone MAC Address function.

Click Apply Changes.



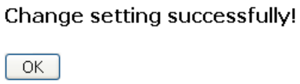
WAN Access Type:	DHCP Client
Host Name:	
MTU Size:	1412 (1400-1492 bytes)

● Attain DNS Automatically
○ Set DNS Manually

DNS 1:	
DNS 2:	
DNS 3:	
Clone MAC Address:	0123456789ab

□ Enable uPNP
□ Enable Ping Access on WAN
□ Enable Web Server Access on WAN
□ Enable IPsec pass through on VPN connection
□ Enable PPTP pass through on VPN connection
□ Enable L2TP pass through on VPN connection

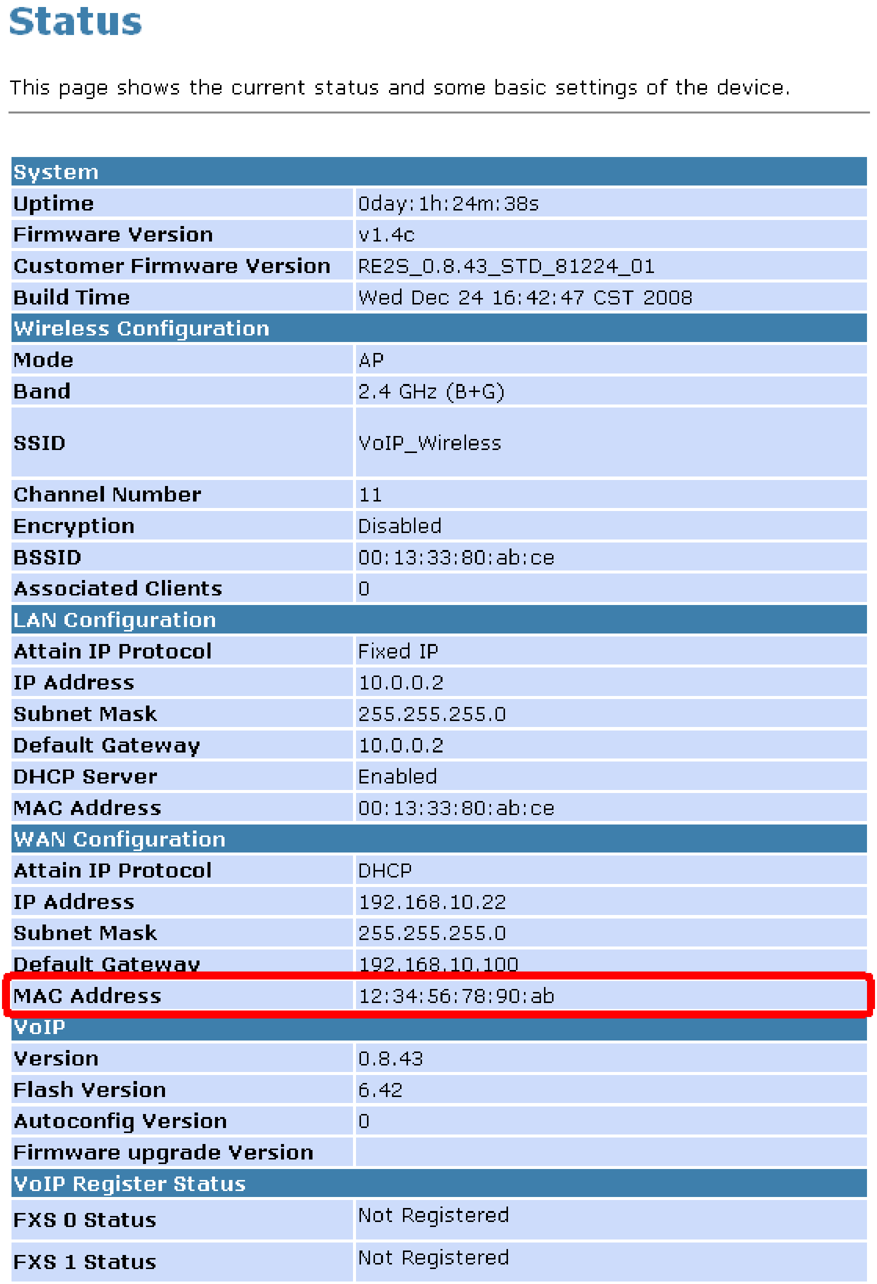
Click OK.



Change setting successfully!

From the left-hand Management -> Status menu. The following page is displayed:

If you could see the WAN Configuration -> MAC Address is changed to the one that you configured.



Status

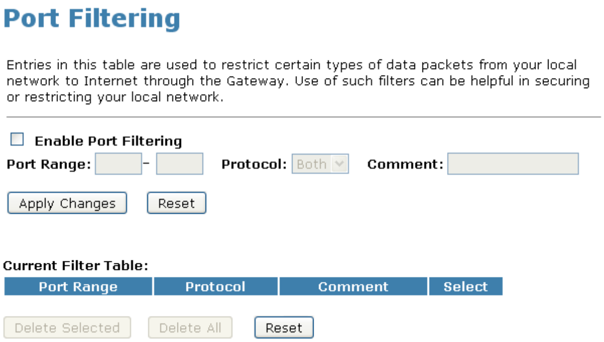
This page shows the current status and some basic settings of the device.

System	
Uptime	0day:1h:24m:38s
Firmware Version	v1.4c
Customer Firmware Version	RE2S_0.8.43_STD_81224_01
Build Time	Wed Dec 24 16:42:47 CST 2008
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	VoIP_Wireless
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:80:ab:ce
Associated Clients	0
LAN 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	00:13:33:80:ab:ce
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.22
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.100
MAC Address	12:34:56:78:90:ab
VoIP	
Version	0.8.43
Flash Version	6.42
Autoconfig Version	0
Firmware upgrade Version	
VoIP Register Status	
FXS 0 Status	Not Registered
FXS 1 Status	Not Registered

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.

From the left-hand Firewall -> Port Filtering menu. The following page is displayed:



Port 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.

□ Enable Port Filtering

Port Range: ____ - ____ Protocol: Both Comment: ____

Current Filter Table:

Port Range	Protocol	Comment	Select

Option	Description
Enable Port Filtering	Enable/Disable the WAN packet filter. Default setting is Disable.
Port Range	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

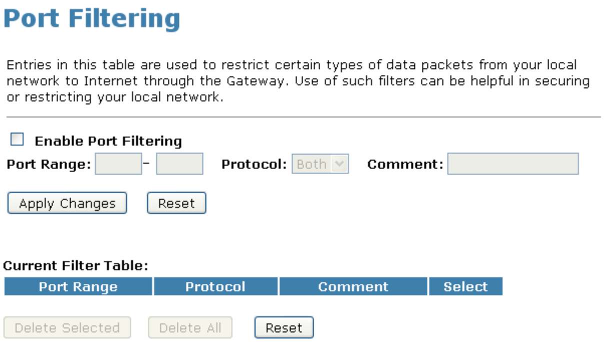
Note

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 Configuring NAT Security.

Port filtering for TCP port 80

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

From the left-hand Firewall -> Port Filtering menu. The following page is displayed:



Port 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.

□ Enable Port Filtering

Port Range: ____ - ____ Protocol: Both Comment: ____

Current Filter Table:

Port Range	Protocol	Comment	Select

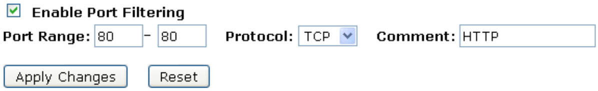
Check the option Enable Port Filtering to enable the port filtering.

Enter 80 and 80 in Port Range field.

From the Protocol drop-down list, select TCP setting.

Enter HTTP in Comment field.

Click Apply Changes.

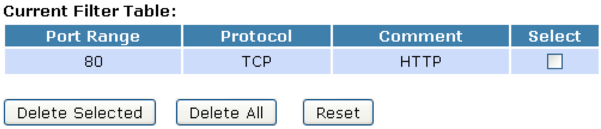


☑ **Enable Port Filtering**

Port Range: 80 - 80 **Protocol:** TCP **Comment:** HTTP

Now the port filter that you created has been added and listed in the Current Filter Table.

Now the TCP port for both Outbound and Inbound packet has been denied.



Current Filter Table:

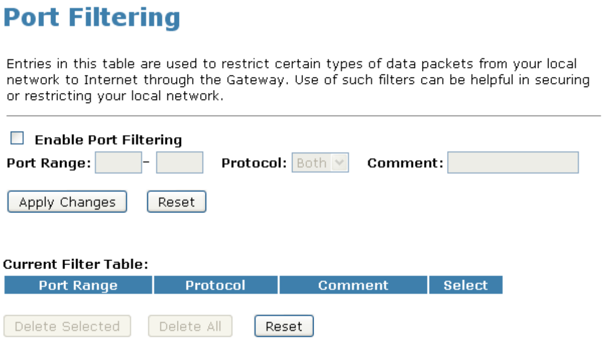
Port Range	Protocol	Comment	Select
80	TCP	HTTP	□

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.

From the left-hand Firewall -> Port Filtering menu. The following page is displayed:



Port 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.

□ **Enable Port Filtering**

Port Range: - **Protocol:** Both **Comment:**

Current Filter Table:

Port Range	Protocol	Comment	Select

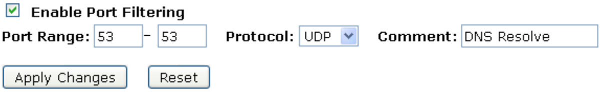
Check the option Enable Port Filtering to enable the port filtering.

Enter 53 and 53 in Port Range field.

From the Protocol drop-down list, select UDP setting.

Enter DNS Resolve in Comment field.

Click Apply Changes.

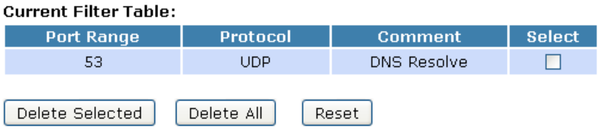


☑ **Enable Port Filtering**

Port Range: 53 - 53 **Protocol:** UDP **Comment:** DNS Resolve

Now the port filter that you created has been added and listed in the Current Filter Table.

Now the UDP port 80 for both Outbound and Inbound packet has been denied.



Current Filter Table:

Port Range	Protocol	Comment	Select
53	UDP	DNS Resolve	□

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.

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.

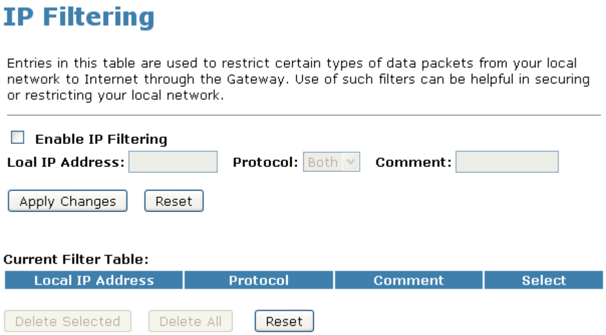
You can create IP filter rules to block attempts by certain computers on your LAN to access certain types of data or Internet locations. You can also block accesses to your LAN computers from the WAN side.

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.

From the left-hand Firewall -> IP Filtering menu. The following page is displayed:



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.

□ Enable IP Filtering

Loal IP Address: Protocol: Both Comment:

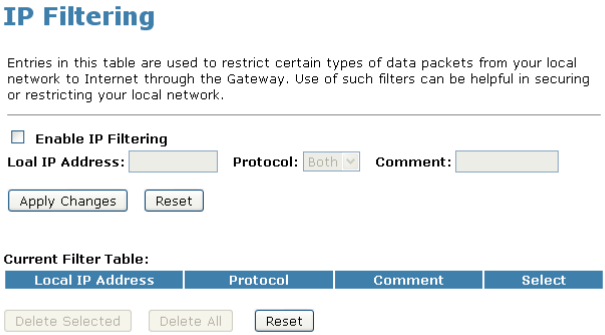
Current Filter Table:

Local IP Address	Protocol	Comment	Select

IP filtering for TCP with specified IP

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

From the left-hand Firewall -> IP Filtering menu. The following page is displayed:



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.

□ **Enable IP Filtering**

Loal IP Address: ____ **Protocol:** Both **Comment:** ____

Current Filter Table:

Local IP Address	Protocol	Comment	Select

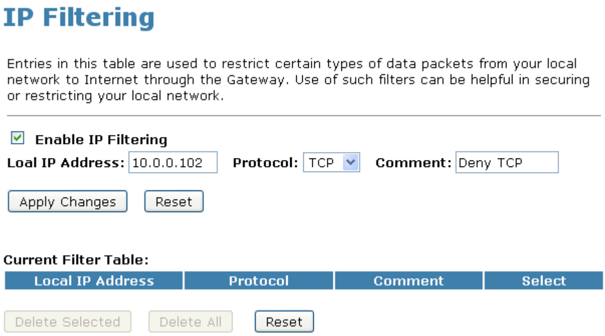
Check the option Enable IP Filtering to enable the IP Filtering.

Enter the IP Address that you want to be denied in Loal IP Address field.

From the Protocol drop-down list, select TCP setting.

Enter any comment in Comment field.

Click Apply Changes.



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.

☑ **Enable IP Filtering**

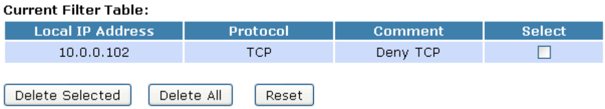
Loal IP Address: 10.0.0.102 **Protocol:** TCP **Comment:** Deny TCP

Current Filter Table:

Local IP Address	Protocol	Comment	Select

Now the IP Filter that you created has been added and listed in the Current Filter Table.

Now the TCP protocol for both Outbound and Inbound packet has been denied.



Current Filter Table:

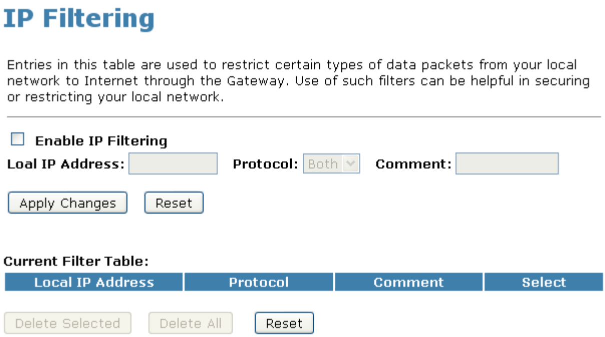
Local IP Address	Protocol	Comment	Select
10.0.0.102	TCP	Deny TCP	□

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.

From the left-hand Firewall -> IP Filtering menu. The following page is displayed:



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.

□ **Enable IP Filtering**

Loal IP Address: ______ **Protocol:** Both **Comment:** ______

Current Filter Table:

Local IP Address	Protocol	Comment	Select

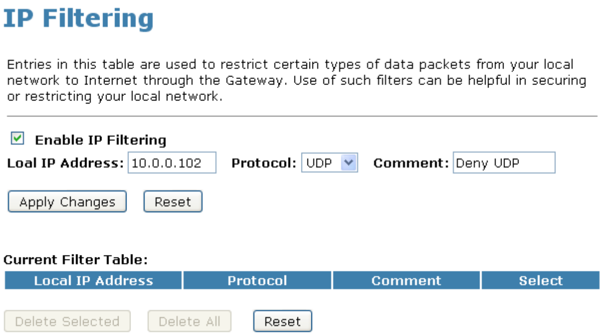
Check the option Enable IP Filtering to enable the IP Filtering.

Enter the IP Address that you want to be denied in Loal IP Address field.

From the Protocol drop-down list, select UDP setting.

Enter any comment in Comment field.

Click Apply Changes.



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.

☑ **Enable IP Filtering**

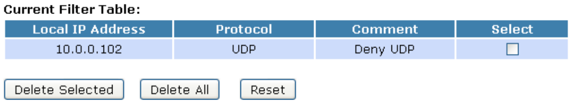
Loal IP Address: 10.0.0.102 **Protocol:** UDP **Comment:** Deny UDP

Current Filter Table:

Local IP Address	Protocol	Comment	Select

Now the IP Filter that you created has been added and listed in the Current Filter Table.

Now the UDP protocol for both Outbound and Inbound packet has been denied.



Current Filter Table:

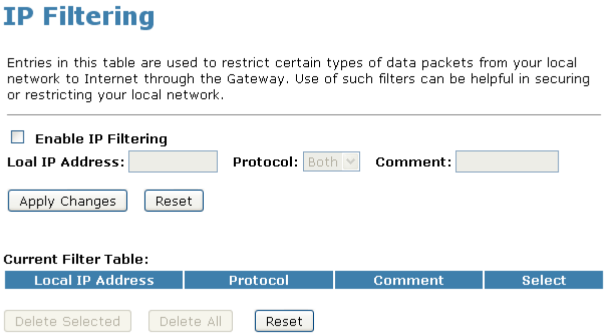
Local IP Address	Protocol	Comment	Select
10.0.0.102	UDP	Deny UDP	□

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.

From the left-hand Firewall -> IP Filtering menu. The following page is displayed:



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.

□ **Enable IP Filtering**

Loal IP Address: ______ **Protocol:** Both **Comment:** ______

Apply Changes   Reset

Current Filter Table:

Local IP Address	Protocol	Comment	Select

Delete Selected   Delete All   Reset

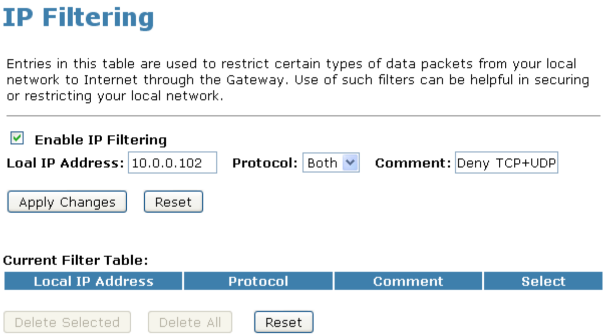
Check the option Enable IP Filtering to enable the IP Filtering.

Enter the IP Address that you want to be denied in Loal IP Address field.

From the Protocol drop-down list, select Both setting.

Enter any comment in Comment field.

Click Apply Changes.



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.

☑ **Enable IP Filtering**

Loal IP Address: 10.0.0.102 **Protocol:** Both **Comment:** Deny TCP+UDP

Apply Changes   Reset

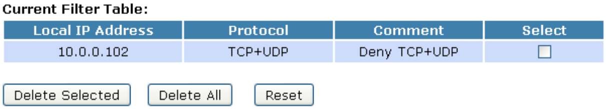
Current Filter Table:

Local IP Address	Protocol	Comment	Select

Delete Selected   Delete All   Reset

Now the IP Filter that you created has been added and listed in the Current Filter Table.

Now the TCP and UDP protocol for both Outbound and Inbound packet has been denied.



Current Filter Table:

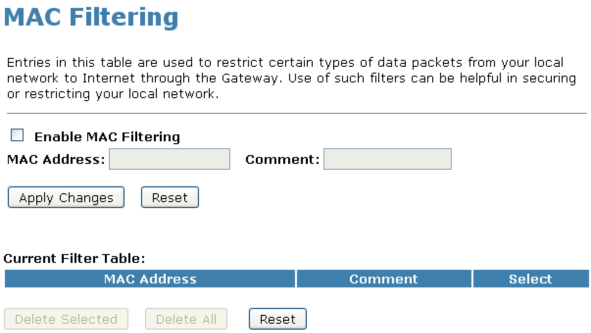
Local IP Address	Protocol	Comment	Select
10.0.0.102	TCP+UDP	Deny TCP+UDP	□

Delete Selected   Delete All   Reset

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.

From the left-hand Firewall -> MAC Filtering menu. The following page is displayed:



MAC 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.

□ Enable MAC Filtering

MAC Address: Comment:

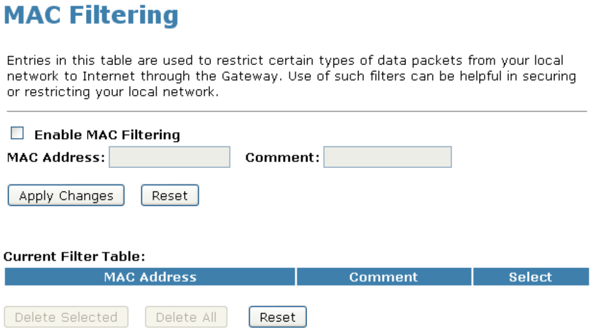
Current Filter Table:

MAC Address	Comment	Select

MAC filtering for specified MAC Address

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

From the left-hand Firewall -> MAC Filtering menu. The following page is displayed:



MAC 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.

□ Enable MAC Filtering

MAC Address: Comment:

Current Filter Table:

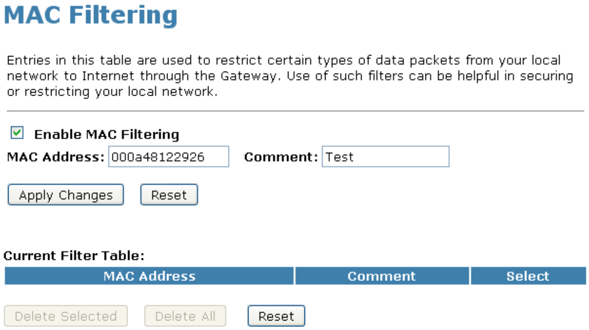
MAC Address	Comment	Select

Check the option Enable MAC Filtering to enable the MAC Filtering.

Enter the MAC Address that you want to be denied in MAC Address field.

Enter any comment in Comment field.

Click Apply Changes.



MAC 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.

☑ Enable MAC Filtering

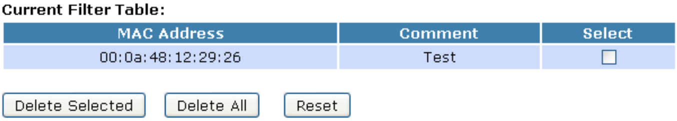
MAC Address: 000a48122926 Comment: Test

Current Filter Table:

MAC Address	Comment	Select

Now the MAC Filter that you created has been added and listed in the Current Filter Table.

Now the MAC Address in the Current Filter Table cannot have the Internet Access.



Current Filter Table:

MAC Address	Comment	Select
00:0a:48:12:29:26	Test	□

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:

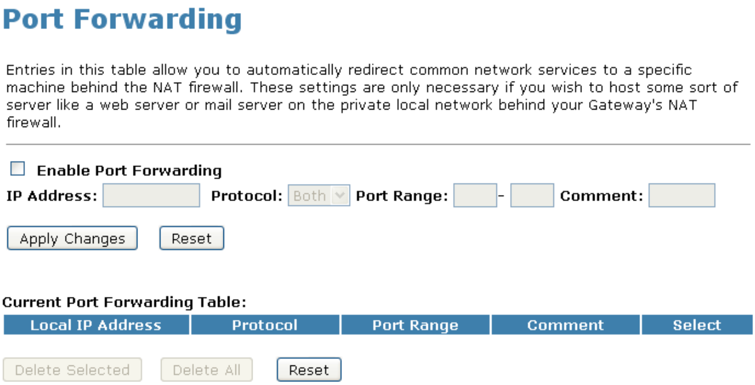
- allow Internet users to browse the user pages on your local network (for example, by providing an FTP or HTTP server)
- play certain games which require accessibility from the Internet

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.

From the left-hand Firewall -> Port Forwarding menu. The following page is displayed:



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.

□ Enable Port Forwarding

IP Address: ___ Protocol: Both Port Range: ___ - ___ Comment: ___

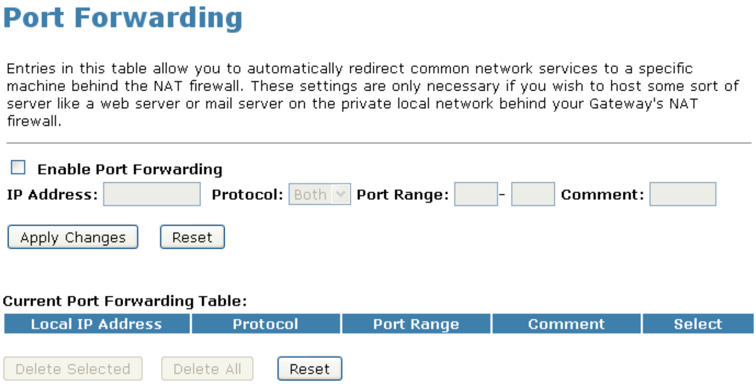
Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Port Forwarding for TCP with specified IP

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

From the left-hand Firewall -> Port Forwarding menu. The following page is displayed:



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.

☐ **Enable Port Forwarding**

IP Address: ____ **Protocol:** Both **Port Range:** ____ - ____ **Comment:** ____

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

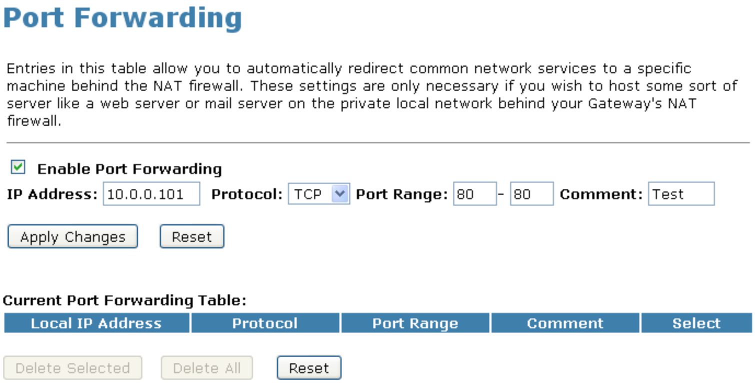
Check the option Enable Port Forwarding to enable the Enable Port Forwarding.

Enter the IP Address that the port you want to be forwarded in IP Address field.

From the Protocol drop-down list, select TCP setting.

Enter any comment in Comment field.

Click Apply Changes.



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.

☑ **Enable Port Forwarding**

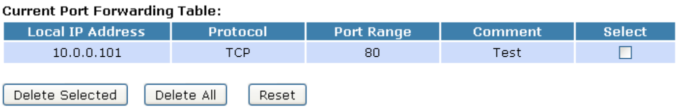
IP Address: 10.0.0.101 **Protocol:** TCP **Port Range:** 80 - 80 **Comment:** Test

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Now the IP Address and port range that you created has been added and listed in the Current Filter Table.

Now the port range of the IP Address in the Current Filter Table can be access from Internet by TCP protocol.



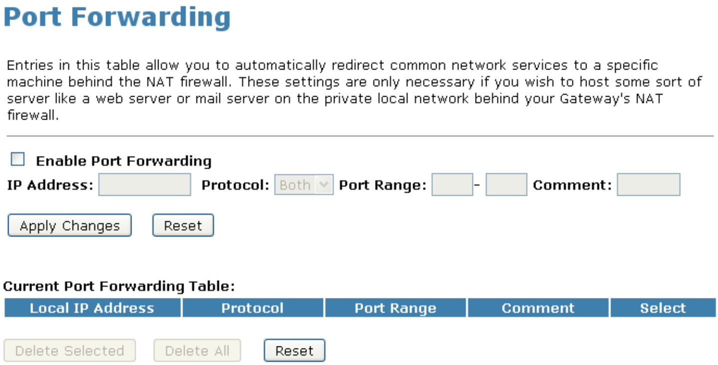
Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
10.0.0.101	TCP	80	Test	☐

Port Forwarding for UDP with specified IP

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

From the left-hand Firewall -> Port Forwarding menu. The following page is displayed:



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.

□ **Enable Port Forwarding**

IP Address: ____ **Protocol:** Both **Port Range:** ____ - ____ **Comment:** ____

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

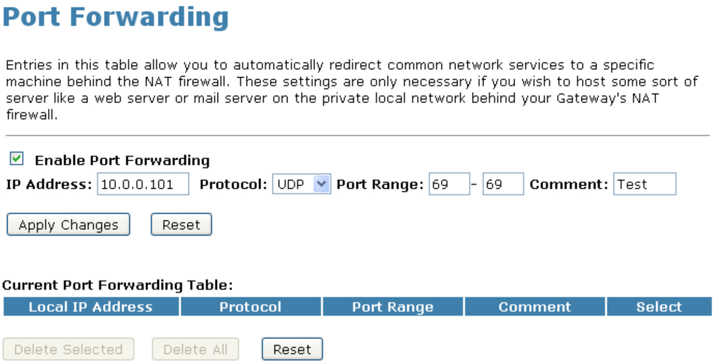
Check the option Enable Port Forwarding to enable the Enable Port Forwarding.

Enter the IP Address that the port you want to be forwarded in IP Address field.

From the Protocol drop-down list, select UDP setting.

Enter any comment in Comment field.

Click Apply Changes.



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.

☑ **Enable Port Forwarding**

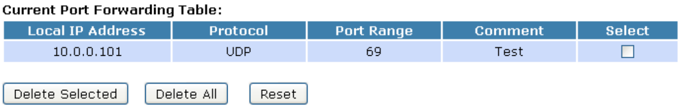
IP Address: 10.0.0.101 **Protocol:** UDP **Port Range:** 69 - 69 **Comment:** Test

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Now the IP Address and port range that you created has been added and listed in the Current Filter Table.

Now the port range of the IP Address in the Current Filter Table can be access from Internet by UDP protocol.



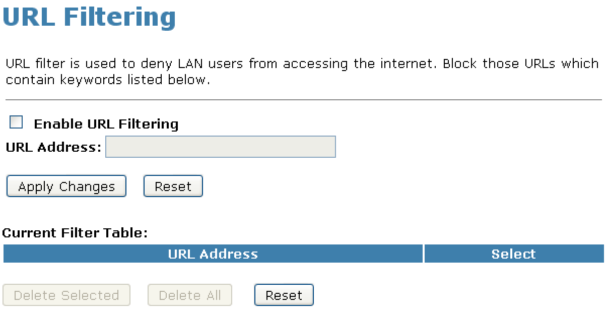
Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
10.0.0.101	UDP	69	Test	□

URL Filtering

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

From the left-hand Firewall -> URL Filtering menu. The following page is displayed:



URL Filtering

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

☐ Enable URL Filtering

URL Address:

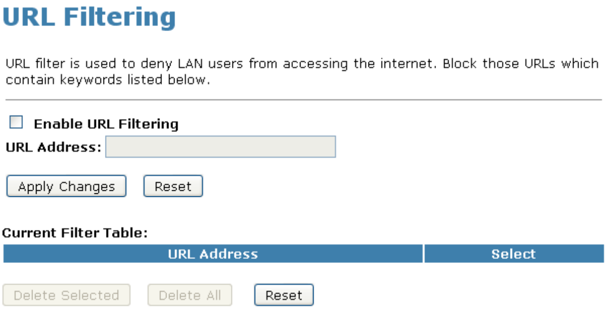
Current Filter Table:

URL Address	Select

URL filtering for specified URL Address

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

From the left-hand Firewall -> URL Filtering menu. The following page is displayed:



URL Filtering

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

☐ Enable URL Filtering

URL Address:

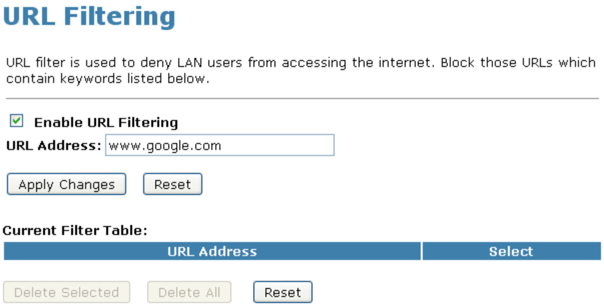
Current Filter Table:

URL Address	Select

Check the option Enable URL Filtering to enable the URL Filtering.

Enter the URL Address that you want to be denied for LAN user.

Click Apply Changes.



URL Filtering

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

☑ Enable URL Filtering

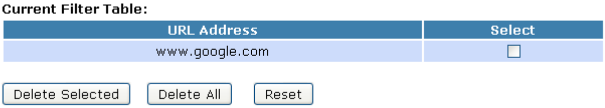
URL Address: www.google.com

Current Filter Table:

URL Address	Select

Now the URL Filter that you created has been added and listed in the Current Filter Table.

Now the URL Address in the Current Filter Table cannot be visited.



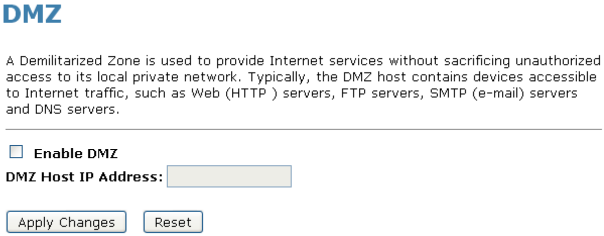
Current Filter Table:

URL Address	Select
www.google.com	□

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.

From the left-hand Firewall -> DMZ menu. The following page is displayed:



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.

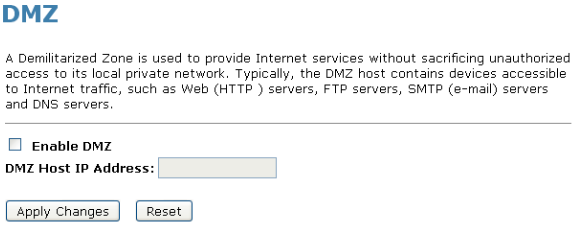
□ Enable DMZ

DMZ Host IP Address:

DMZ Host IP Address

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

From the left-hand Firewall -> DMZ menu. The following page is displayed:



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.

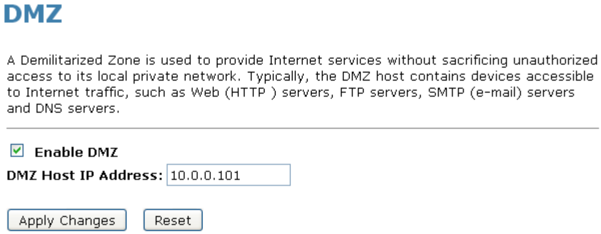
□ Enable DMZ

DMZ Host IP Address:

Check the option Enable DMZ to enable the Enable DMZ.

Enter the IP Address that to be the DMZ Host in DMZ Host IP Address field.

Click Apply Changes.



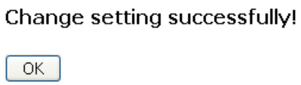
DMZ

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.

☑ Enable DMZ

DMZ Host IP Address: 10.0.0.101

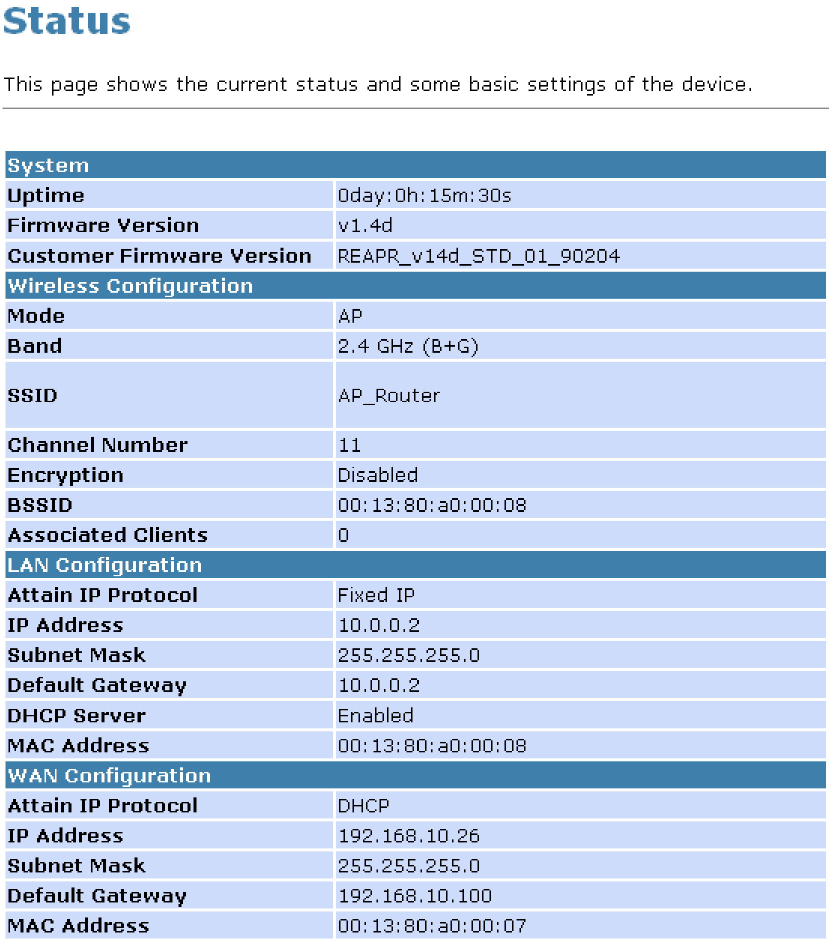
Click OK.


Change setting successfully!

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).

From the left-hand Management -> Status menu. The following page is displayed:


Status

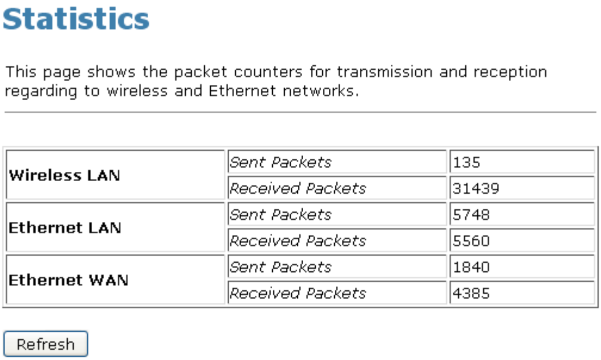
This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:15m:30s
Firmware Version	v1.4d
Customer Firmware Version	REAPR_v14d_STD_01_90204
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	AP_Router
Channel Number	11
Encryption	Disabled
BSSID	00:13:80:a0:00:08
Associated Clients	0
LAN 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	00:13:80:a0:00:08
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.26
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.100
MAC Address	00:13:80:a0:00:07

Statistics

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

From the left-hand Management -> Statistics menu. The following page is displayed:



Statistics

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

Wireless LAN	*Sent Packets*	135
	Received Packets	31439
Ethernet LAN	*Sent Packets*	5748
	Received Packets	5560
Ethernet WAN	*Sent Packets*	1840
	Received Packets	4385

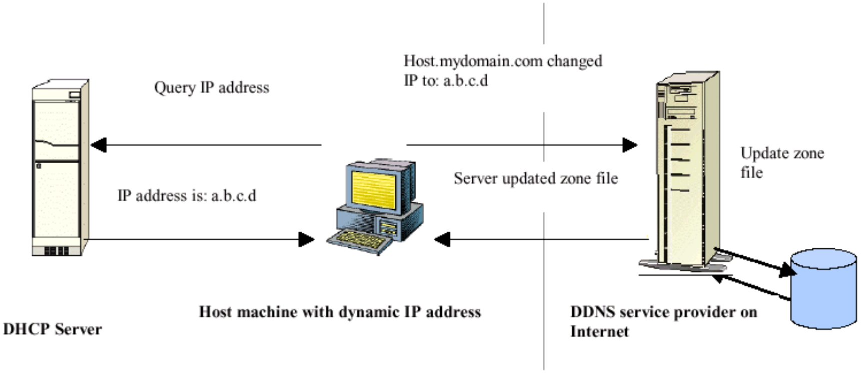
Dynamic DNS

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 configuration details related to it.

Overview

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



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

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

Registering With Dynamic DNS Service Provider

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

Configuring IP Interfaces

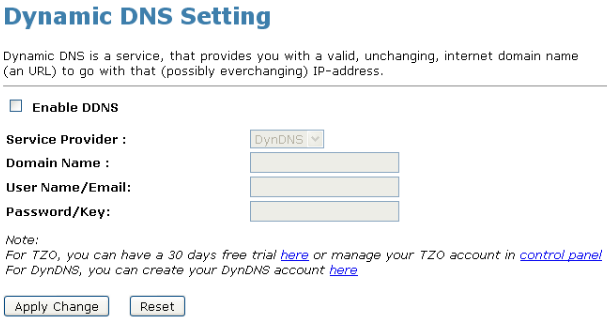
You need to create a Dynamic DNS interface per IP interface and can only create one Dynamic DNS interface service on one IP interface. For more information on creating IP interfaces, refer to section Creating IP interfaces.

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.

From the left-hand Management -> DDNS menu. The following page is displayed:



Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

☐ **Enable DDNS**

Service Provider : DynDNS

Domain Name :

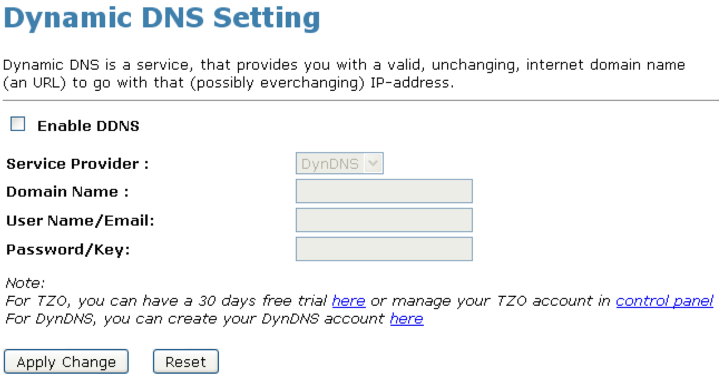
User Name/Email:

Password/Key:

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

Configure DynDNS

From the left-hand Management -> DDNS menu. The following page is displayed:



Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

□ Enable DDNS

Service Provider :	DynDNS
Domain Name :	
User Name/Email:	
Password/Key:	

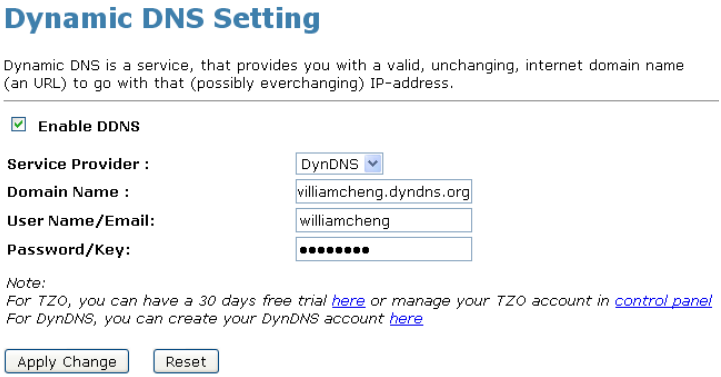
Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

Click on Enable DDNS

Select the DynDNS from the Service Provider drop-down list.

Type your own unique User Name, Password and Domain Name which you applied from www.dyndns.com in the relevant boxes. They can be any combination of letters or numbers with a maximum of 20 characters.

Click Apply Changes.



Dynamic DNS Setting

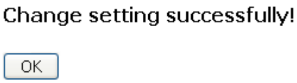
Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

☑ Enable DDNS

Service Provider :	DynDNS
Domain Name :	villiamcheng.dyndns.org
User Name/Email:	williamcheng
Password/Key:	●●●●●●●●●

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

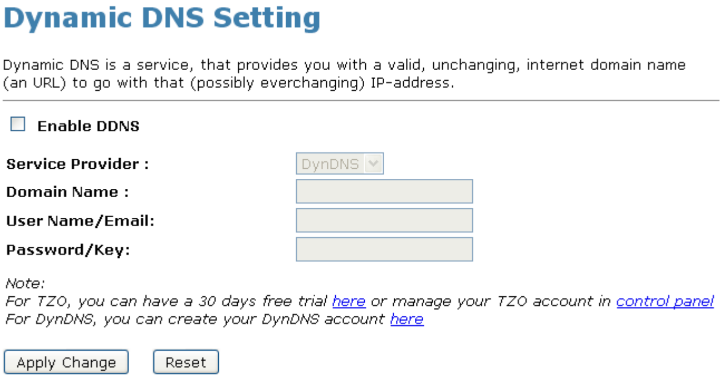
Click OK.



Change setting successfully!

Configure TZO

From the left-hand Management -> DDNS menu. The following page is displayed:



Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

□ Enable DDNS

Service Provider :	DynDNS
Domain Name :	
User Name/Email:	
Password/Key:	

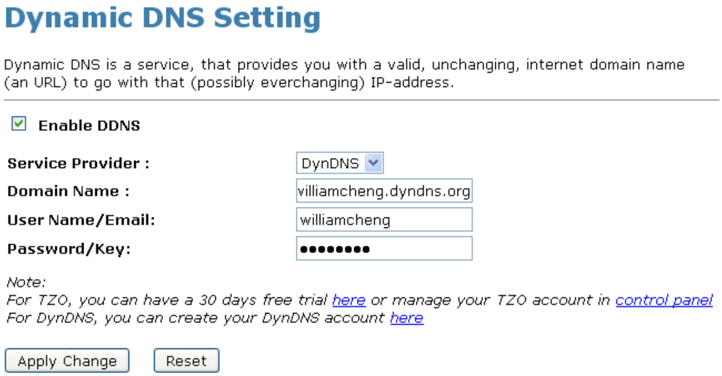
Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

Click on Enable DDNS

Select the TZO from the Service Provider drop-down list.

Type your own unique Email, Key and Domain Name which you applied from http://www.tzo.com/MainPageWebClient/clientsignup.html in the relevant boxes. They can be any combination of letters or numbers with a maximum of 20 characters.

Click Apply Changes.



Dynamic DNS Setting

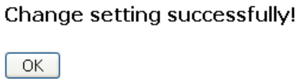
Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

☑ Enable DDNS

Service Provider :	DynDNS
Domain Name :	villiamcheng.dyndns.org
User Name/Email:	williamcheng
Password/Key:	●●●●●●●●●

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

Click OK.



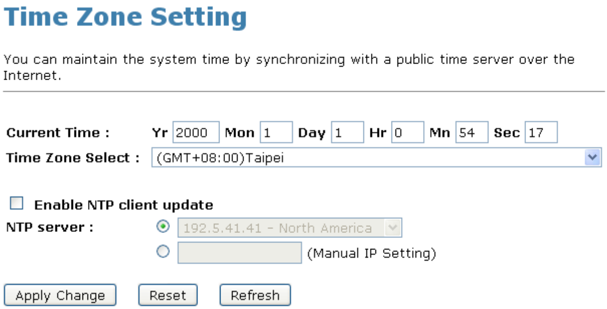
Change setting successfully!

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

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



Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr 2000 Mon 1 Day 1 Hr 0 Mn 54 Sec 17

Time Zone Select : (GMT+08:00)Taipei

□ Enable NTP client update

NTP server : ● 192.5.41.41 - North America

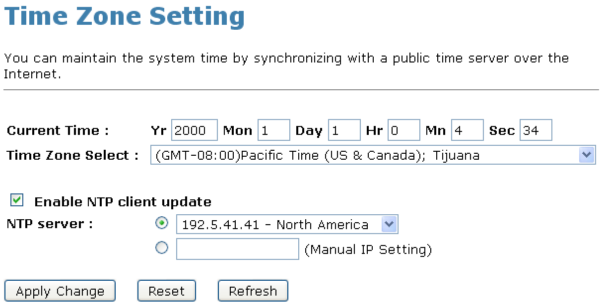
○ (Manual IP Setting)

From the Time Zone Select drop-down list, select Your Own Time Zone.

Check the option Enable NTP client update.

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.

Click Apply Changes.



Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr 2000 Mon 1 Day 1 Hr 0 Mn 4 Sec 34

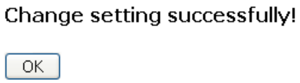
Time Zone Select : (GMT-08:00)Pacific Time (US & Canada); Tijuana

☑ Enable NTP client update

NTP server : ● 192.5.41.41 - North America

○ (Manual IP Setting)

Click OK.



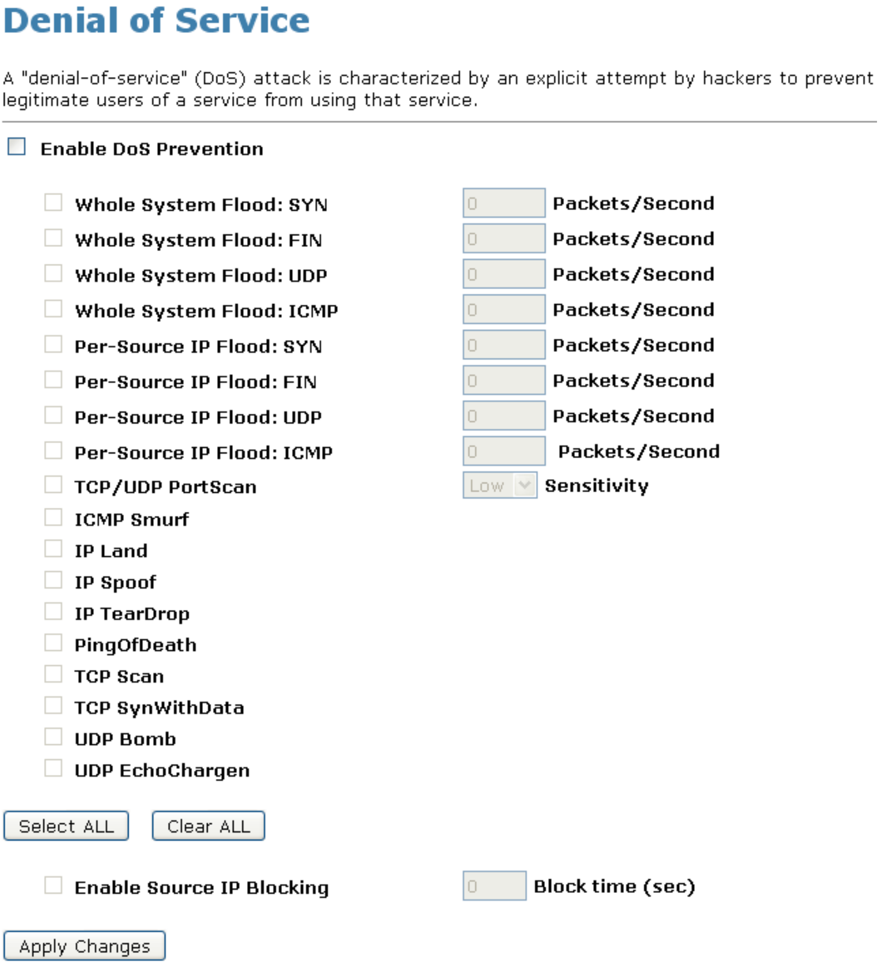
Change setting successfully!

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

From the left-hand Management menu, click on Denial-of-Service. The following page is displayed:



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.

□ Enable DoS Prevention

□ Whole System Flood: SYN	0	Packets/Second
□ Whole System Flood: FIN	0	Packets/Second
□ Whole System Flood: UDP	0	Packets/Second
□ Whole System Flood: ICMP	0	Packets/Second
□ Per-Source IP Flood: SYN	0	Packets/Second
□ Per-Source IP Flood: FIN	0	Packets/Second
□ Per-Source IP Flood: UDP	0	Packets/Second
□ Per-Source IP Flood: ICMP	0	Packets/Second
□ TCP/UDP PortScan	Low	Sensitivity
□ ICMP Smurf		
□ IP Land		
□ IP Spoof		
□ IP TearDrop		
□ PingOfDeath		
□ TCP Scan		
□ TCP SynWithData		
□ UDP Bomb		
□ UDP EchoChargen		

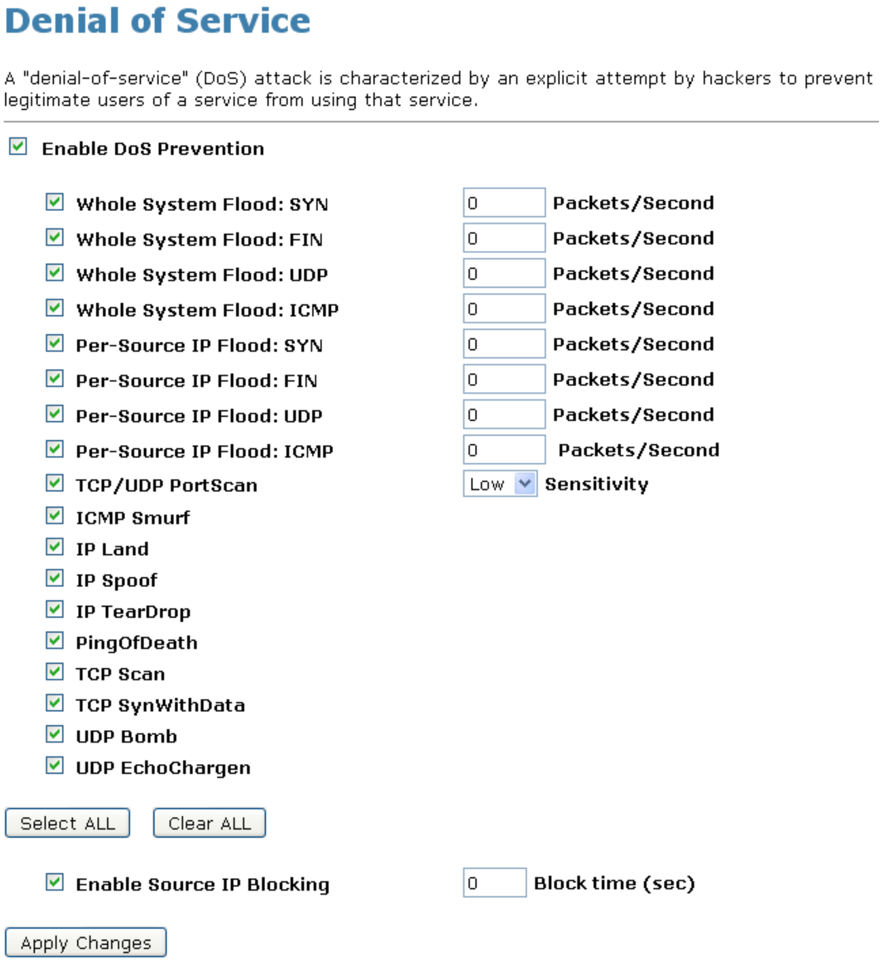
□ Enable Source IP Blocking 0 Block time (sec)

Check the option Enable NTP client update.

Check the option of each Service.

Check the option Enable Source IP Blocking.

Click Apply Changes.



Denial of Service

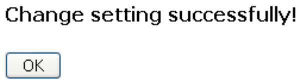
A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

☑ Enable DoS Prevention

☑ Whole System Flood: SYN	0	Packets/Second
☑ Whole System Flood: FIN	0	Packets/Second
☑ Whole System Flood: UDP	0	Packets/Second
☑ Whole System Flood: ICMP	0	Packets/Second
☑ Per-Source IP Flood: SYN	0	Packets/Second
☑ Per-Source IP Flood: FIN	0	Packets/Second
☑ Per-Source IP Flood: UDP	0	Packets/Second
☑ Per-Source IP Flood: ICMP	0	Packets/Second
☑ TCP/UDP PortScan	Low	Sensitivity
☑ ICMP Smurf		
☑ IP Land		
☑ IP Spoof		
☑ IP TearDrop		
☑ PingOfDeath		
☑ TCP Scan		
☑ TCP SynWithData		
☑ UDP Bomb		
☑ UDP EchoChargen		

☑ Enable Source IP Blocking	0	Block time (sec)

Click OK.



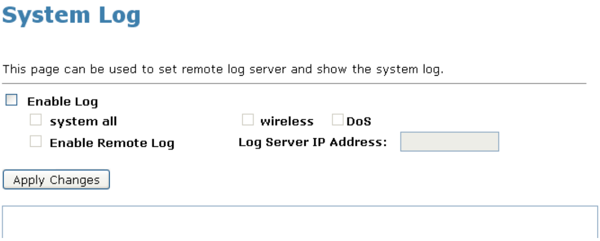
Change setting successfully!

Log

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

System Log

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



System Log

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

☐ Enable Log

☐ system all ☐ wireless ☐ DoS

☐ Enable Remote Log Log Server IP Address:

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.

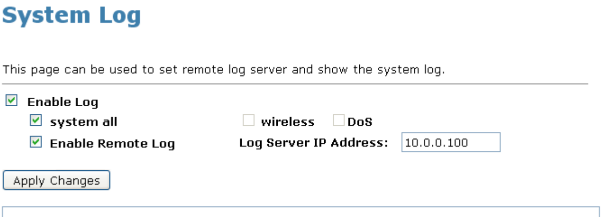
Check the option Enable Log.

Check the option system all, wireless or DoS.

Check the option Enable Remote Log if you

Enter the IP Address in the Log Server IP Address field.

Click Apply Changes.



System Log

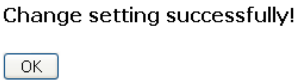
This page can be used to set remote log server and show the system log.

☑ Enable Log

☑ system all ☐ wireless ☐ DoS

☑ Enable Remote Log Log Server IP Address: 10.0.0.100

Click OK.



Change setting successfully!

Firmware Update

The Firmware Update page allows you to:

check if an updated firmware version is available from [Provider].

download an updated firmware version and install it on your device.

manually download the latest firmware version from [Provider]'s website and manually update your firmware. See Manually updating firmware.

About firmware versions

Firmware is a software program. It is stored as read-only memory on your device. [Provider] is continually improving this firmware by adding new features to it, and these features are saved in later versions of the firmware.

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.

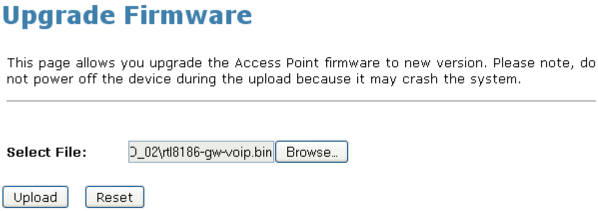
Manually updating firmware

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

Once you have downloaded the latest firmware version to your PC, you can manually select and install it as follows:

From the left-hand Management menu, click on Upgrade Firmware Upgrade. The following page is displayed:

Click on the Browse… button.



Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File: D_02\rtl8186-gw-voip.bin

(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.

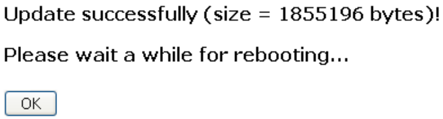
Once you have selected the file to be installed, click Open. The file's directory path is displayed in the New Firmware Image: text box.

Click Upgrade >. The device checks that the selected file contains an updated version of firmware. A status screen pops up, please wait for a while…….

Please wait...

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

Click OK.



Update successfully (size = 1855196 bytes)!

Please wait a while for rebooting...

Save/Reload Settings

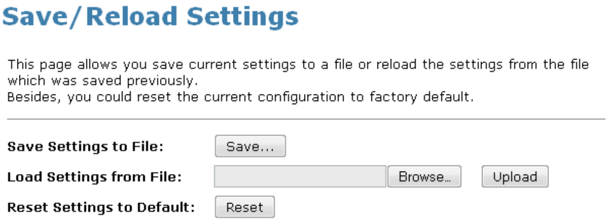
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

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.

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



Save/Reload Settings

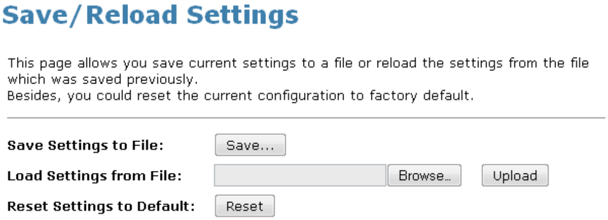
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.

Save Settings to File: Save...
Load Settings from File: Browse... Upload
Reset Settings to Default: Reset

Reset to Defaults page

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

Click on Save….

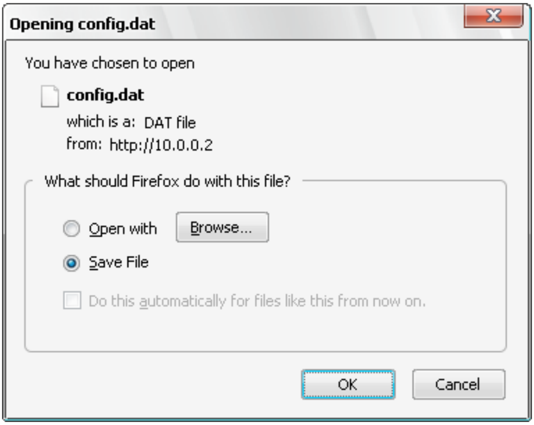


Save/Reload Settings

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.

Save Settings to File: Save...
Load Settings from File: Browse... Upload
Reset Settings to Default: Reset

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



Opening config.dat

You have chosen to open

config.dat
which is a: DAT file
from: http://10.0.0.2

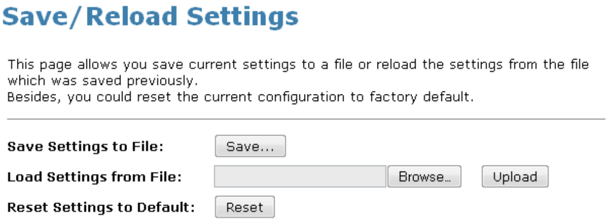
What should Firefox do with this file?

○ Open with Browse...
● Save File
□ Do this automatically for files like this from now on.

Load Settings from File

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

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



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.

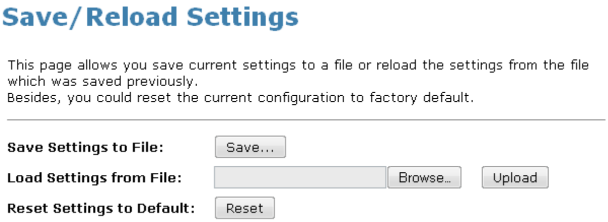
Save Settings to File: Save...

Load Settings from File: Browse... Upload

Reset Settings to Default: Reset

Reset to Defaults page

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



Save/Reload Settings

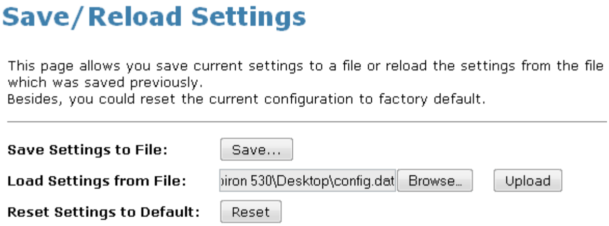
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.

Save Settings to File: Save...

Load Settings from File: Browse... Upload

Reset Settings to Default: Reset

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



Save/Reload Settings

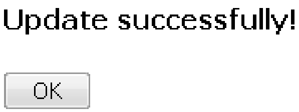
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.

Save Settings to File: Save...

Load Settings from File: ɔiron 530\Desktop\config.dat Browse... Upload

Reset Settings to Default: Reset

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



Update successfully!

OK

Resetting to Defaults

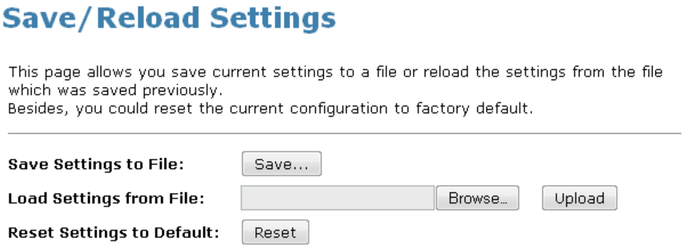
If you do make changes to the default configuration but then wish to revert back to the original factory configuration, you can do so by resetting the device to factory defaults.

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:

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



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.

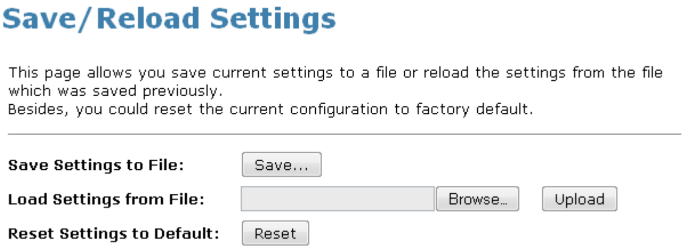
Save Settings to File:

Load Settings from File:

Reset Settings to Default:

Reset to Defaults page

Click on Reset Settings to Default.



Save/Reload Settings

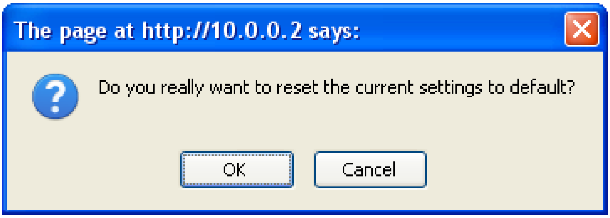
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

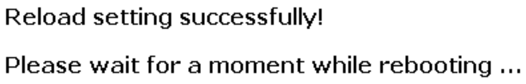
This page reminds you that resetting to factory defaults cannot be undone – any changes that you have made to the basic settings will be replaced. If you are happy with this, click OK. Or click Cancel to cancel it.



The page at http://10.0.0.2 says:

Do you really want to reset the current settings to default?

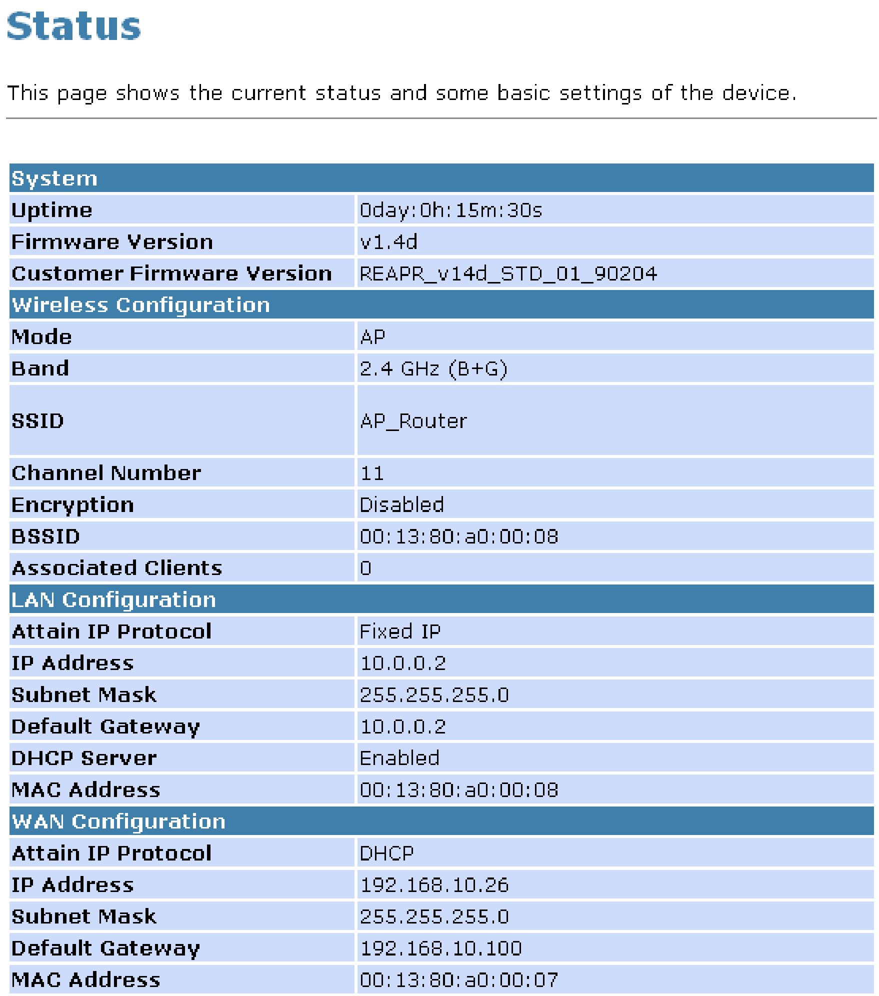
Reload setting successfully! Please wait for a moment while rebooting ...



Reload setting successfully!

Please wait for a moment while rebooting ...

Once it finished resetting to factory, it'll show the Status page.



Status

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

System	
Uptime	0day:0h:15m:30s
Firmware Version	v1.4d
Customer Firmware Version	REAPR_v14d_STD_01_90204
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	AP_Router
Channel Number	11
Encryption	Disabled
BSSID	00:13:80:a0:00:08
Associated Clients	0
LAN 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	00:13:80:a0:00:08
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.26
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.100
MAC Address	00:13:80:a0:00:07

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

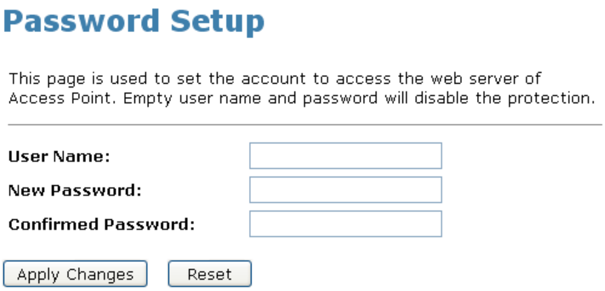
Setting your username and password

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:

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



Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:

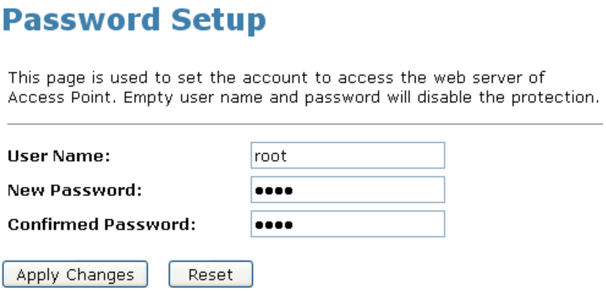
New Password:

Confirmed Password:

Currently Defined Administration Password: Setup page

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.

If you are happy with these settings, click 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 username and new password.



Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

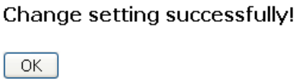
User Name: root

New Password: ●●●●

Confirmed Password: ●●●●

Administration Password

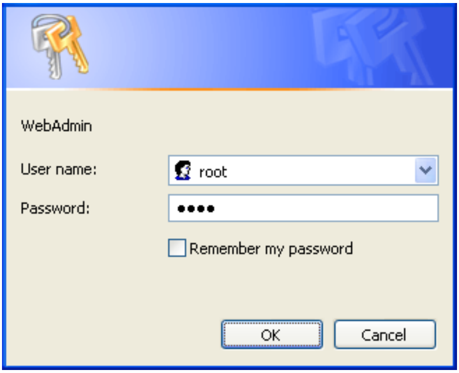
Click OK.



Change setting successfully!

Enter new User name and Password.

Click Apply.



WebAdmin

User name: root

Password: ●●●●

□ Remember my password

Logout

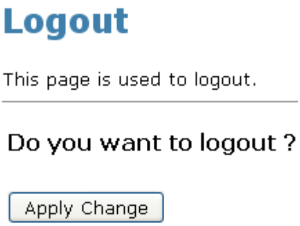
This page is used to logout.

Logout

To logout:

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

Click Apply Change.



Logout

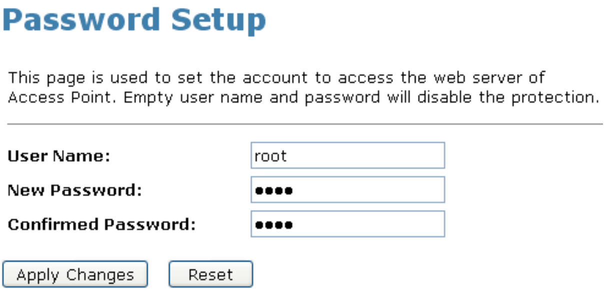
This page is used to logout.

Do you want to logout ?

Logout page

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.

If you are happy with these settings, click 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 username and new password.



Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

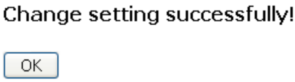
User Name: root

New Password: ●●●●

Confirmed Password: ●●●●

Administration Password

If you want to login the web page again, please click OK.



Change setting successfully!

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

In the Windows task bar, click the Start button, and then click Control Panel.

Double-click the Network Connections icon.

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.

Ensure that the check box to the left of the item labeled Internet Protocol TCP/IP is checked and click Properties.

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.

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:

In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.

Double-click the Network and Dial-up Connections icon.

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.

If Internet Protocol (TCP/IP) does not display as an installed component, click Install…

In the Select Network Component Type dialog box, select Protocol, and then click Add…

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.

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:

In the Control Panel, double-click the Network and Dial-up Connections icon.

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

In the Local Area Connection Properties dialog box, select Internet Protocol (TCP/IP), and then click Properties.

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.

Click OK twice to confirm and save your changes, and then close the Control Panel.

Windows Me PCs

In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.

Double-click the Network and Dial-up Connections icon.

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.

If Internet Protocol (TCP/IP) does not display as an installed component, click Add…

In the Select Network Component Type dialog box, select Protocol, and then click Add…

Select Microsoft in the Manufacturers box.

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.

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:

In the Control Panel, double-click the Network and Dial-up Connections icon.

In Network and Dial-up Connections window, right-click the Network icon, and then select Properties.

In the Network Properties dialog box, select TCP/IP, and then click Properties.

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.

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:

In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.

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.

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

The Select Network Component Type dialog box displays.

Select Protocol, and then click Add…

The Select Network Protocol dialog box displays.

Click on Microsoft in the Manufacturers list box, and then click TCP/IP in the Network Protocols list box.

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.

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:

Open the Control Panel window, and then click the Network icon.

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.

In the TCP/IP Properties dialog box, click the IP Address tab.

Click the radio button labeled Obtain an IP address automatically.

Click the DNS Configuration tab, and then click the radio button labeled Obtain an IP address automatically.

Click OK twice to confirm and save your changes.

You will be prompted to restart Windows.

Click Yes.

Windows NT 4.0 workstations

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

In the Windows NT task bar, click the Start button, point to Settings, and then click Control Panel.

In the Control Panel window, double click the Network icon.

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.

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

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.

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:

Open the Control Panel window, and then double-click the Network icon.

In the Network dialog box, click the Protocols tab.

In the Protocols tab, select TCP/IP, and then click Properties.

In the Microsoft TCP/IP Properties dialog box, click the radio button labeled Obtain an IP address from a DHCP server.

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.

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.

UPnP Control Point Software on Windows ME/XP

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

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

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

UPnP Control Point Software on Windows ME

To install the control point software on Windows ME:

1. In the Control Panel, select "Add/Remove Programs".
2. In the "Add/Remove Programs Properties" dialog box, select the "Windows Setup" tab. In the "Components" list, double click on the "Communications" entry.
3. In the "Communications" dialog box, scroll down the "Components" list to display the UPnP entry. Select the entry, click "OK".
4. Click "OK" to finish the "Add/Remove Programs" dialog.
5. Reboot your system.

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

UPnP Control Point Software on Windows XP with Firewall

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

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

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

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

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

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

5. Click "OK".

SSDP requirements

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

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

Installation procedure

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

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

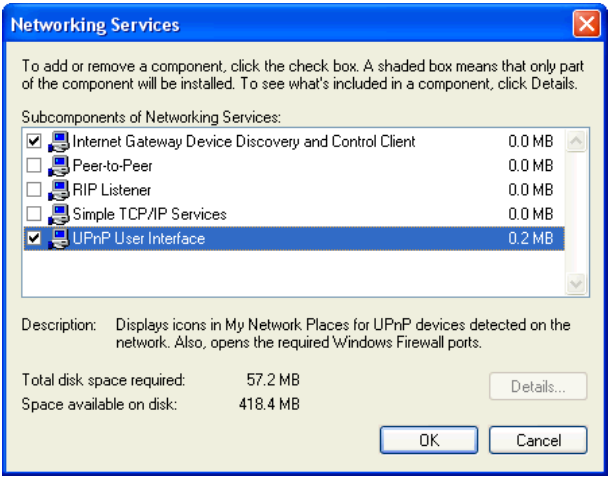
2. In the "Add or Remove Programs" dialog box, click the "Add / Remove Windows Components" button.

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

4. The "Networking Services" window is displayed.

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

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



Networking Services

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

Subcomponents of Networking Services:

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

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

Total disk space required: 57.2 MB

Space available on disk: 418.4 MB

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

If you are using Windows XP, select:

- "Universal Plug and Play".

If you are using Windows XP SP1, select:

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

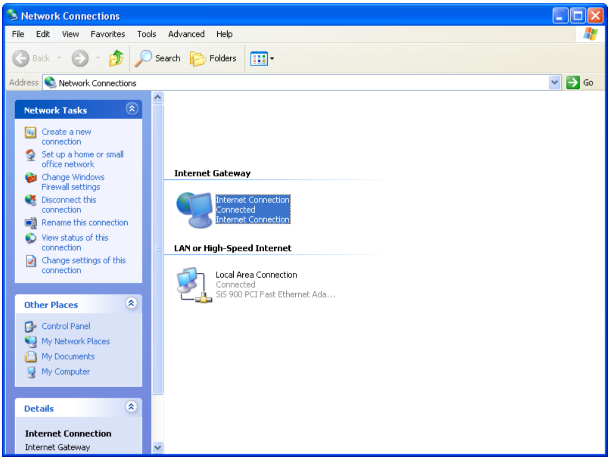
If you are using Windows XP SP2, select:

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

6. Reboot your system.

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

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



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.

Problem	Troubleshooting Suggestion
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	
I forgot/lost my user ID or pasword.	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.

Diagnosing Problem using IP Utilities

ping

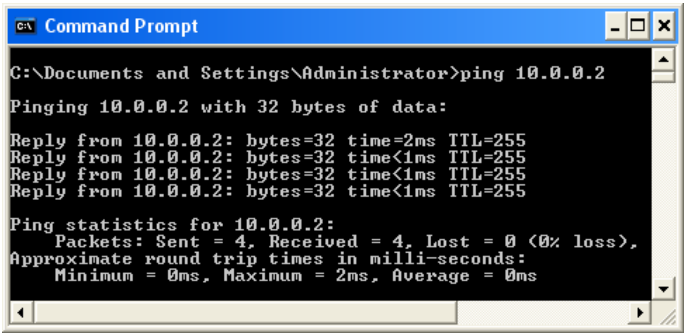
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer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

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

ping 10.0.0.2

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:



```
C:\Documents and Settings\Administrator>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=2ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

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

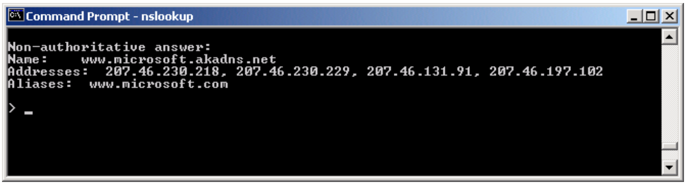
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then 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:



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

> _
```

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.

Glossary

10BASE-T

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

100BASE-T

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

ADSL

Asymmetric Digital Subscriber Line

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

analog

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

ATM

Asynchronous Transfer Mode

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

authenticate

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

binary

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

bit

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

bps

bits per second

bridging

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

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

broadcast To send data to all computers on a network.

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

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

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

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

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

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

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

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

encryption keys
See network keys

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

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

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

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

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

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

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

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

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

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

IP
See TCP/IP.

IP address

Internet Protocol address

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

ISP

Internet Service Provider

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

LAN

Local Area Network

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

LED

Light Emitting Diode

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

MAC address

Media Access Control address

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

mask

See network mask.

Mbps

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

NAT

Network Address Translation

A service performed by many routers that translates your network's publicly known IP address into a private IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.

network

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

network mask

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

NIC

Network Interface Card

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

packet

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

ping

Packet Internet (or Inter-Network) Groper

A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.

port

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

PPP

Point-to-Point Protocol

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

PPPoA

Point-to-Point Protocol over ATM

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

PPPoE

Point-to-Point Protocol over Ethernet

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

protocol

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

remote

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

RIP

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

RJ-11

Registered Jack Standard-11
The standard plug used to connect telephones, fax machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.

RJ-45

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

routing

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

SDNS

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

subnet

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

subnet mask

A mask that defines a subnet. See network mask.

TCP

See TCP/IP.

TCP/IP

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

Telnet

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

TFTP

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

TKIP

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

triggers

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

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

twisted pair

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

unnumbered interfaces

An unnumbered interface is an IP interface that does not have a local subnet associated with it. Instead, it uses a router-id that serves as the source and destination address of packets sent to and from the router. Unlike the IP address of a normal interface, the router-id of an unnumbered interface is allowed to be the same as the IP address of another interface. For example, the WAN unnumbered interface of your device uses the same IP address of the LAN interface (10.0.0.2).

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

upstream

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

VC

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

VCI

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

VPI

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

WAN

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

Web browser

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

Web page

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

Web site

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

WWW

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

Environment protection:

This symbol on our product nameplates proves its compatibility with the EU Directive2002/96 concerning proper disposal of waste electric and electronic equipment (WEEE). By using the appropriate disposal systems you prevent the potential negative consequences of wrong product take-back that can pose risks to the environment and human health. The symbol indicates that this product must not be disposed of with your other waste. You must hand it over to a designated collection point for the recycling of electrical and electronic equipment waste. The disposal of the product should obey all the specific Community waste management legislations. Contact your local city office, your waste disposal service or the place of purchase for more information on the collection. Weight of the device: 0,8 kg

MODECOM S.A.
00-124 Warszawa, Rondo ONZ 1.
www.modecom.eu

MODECOM