WIRELESS 300N ADSL2+ MODEM ROUTER

USER MANUAL

MODELS 524780 (ANNEX A), 524797 (ANNEX B)

INTELLINET™
NETWORK SOLUTIONS

INT-524780/524797-UM-1109-01

Federal Communications Commission Interference Statement

FCC Part 68

This equipment complies with Part 68 of the FCC Rules. On the bottom of this device is a label that contains the FCC registration number and ringer equivalence number (REN) for this equipment. You must provide this information to the telephone company upon request. The REN is useful to determine the quantity of devices you may connect to the telephone line and still have all of those devices ring when your number is called.

In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.
If the modem causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC.
The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper operation of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this modem, contact your dealer for repair/warranty information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected or you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

Installation

This device is equipped with a USOC RJ11C connector.

FCC Part 15

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

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

FCC Caution

This equipment must be installed and operated in accordance with provided instructions, and a minimum of 20 cm spacing must be provided between computer-mounted antenna and a person's body (excluding extremities of hands, wrists and feet) during wireless modes of operation.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: 1) This device may not cause harmful interference; and 2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding these limits, human proximity to the antenna shall not be less than 20 cm (8 inches)

during normal operation. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of Directive 1999/5/EC of the European Parliament and the Council of March 9, 1999, on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines must therefore be followed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway and Switzerland.

EU Countries Not Intended for Use

None.

Contents

1 INTRODUCTION 1

2 HARDWARE 3

3 SETUP WIZARD 6

3.1 Getting Started 6

3.2 Automatically Set the ISP 9

3.3 Manually Set the ISP 12

4 IP ADDRESS SETTING 17

Windows Vista 17

Windows XP 18

Windows 2000 19

5 WEB MANAGEMENT CONFIGURATION 21

5.1 Quick Setup 23

5.2 General Setup 25

5.2.1 System 25

5.2.1.1 Time Zone 25

5.2.1.2 Password Settings 26

5.2.1.3 Remote Management 27

5.2.1.4 SNMP 29

5.2.2 WAN 30

5.2.2.1 Channel Config 30

5.2.2.2 ATM Setting 34

5.2.2.3 ADSL Setting 36

5.2.2.4 DNS 37

5.2.2.5 DDNS 38

5.2.2.6 RIP 39

5.2.3 LAN 41

5.2.3.1 DHCP Mode 43

5.2.3.2 DHCP Relay 43

5.2.3.3 DHCP Server 44

5.2.3.4 ARP Table 46

5.2.3.5 Bridging 46

5.2.4 Wireless 47

5.2.4.1 Basic Settings 47

5.2.4.2 Advanced Settings 49
5.2.4.3 Security 53
5.2.4.4 Access Control 55
5.2.4.5 WPS 56
5.2.5 QoS 58
5.2.6 NAT (Network Address Translations) 60
5.2.6.1 Port Forwarding 61
5.2.6.2 Port Mapping 62
5.2.6.3 UPNP 64
5.2.6.4 IGMP Proxy 65
5.2.7 Firewall 66
5.2.7.1 IP/Port Filtering 66
5.2.7.2 MAC Filtering 68
5.2.7.3 URL Blocking 70
5.2.7.4 Domain Blocking 71
5.2.7.5 Routing Configuration 72
5.2.7.6 ACL Configuration 74
5.2.7.7 DMZ 75
5.3 Status 76
5.3.1 Interface 77
5.3.2 ADSL 78
5.4 Tools 79
5.4.1 Configuration Tools 79
5.4.2 Firmware Upgrade 80
5.4.3 Ping 80
5.4.4 ATM Loopback 81
5.4.5 Diagnostic Test 82
5.4.6 Reboot 82
6 TROUBLESHOOTING 83
7 GLOSSARY 87
8 SPECIFICATIONS 92

1 Introduction

Thank you for purchasing this INTELLINET NETWORK SOLUTIONS™ Wireless 300N ADSL2+ Modem Router, Model 524780 (Annex A) or Model 524797 (Annex B).

This is an all-in-one modem, router, Wireless N access point, firewall and Fast Ethernet four-port switch that allows you to access the Internet and download music, play interactive games online or surf the Web at double the speed (depending on operating environment and distance between networked devices) previously available through ADSL2.

Features of this router include:

- 2T2R MIMO technology for enhanced throughput and coverage
- Supports ADSL standards G.992.1 (G.dmt), G.992.2 (G.lite), G.992.3 (ADSL2), G.992.4 (splitterless ADSL2) and G.992.5 (ADSL2+) for Annex A
- Supports 24 Mbps ADSL2+ downstream data rate
- Supports Wi-Fi Protected Setup (WPS)
- Supports WEP and WPA/WPA2 (TKIP and AES) data encryption
- Integrated 10/100 Mbps LAN switch with Auto MDI/MDI-X support
- DHCP server assigns IP addresses for all LAN users
- DHCP server supports static lease management
- Supports virtual server, port forwarding and DMZ
- Supports DDNS (dynamic DNS)
- Supports UPnP (Universal Plug and Play)
- Integrated SPI firewall
- QoS (Quality of Service) bandwidth management
- VPN Passthrough (PPTP, IPSec, L2TP)
- Supports SNMP management
- Easy installation through Web-based user interface
- Complies with 2.4 GHz Draft IEEE 802.11n standard and is backward compatible with IEEE 802.11g/b standards
- System status
- Security log
- Firmware upgradeable
- Lifetime Warranty

Ex.1017
CISCO SYSTEMS, INC. / Page 7 of 100

Minimum Requirements

- A PC with pre-installed Ethernet adapter (required) and a Web browser (Internet Explorer 4.0 or higher)
- RJ45 Ethernet crossover cable (included in the package)
- RJ11 (ADSL-ready) phone line

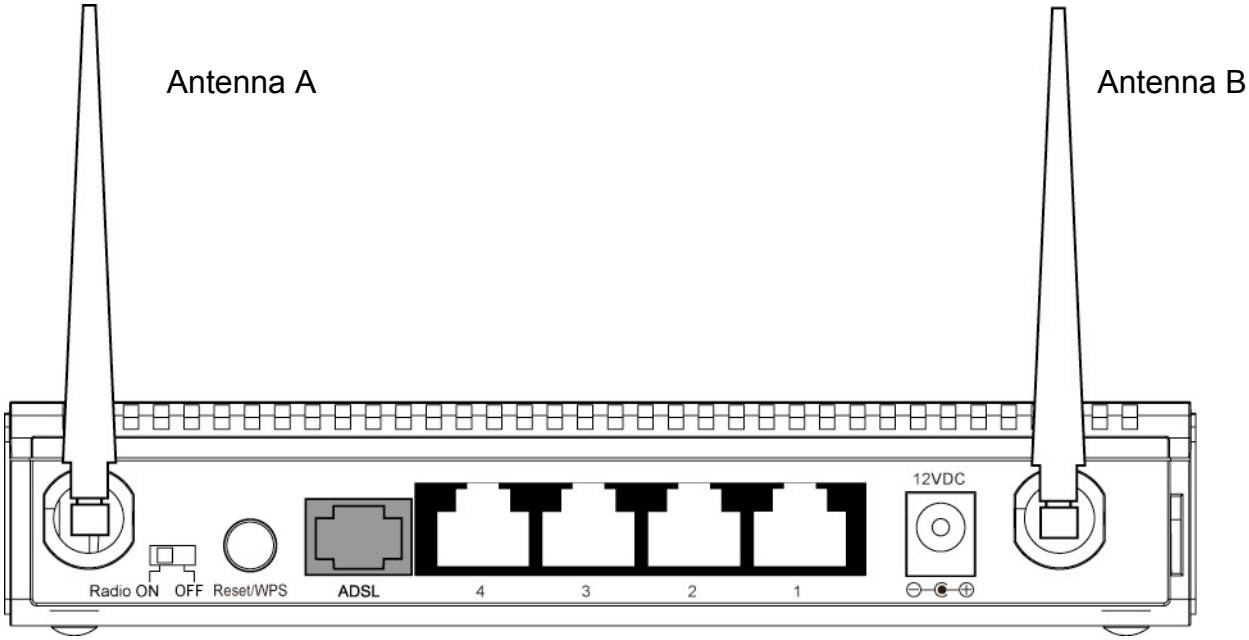
Package Contents

- ADSL 2+ Router (Annex A or B)
- Power adapter
- Ethernet Cat5 RJ45 cable, 1.0 m (3 ft.)
- RJ11 telephone cable, 1.8 m (5.9 ft.)
- Quick installation guide
- Setup CD with user manual

Ex.1017
CISCO SYSTEMS, INC. / Page 8 of 100

2 Hardware

Rear Panel

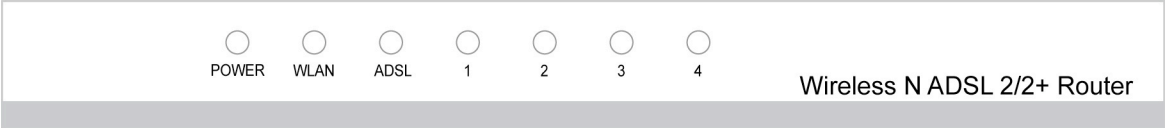


Item Name	Description
Antenna A/B	These antennas are 3dBi dipole antennas.
Radio ON/OFF	Position the switch to activate or deactivate the wireless functions.
Reset / WPS	Reset the router to factory default settings (clear all settings) or start the WPS function. Press this button and hold for 10 seconds to restore all settings to factory defaults; press this button for less than 5 seconds to start the WPS function.
1 - 4	The router's 4 LAN ports are where you connect your LAN's PCs, printer servers, hubs and switches, etc.
ADSL	Connect the supplied RJ11 telephone line to this port and your ADSL/telephone network.
Power	Plug the included power adapter into the power jack.

Ex.1017
CISCO SYSTEMS, INC. / Page 9 of 100

Front Panel

On the router's front panel, there are LEDs that inform you of the router's current status, as explained below.



LED	Status	Description
POWER (Green)	On	Router is switched on and correctly powered.
WLAN (Yellow)	On	Wireless LAN WPS is on.
	Off	Wireless LAN is disabled.
	Blinking	Wireless traffic is transmitting or receiving.
ADSL (Green)	On	Connected to an ADSL DSLAN successfully.
	Blinking	ADSL line is not connected to Internet.
LAN LNK/ACT (Port 1-4)	On	The LAN cable is connected to the router.
	Off	No network connection.
	Blinking	Network traffic transferring or receiving through the LAN port.

Ex.1017
CISCO SYSTEMS, INC. / Page 10 of 100

Installation

1. Connect the router to your ADSL cable through the supplied RJ11 cable.
2. Connect the router to your PC, hub or switch by attaching the Ethernet cable to the LAN port of the router.
3. Connect the power adapter to the power jack on the rear panel of the router.
4. The ADSL LED will be on if the router is connected to the ADSL cable and receives the ADSL signals successfully. If the LED is blinking, contact your ISP (Internet service provider) to check the problem.

NOTE: Use only the power adapter included with the router, and *not* any other power adapter.

Ex.1017
CISCO SYSTEMS, INC. / Page 11 of 100

3 Setup Wizard

This router provides a Setup Wizard tool to configure the ADSL settings. This wizard collects some ISPs' ADSL settings so that you can easily configure the router's ADSL settings by only selecting the ISP vendor from the wizard.
If you cannot find your ISP from the list in the wizard, manually set the ISP information through the wizard.

3.1 Getting Started

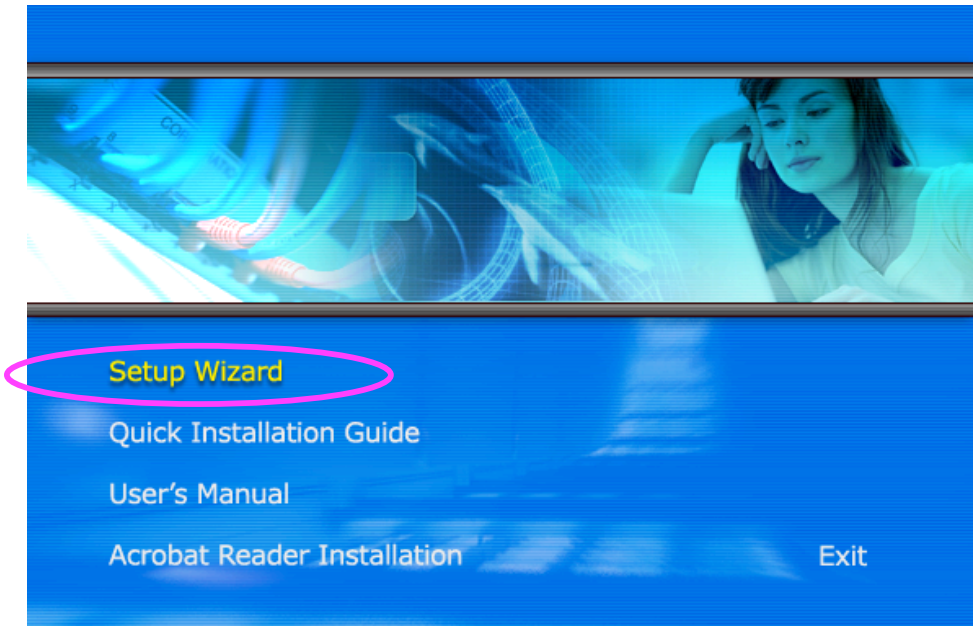
Before starting, check the following items:

1. Make sure that you have connected the ADSL cable to the router correctly. When the ADSL cable is worked normally, the ADSL LED will be on.
2. Un-install any dial-up programs installed previously for the USB modem or other dial-up devices.
3. It is recommended that you initially configure the router through the Ethernet cable before you set the wireless functions.

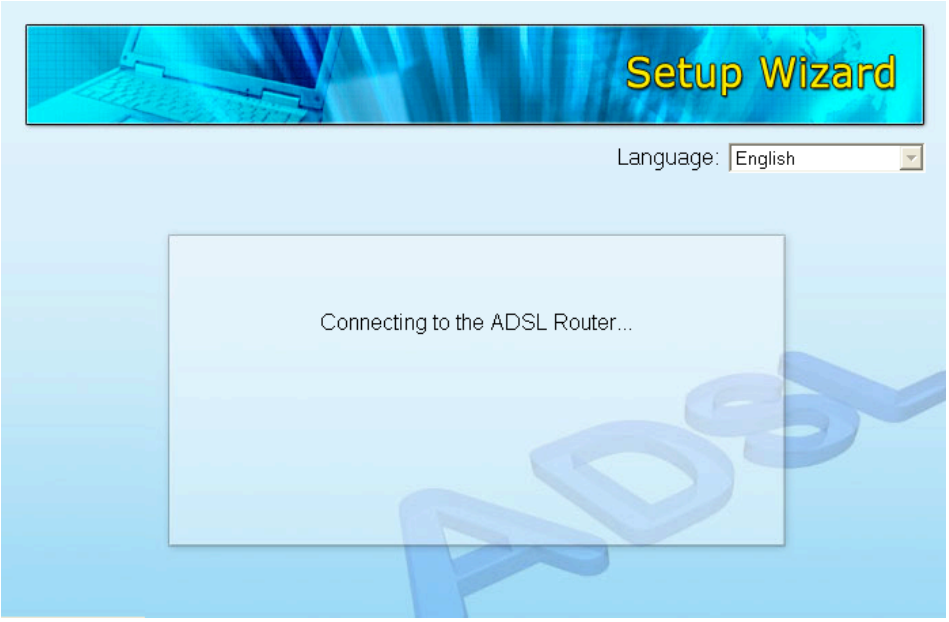
This wizard can be run in Windows 98SE/Me/2000/XP/Vista. The following procedures are operated in Windows XP. (Procedures are similar for Windows 98SE/Me/2000/Vista.)

1. Insert the enclosed setup CD into your CD-ROM drive. The Autorun.exe program should be executed automatically. If not, run Autorun.exe manually from the "Autorun" folder on the CD.
2. The following screen will be displayed. Click "Setup Wizard."

Ex.1017
CISCO SYSTEMS, INC. / Page 12 of 100



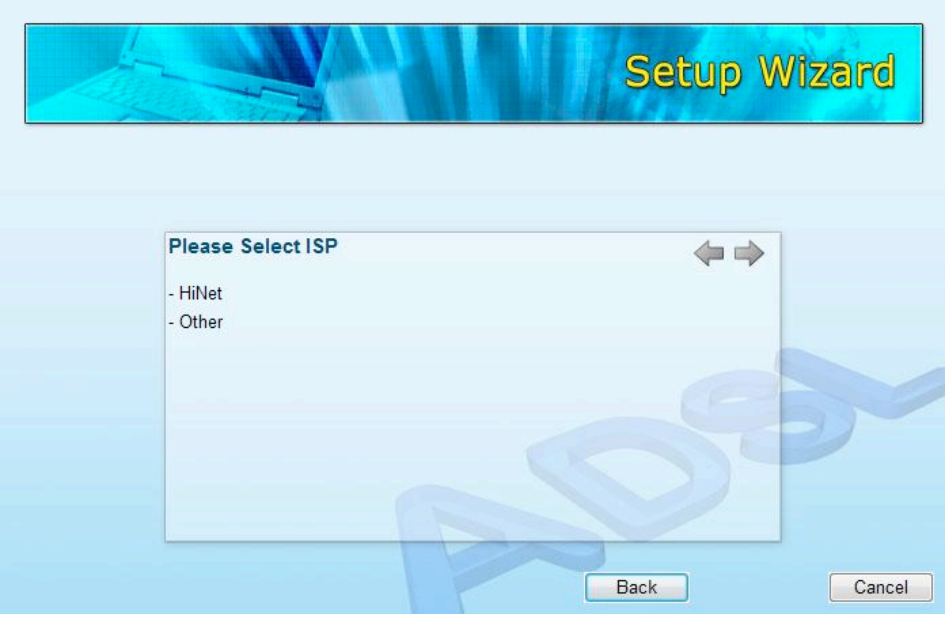
3. The wizard will run and try to search for the router. If the router is found, the wizard will guide you to Step 5.



Ex.1017
CISCO SYSTEMS, INC. / Page 13 of 100

4. If the router cannot be found, enter the IP address and the password of the router to search again. Click “Next” to continue.

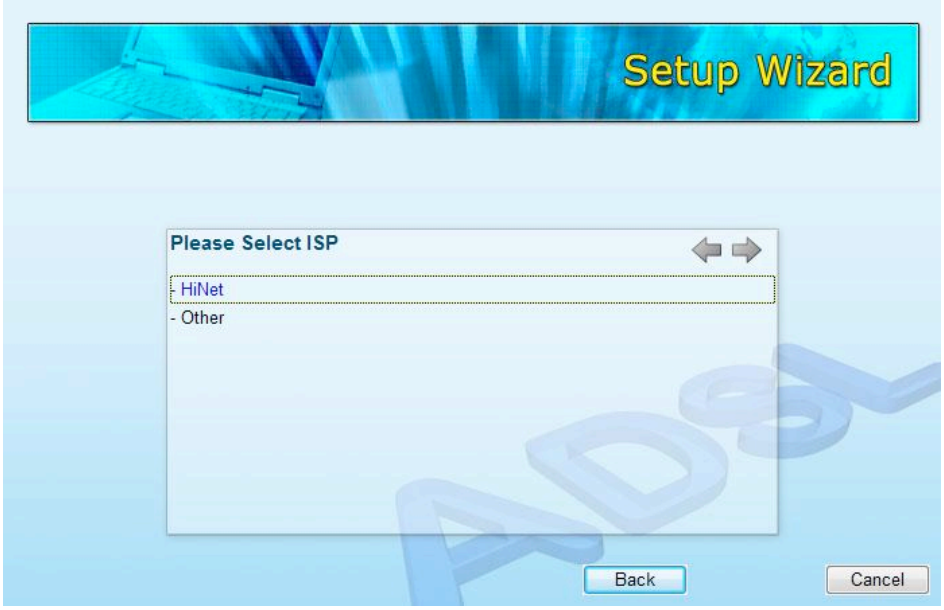
5. The wizard will automatically select the country you are in by checking the language of the operating system in your computer and then advance to the Select ISP screen. Select the ISP. If you cannot find the ISP, click “Other” to reselect the country or manually configure the ISP information.



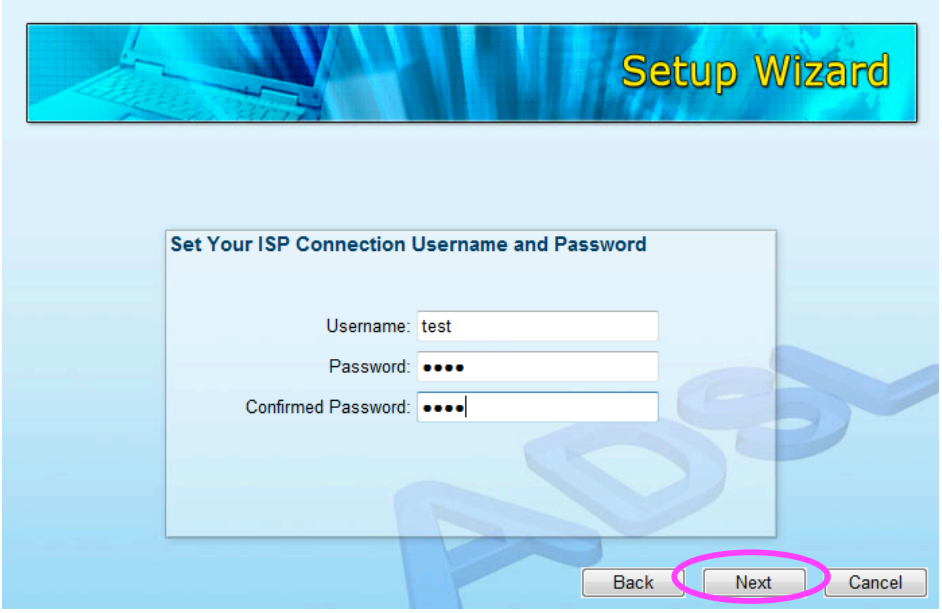
3.2 Automatically Set the ISP

If you can find the ISP from the wizard, follow the procedures below to let the wizard set the ISP settings automatically.

1. Select the ISP of your ADSL service.



2. Enter the username and password that your ISP has provided to you, if needed. Click “Next.”

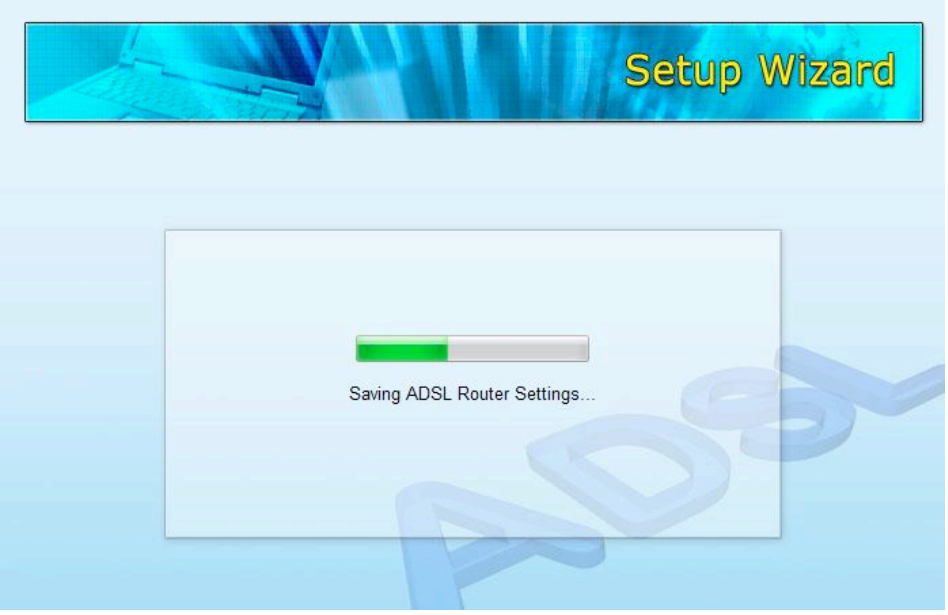


Ex.1017
CISCO SYSTEMS, INC. / Page 15 of 100

3. Click “Save” to save the settings and reboot the router.

4. After saving and rebooting the router, the ISP settings are completed. The wizard will then help to set your computer to obtain an IP address from the router automatically.

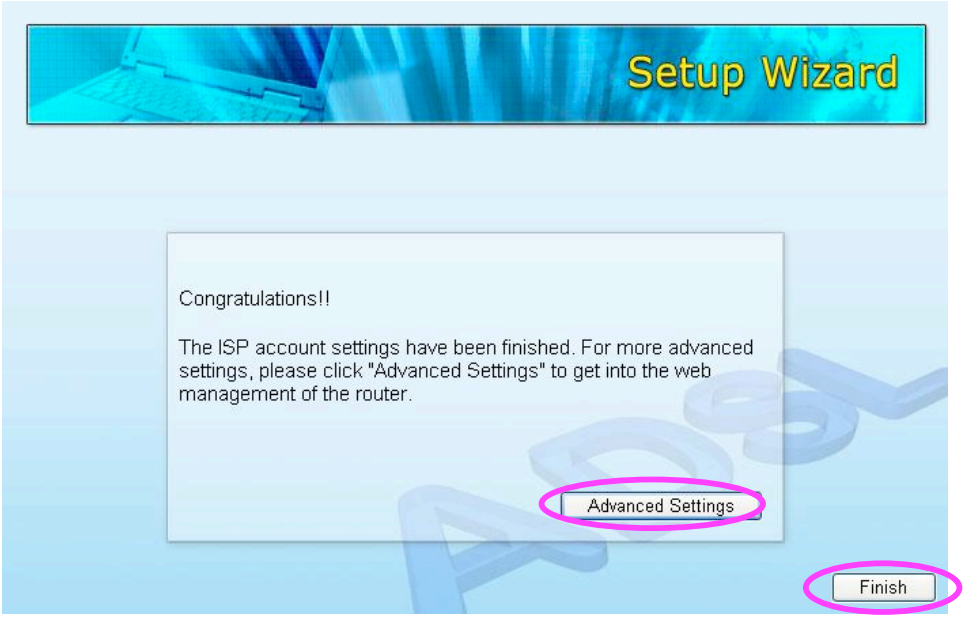
NOTE 1: To use the router to access the Internet, the IP address of each PC needs to be set in the same network segment as the router. The wizard will help to set the proper IP address for your computer.
NOTE 2: By default, the router’s DHCP server is enabled. If it is disabled before running the wizard, the wizard will enable the DHCP server automatically.



Ex.1017
CISCO SYSTEMS, INC. / Page 16 of 100

5. The wizard will try to connect to the ISP you have selected. If the connection fails, run the wizard to select the ISP again.

6. If you successfully connect to the ISP, you will see the screen below. To configure additional settings, click “Advanced Settings” to go the Web management of the router, or click “Finish” to close the wizard.



Ex.1017
CISCO SYSTEMS, INC. / Page 17 of 100

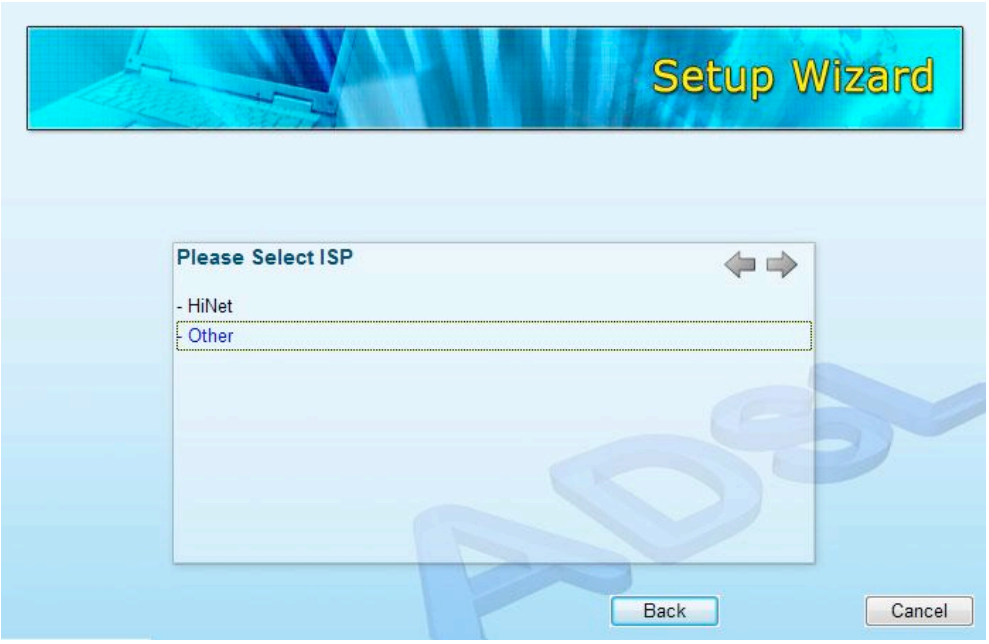
5.3 Manually Set the ISP

If you cannot find the ISP from the wizard, follow the steps below to set the ISP settings manually.

Before configuring the ISP manually, check with your ISP (Internet service provider) as to what kind of service is provided, such as PPPoE, PPPoA or RFC1483/2684. Gather the information as illustrated in the following table and keep it for reference.

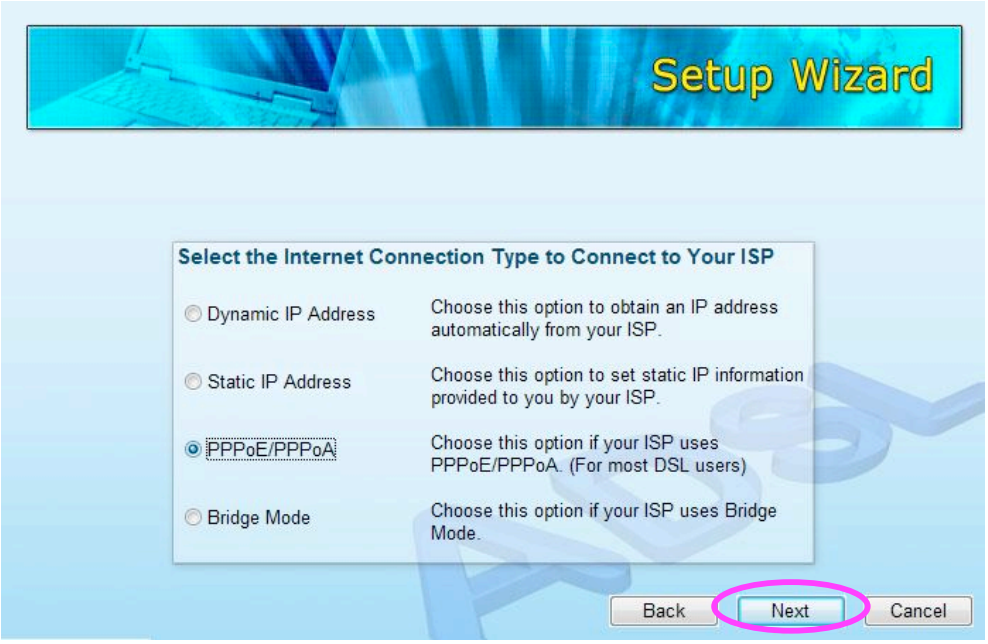
PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password (and Service Name).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password.
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing to use Bridged Mode.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing, IP Address, Subnet Mask, Gateway Address, and Domain Name System (DNS) IP Address (It is a fixed IP Address).

1. Select “Other.”

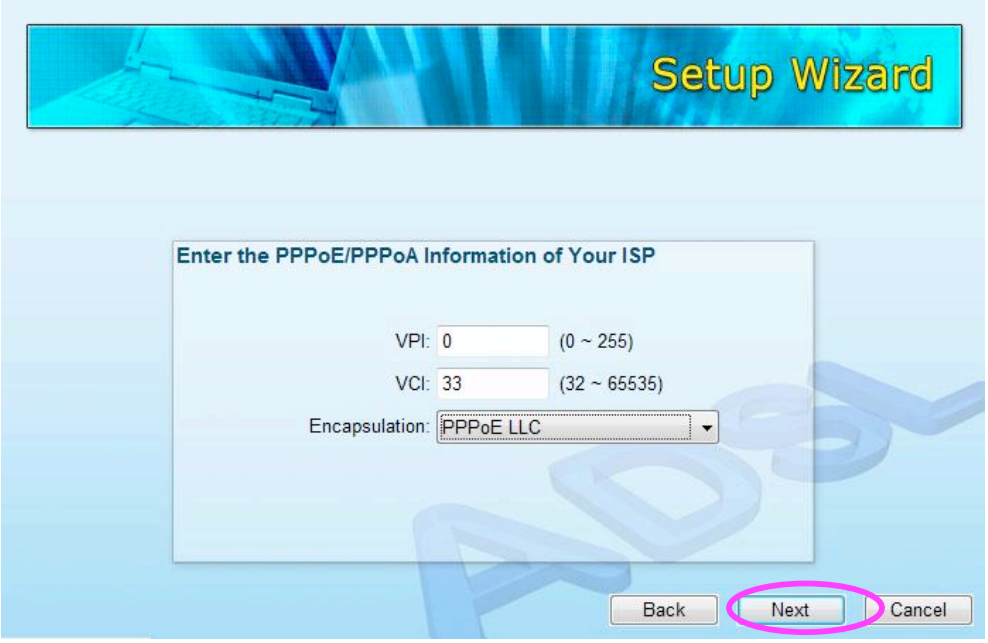


Ex.1017
CISCO SYSTEMS, INC. / Page 18 of 100

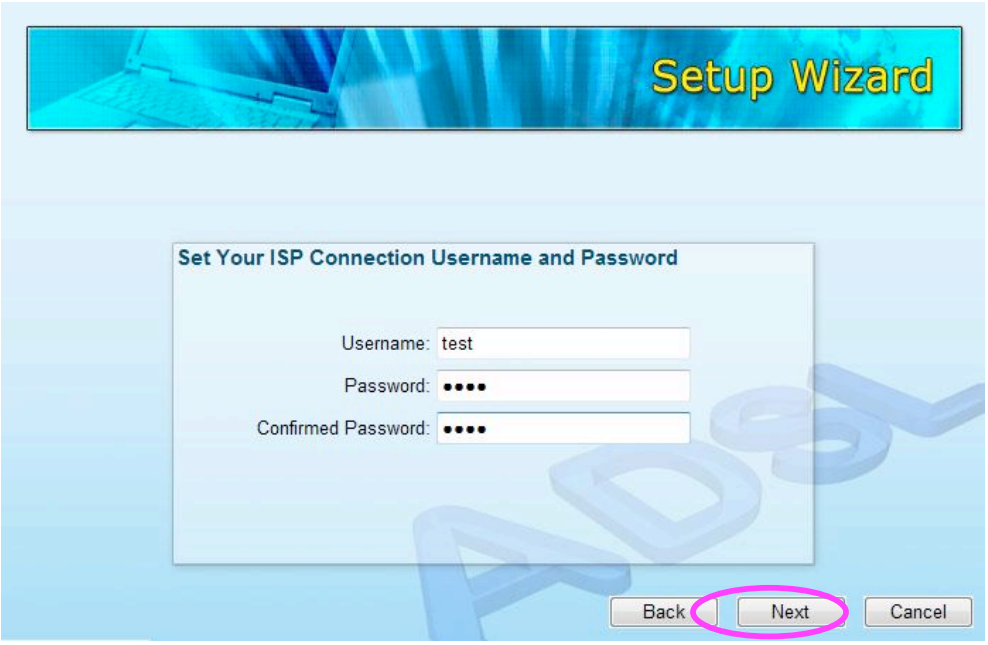
2. Check with your ISP as to the connection type of the ADSL line. Select the Connection Type and click “Next.”



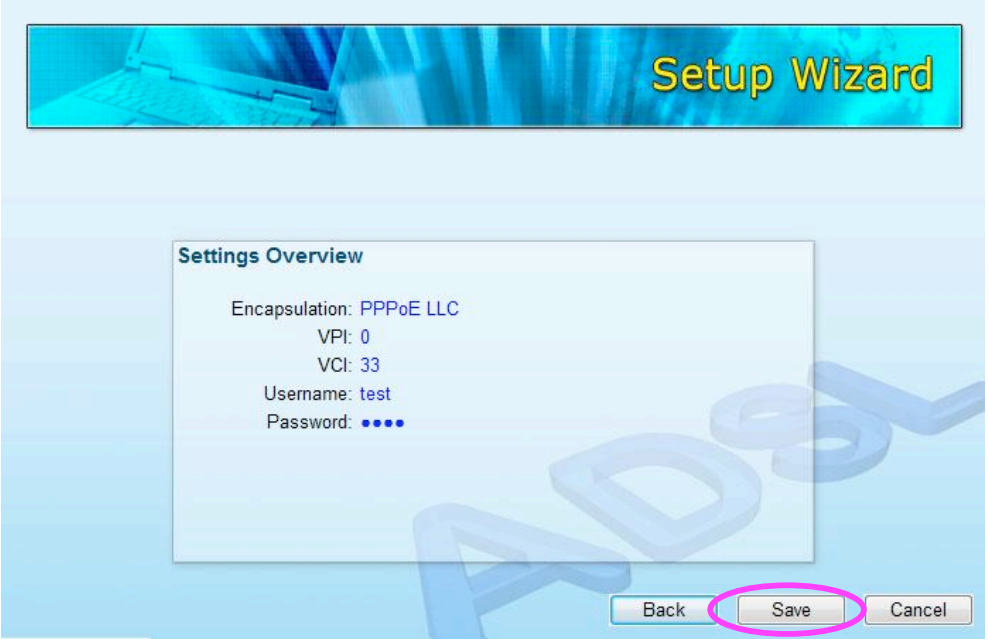
3. Input the VPI, VCI and encapsulation data supplied by your ISP. If the Connection Type is “Static IP Address,” you need to input the IP address information supplied by your ISP. For details about each setting, refer to Section 5.2.



4. Enter the username and password that your ISP has provided to you, if needed. Click “Next.”



5. Click “Save” to save the settings and reboot the router.

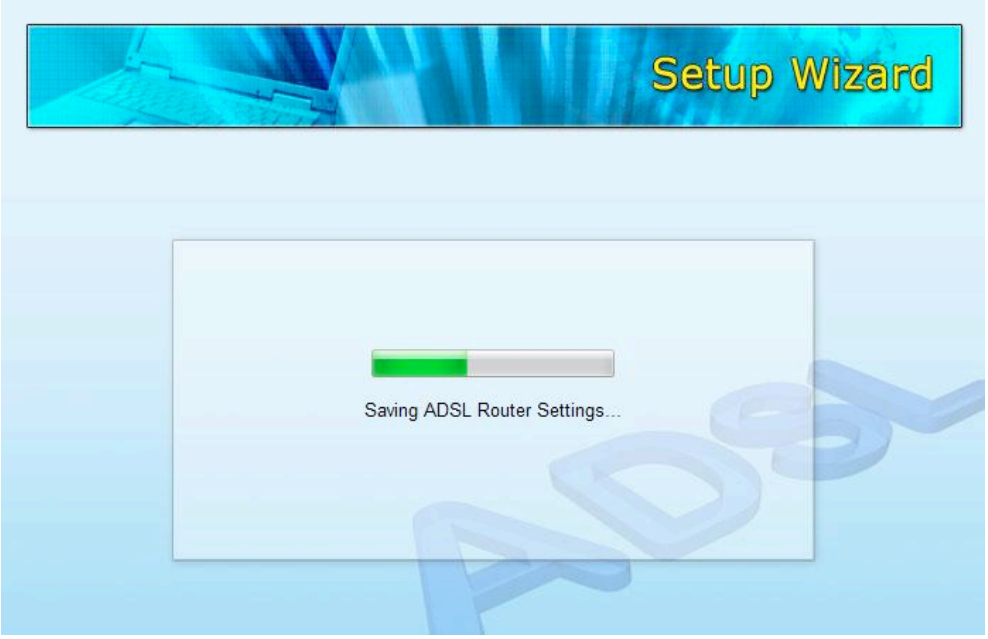


6. After saving and rebooting the router, the ISP settings are completed. The wizard will then help to set your computer to obtain an IP address from the

Ex.1017
CISCO SYSTEMS, INC. / Page 20 of 100

router automatically.

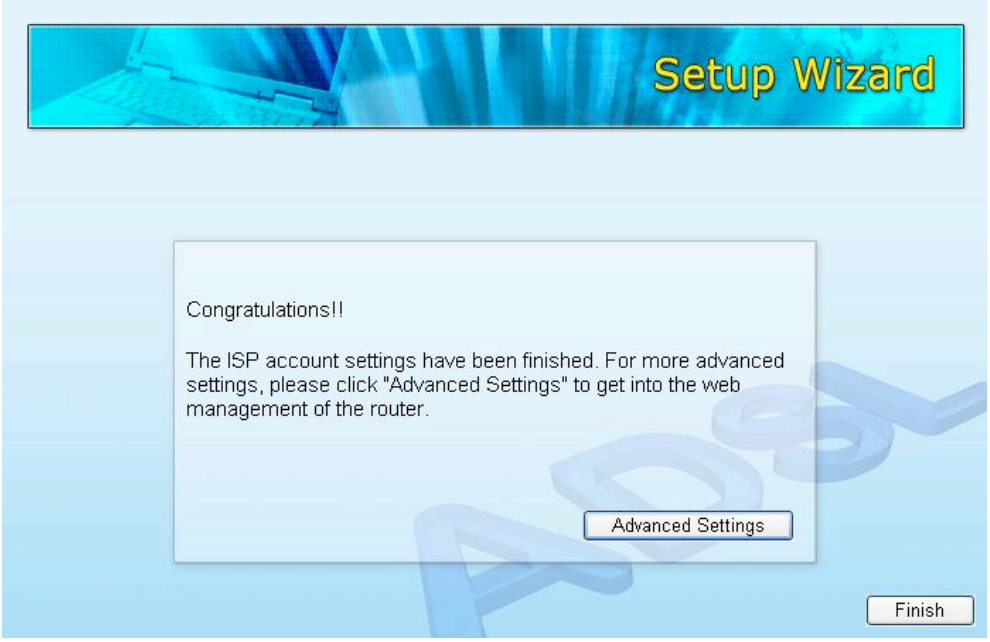
NOTE 1: To use the router to access the Internet, the IP address of each PC needs to be set in the same network segment as the router. The wizard will help to set the proper IP address for your computer.
NOTE 2: By default, the router's DHCP server is enabled. If it is disabled before running the wizard, the wizard will enable the DHCP server automatically.



7. The wizard will try to connect to the ISP you have selected. If the connection fails, run the wizard to select the ISP again.

Ex.1017
CISCO SYSTEMS, INC. / Page 21 of 100

8. If you successfully connect to the ISP, you will see the screen below. To configure additional settings, click “Advanced Settings” to go to the Web management of the router, or click “Finish” to close the wizard.



4 IP Address Setting

To use the router to access the Internet, the PCs in the network must have am Ethernet adapter installed and be connected to the router either directly or through a hub or switch. The TCP/IP protocol of each PC needs to be installed, and the IP address of each PC has to be set in the same subnet as the router.

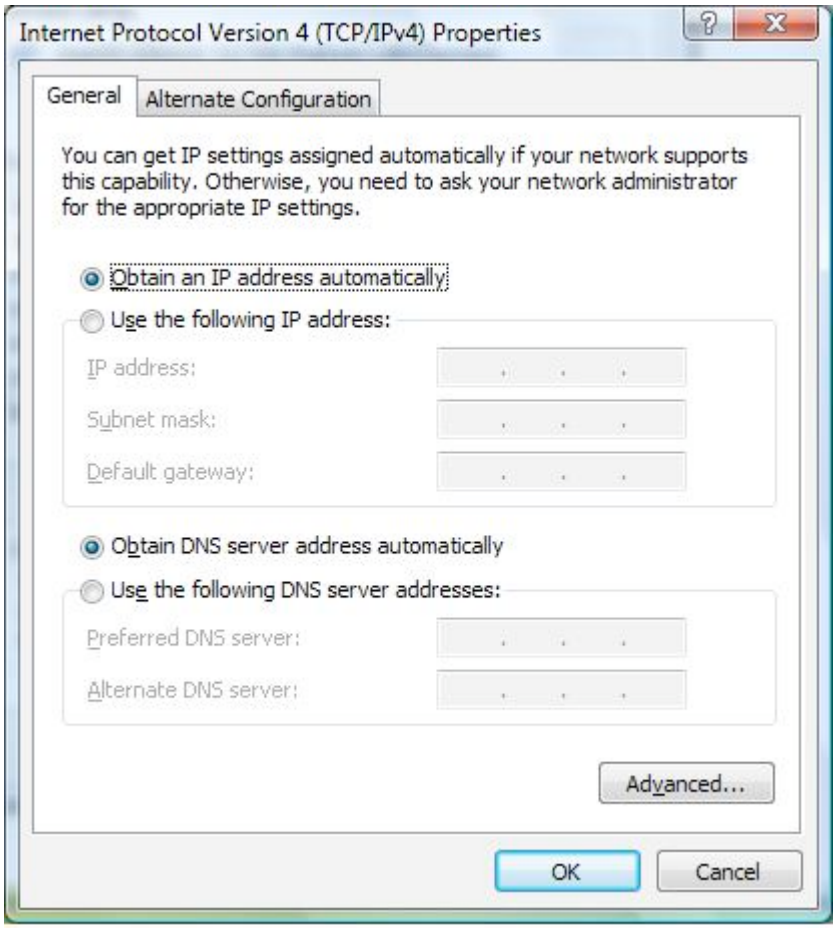
The router's default IP address is **192.168.2.1** and the subnet mask is **255.255.255.0**. PCs can be configured to obtain an IP address automatically through the DHCP server of the router, or with a fixed IP address in order to be in the same subnet as the router. By default, the DHCP server of the router is enabled and will dispatch an IP address to the PC in the range of **192.168.2.100** to **192.168.2.200**. It is strongly recommended that you obtain the IP address automatically.

This section shows you how to configure your PC so that it can obtain an IP address automatically for Windows 95/98/Me, 2000 or NT operating systems. For other operating systems (Macintosh, Sun, etc.), follow the manual of the operating systems. The following are step-by-step procedures for configuring your PC to obtain an IP address automatically for Windows Vista, Windows XP and Windows 2000.

Windows Vista

1. Click "Start" and select "Settings," then select "Control Panel." Double-click "Network and Sharing Center"; the Network and Sharing Center window will appear.
2. Click "Manage network connections"; right-click on the Local Area Connection icon and select "Properties." The Local Area Connection window will appear.
3. Check your list of Network Components. You should see "Internet Protocol Version 4 (TCP/IPv4)" on your list. Select it and click "Properties."
4. In the Internet Protocol Version 4 (TCP/IPv4) Properties window, select "Obtain an IP address automatically" and "Obtain DNS server address automatically," as shown on the following screen.

Ex.1017
CISCO SYSTEMS, INC. / Page 23 of 100



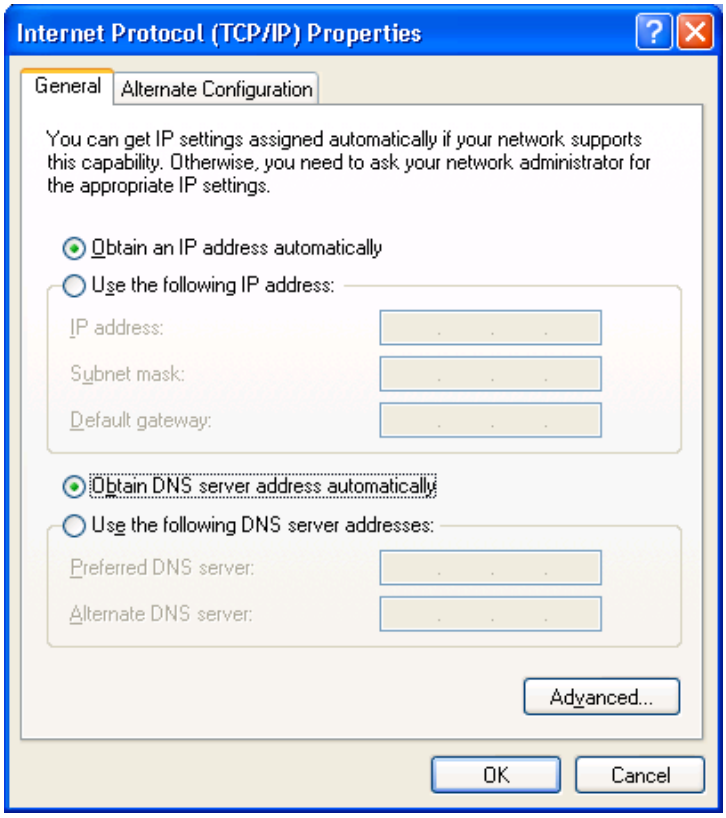
5. Click “OK” to confirm the setting. Your PC will now obtain an IP address automatically from your router’s DHCP server.

NOTE: Make sure that the router’s DHCP server is the only DHCP server available on your LAN.

Windows XP

1. Click “Start” and select “Control Panel”; then double-click “Network Connections.” The Network Connections window will appear.
2. Right-click on the Local Area Connection icon and select “Properties.” The Local Area Connection window will appear.
3. Check your list of Network Components. You should see “Internet Protocol [TCP/IP]” on your list. Select it and click “Properties.”
4. In the Internet Protocol (TCP/IP) Properties window, select “Obtain an IP address automatically” and “Obtain DNS server address automatically,” as shown on the following screen.

Ex.1017
CISCO SYSTEMS, INC. / Page 24 of 100



5. Click “OK” to confirm the setting. Your PC will now obtain an IP address automatically from your router’s DHCP server.

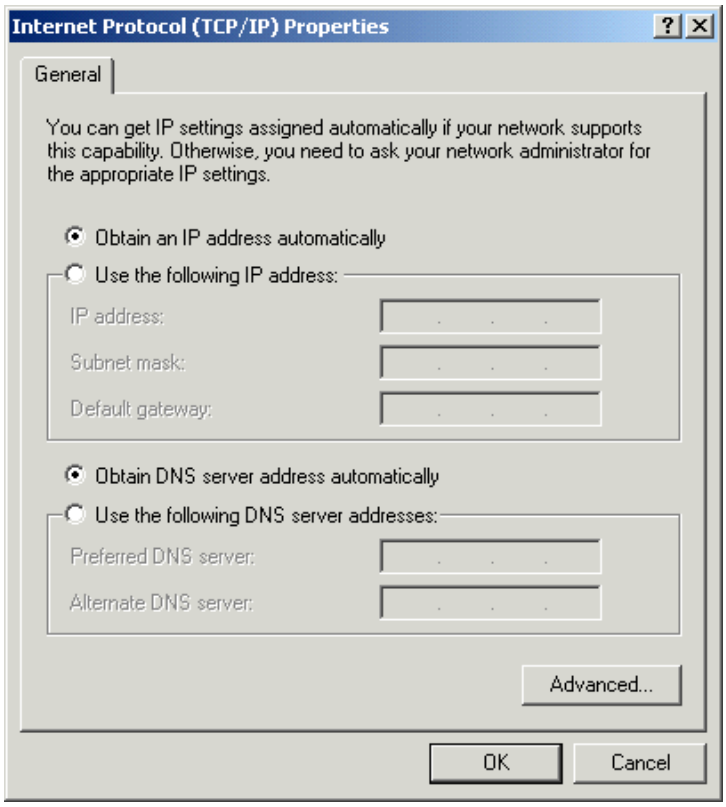
NOTE: Make sure that the router’s DHCP server is the only DHCP server available on your LAN.

Windows 2000

1. Click “Start” and select “Settings,” then click “Control Panel.” The Control Panel window will appear.
2. Double-click the Network and Dial-up Connections icon. In the Network and Dial-up Connection window, double-click the Local Area Connection icon. The Local Area Connection window will appear.
3. In the Local Area Connection window, click “Properties.”
4. Check your list of Network Components. You should see “Internet Protocol [TCP/IP]” on your list. Select it and click “Properties.”

Ex.1017
CISCO SYSTEMS, INC. / Page 25 of 100

5. In the Internet Protocol (TCP/IP) Properties window, select “Obtain an IP address automatically” and “Obtain DNS server address automatically,” as shown on the following screen.



6. Click “OK” to confirm the setting. Your PC will now obtain an IP address automatically from your router’s DHCP server.

NOTE: Make sure that the router’s DHCP server is the only DHCP server available on your LAN.

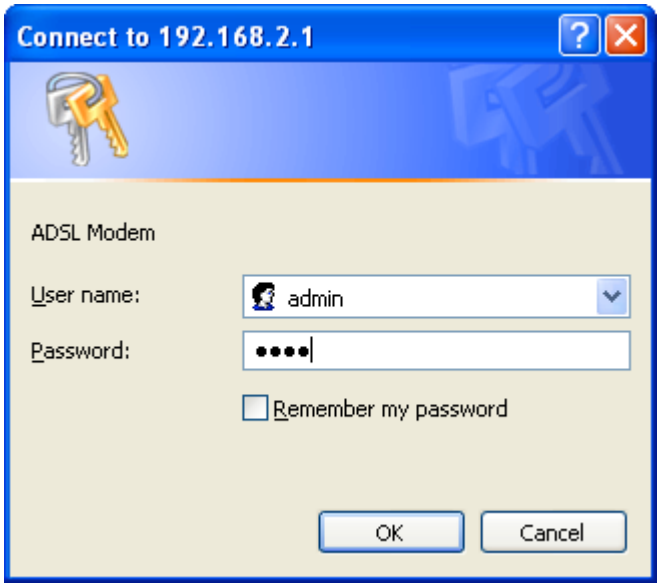
Ex.1017
CISCO SYSTEMS, INC. / Page 26 of 100

5 Web Management Configuration

Once you have configured your PCs to obtain an IP address automatically, the router's DHCP server will automatically give your LAN clients an IP address. By default, the router's DHCP server is enabled so you can obtain an IP address automatically.

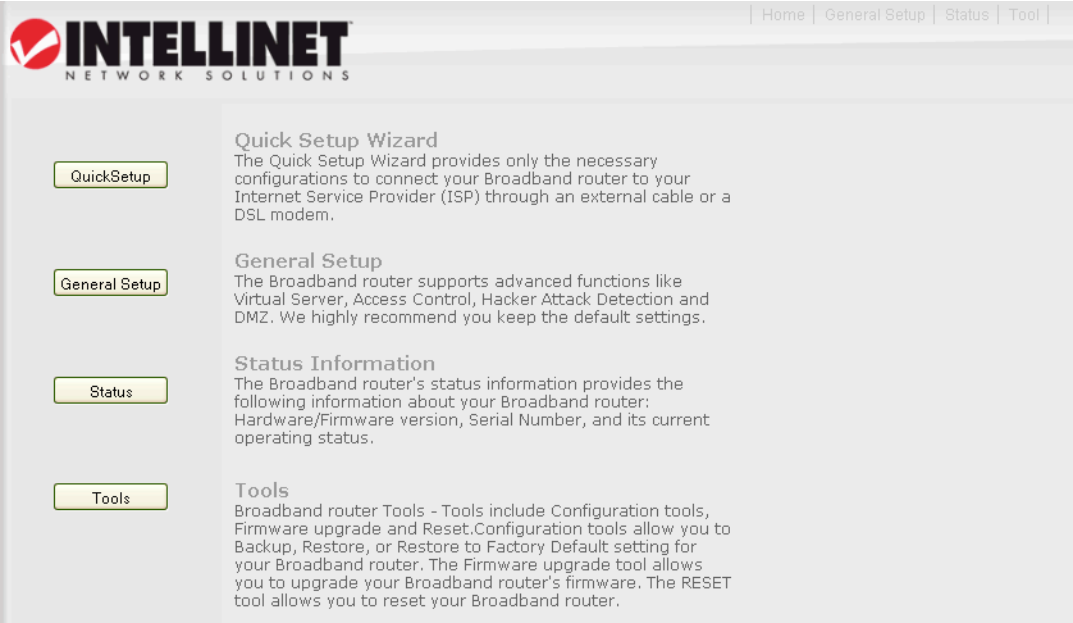
Once your PC has obtained an IP address from your router, enter the default IP address **192.168.2.1** (router's IP address) into your PC's Web browser and press <Enter> on your keyboard.

The login screen below will appear. Fill in the "User Name" and "Password" text fields, then click "OK" to log in. By default, the username is "**admin**" and the password is "**1234**." For security reasons, it is recommended that you change the password as soon as possible.



The **HOME** screen screen below will appear. The **Home** Screen is divided into four sections: **Quick Setup, General Setup, Status, Tools.**

Ex.1017
CISCO SYSTEMS, INC. / Page 27 of 100



Quick Setup *(Section 5.1)*

The Quick Setup Wizard provides only the necessary configurations to connect your router to your Internet service provider (ISP).

General Setup *(Section 5.2)*

The router supports advanced functions like virtual server, access control, hacker attack detection and DMZ. It's highly recommended that you keep the default settings.

Status *(Section 5.3)*

The status section provides the following information about your router: hardware/firmware version, serial number and its current operating status.

Tools *(Section 5.4)*

Tools include configuration tools, firmware upgrading and reset configuration tools that allow you to back up, restore or restore to factory default settings.

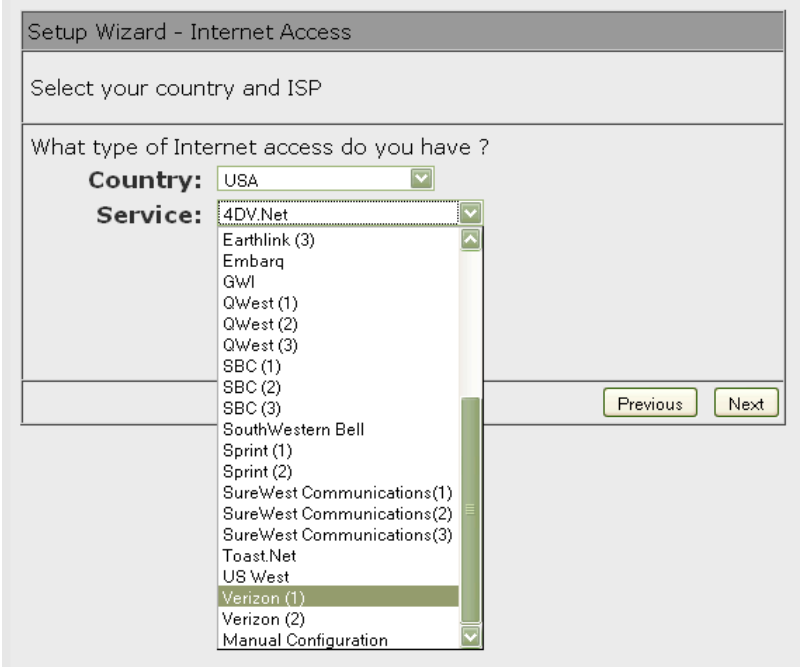
5.1 Quick Setup

The Quick Setup section is designed to get you using the router as quickly as possible. Before configuring the router, check with your ISP (Internet service provider) as to what kind of the service is provided, such as PPPoE, PPPoA or RFC1483/2684. Gather the information as illustrated in the table below and keep it for reference.

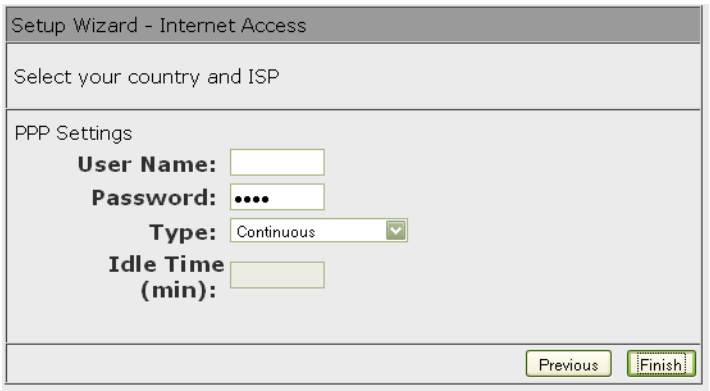
PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password (and Service Name).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password.
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing to use Bridged Mode.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing, IP Address, Subnet Mask, Gateway Address, and Domain Name System (DNS) IP Address (It is a fixed IP Address).

1. Click “Quick Setup” and the following screen will be displayed.

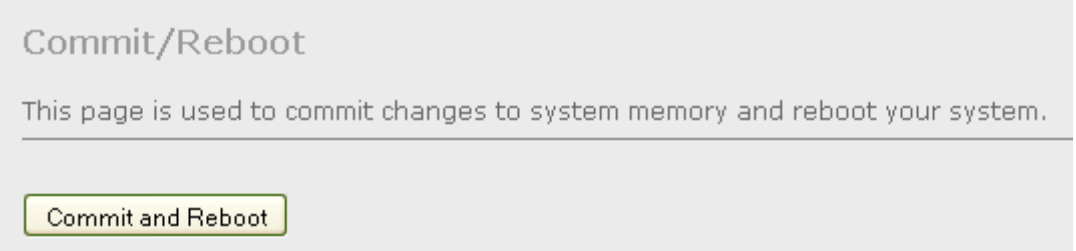
2. Select the country you're in and your ISP (Internet service provider).



3. Enter the username and password your ISP has provided to you, if needed. Click "Finish" to save the settings.



4. Click "Commit and Reboot" to reboot the router.



5.2 General Setup

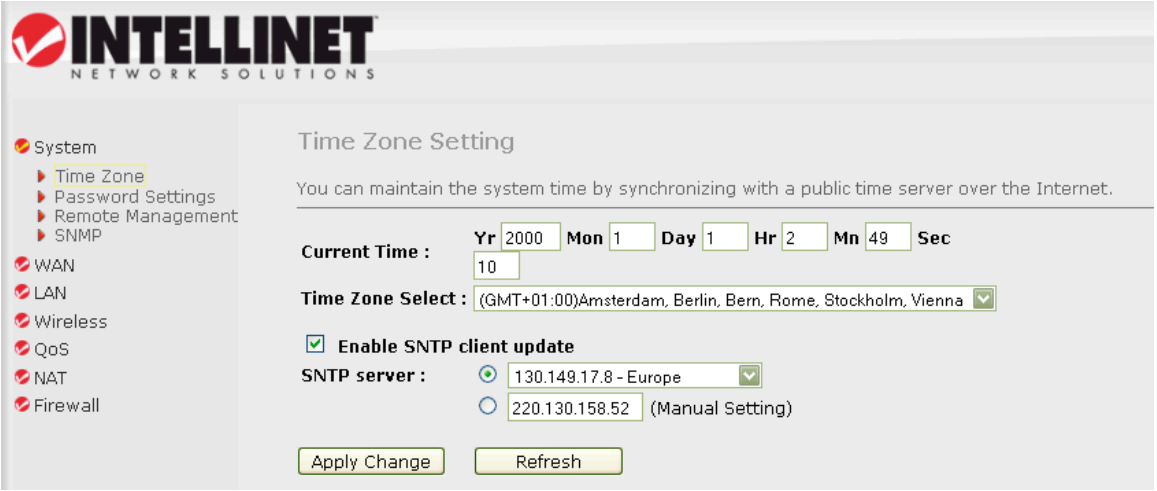
Start your Web browser and log on to the Web management interface of the router, then either click “General Setup” on the left menu or click the “General Setup” link at the upper-right corner of the Web management interface.

5.2.1 System

This screen includes the basic configuration tools for the router’s remote management access function.

5.2.1.1 Time Zone

Time Zone allows your router to set its time, especially useful when recording System Log entries.



Parameter	Description
Current Time	The current time of the specified time zone. You can set the current time yourself or configure it via SNTP server.
Time Zone Select	Select the time zone of the country you are in. The router will set its time based on your selection.
Enable SNTP client update	Check the box to enable the router to update time from the SNTP server.
SNTP server	The IP address or the host name of the SNTP server. You can select from the list or set it manually.

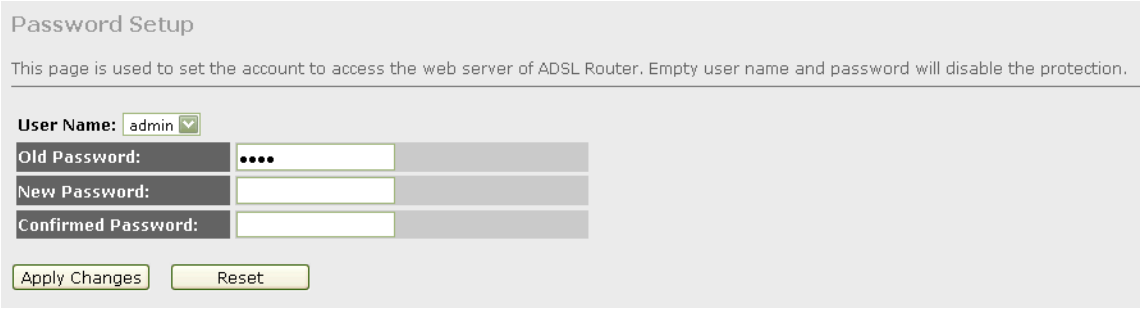
Ex.1017
CISCO SYSTEMS, INC. / Page 31 of 100

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

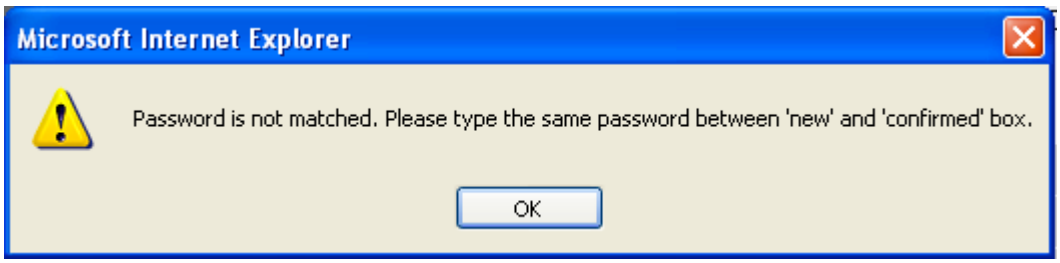
Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings and restart the router so the settings will take effect after it reboots.

5.2.1.2 Password Settings

This screen allows you to set the password to access the Web server of the router. Select the “admin” (as administrator) or “user” (as user) account and configure the password.



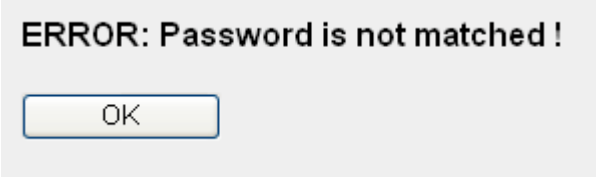
When you finish, click “Apply Changes.”
If the passwords you entered in the “New Password” and “Confirmed Password” fields are not the same, you’ll see the following message:



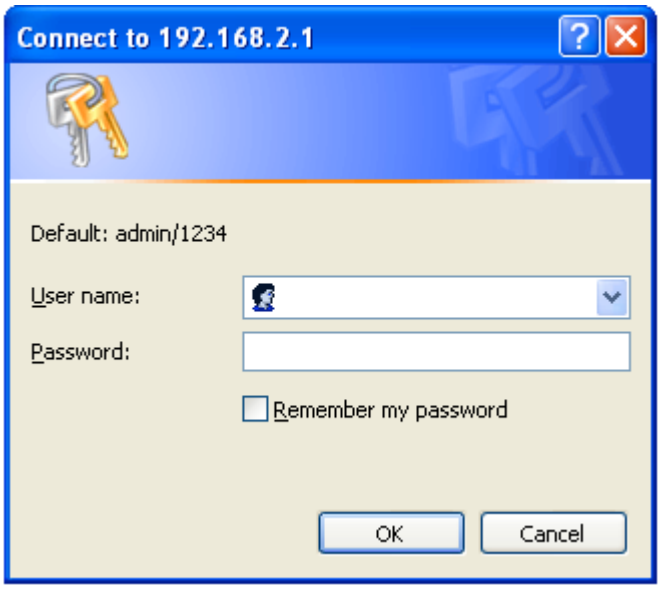
Re-enter the new password again when you see above message.

Ex.1017
CISCO SYSTEMS, INC. / Page 32 of 100

If you see the following message:



It means the content in the “Current Password” field is wrong. Click “OK” to go back to the previous menu and input the current password again.
If the current and new passwords are correctly entered, after you click “Apply” you’ll be prompted to input your new password:



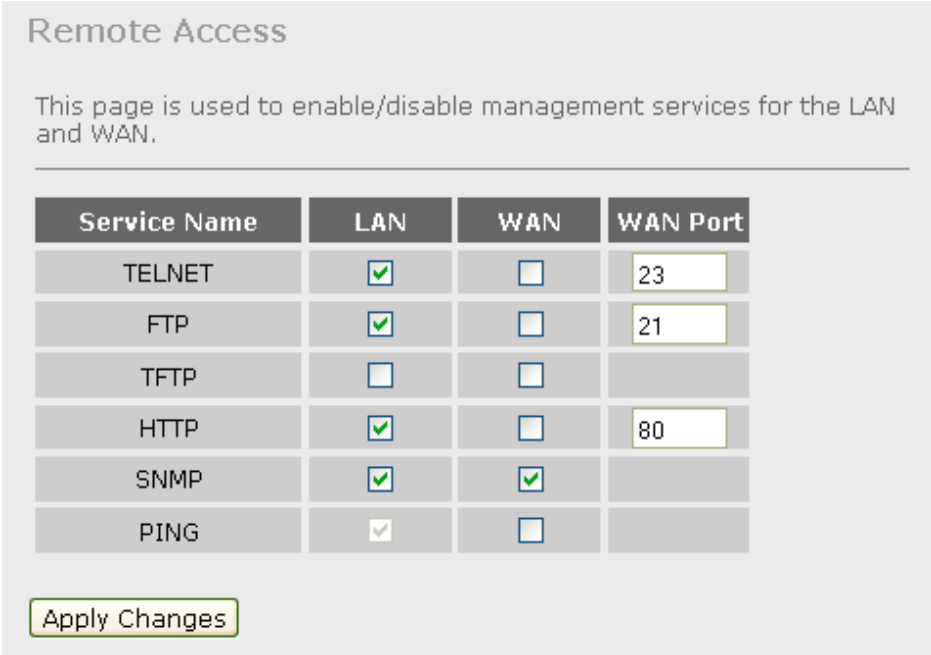
Use the new password to enter the Web management interface again, and you should be able to log in with the new password.

5.2.1.3 Remote Management

The Remote Access function can secure remote host access to your router from LAN and WAN interfaces for some services provided by the router. These services include Telnet, FTP, TFTP, HTTP, SNMP and PING.

Click the “System” menu on the left of the Web management interface, then click “Remote Management” and the following screen will be displayed on your Web browser.

Ex.1017
CISCO SYSTEMS, INC. / Page 33 of 100



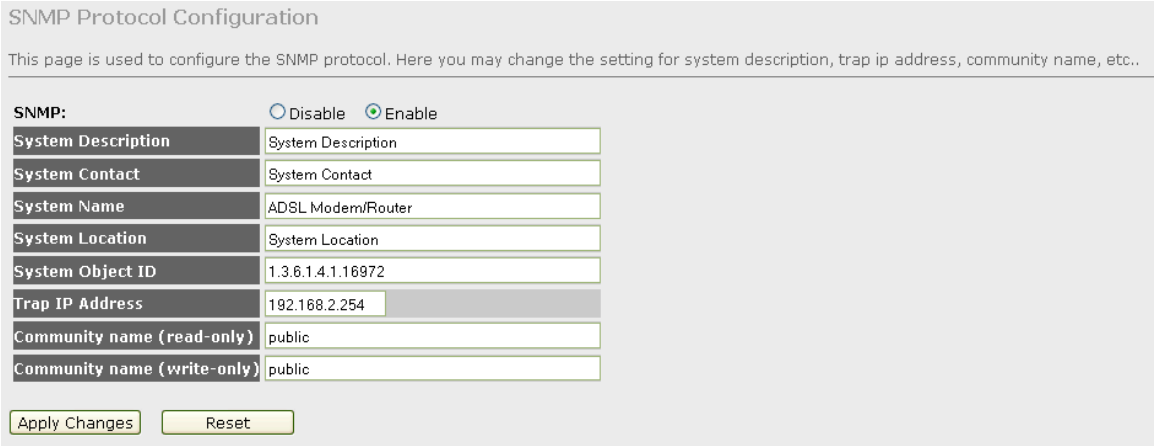
Parameter	Description
LAN	Check/un-check the services on the LAN column to allow/ disallow the services access from the LAN side.
WAN	Check/un-check the services on the WAN column to allow/ disallow the services access from the WAN side.
WAN Port	This field allows the user to specify the port corresponding to the service. Take the HTTP service, for example: When it is changed to 8080, the HTTP server address for the WAN side is http://dsl_addr:8080, where “dsl addr” is the WAN-side IP address of the router.

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.1.4 SNMP

Simple Network Management Protocol (SNMP) is a troubleshooting and management protocol that uses the UDP protocol on Port 161 to communicate between clients and servers. The router can be managed locally or remotely by SNMP protocol.



Parameter	Description
SNMP	Select “Disable” or “Enable” to disable or enable the SNMP feature.
System Description	Enter the system description of the router.
System Contact	Enter the contact person and/or contact information for the router.
System Name	Assign an administrative name for the router.
System Location	The physical location of the router.
System Object ID	This is the vendor object identifier: the vendor’s authoritative identification of the network management subsystem contained in the entity.
Trap IP Address	Destination IP address of the SNMP trap.
Community name (read-only)	Name of the read-only community. This read-only community allows read operation to all objects in the MIB.

Ex.1017
CISCO SYSTEMS, INC. / Page 35 of 100

Community name (write-only)	Name of the write-only community. This write-only community allows write operation to the objects defines as read-writable in the MIB.

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.2 WAN

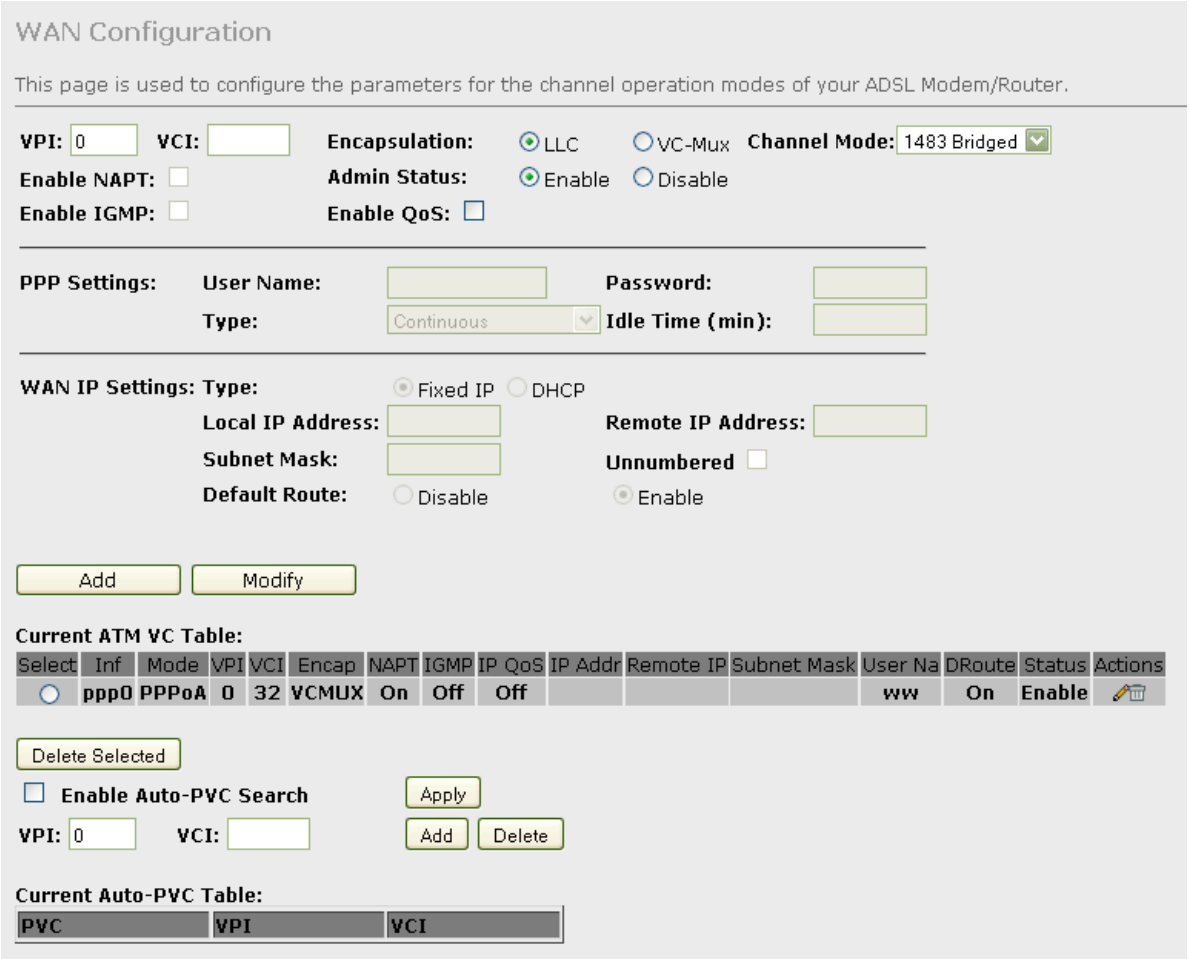
Use the WAN Settings screen if you have already configured the Quick Setup Wizard section and you would like to change your Internet connection type. The WAN Settings screen allows you to specify the type of WAN port connection you want to establish with your ISP. The WAN settings offer the following selections for the router’s WAN port: Channel, ATM Setting, ADSL Setting, DNS, DDNS and RIP.

5.2.2.1 Channel Config

The router supports eight ATM permanent virtual channels (PVCs) at the most. This screen is used to configure the parameters for the channel operation modes of your router. Before configuring the router, check with your ISP as to what kind of service is provided, such as PPPoE, PPPoA or RFC1483/2684. Gather the information as illustrated in the table below and keep it for reference.

Ex.1017
CISCO SYSTEMS, INC. / Page 36 of 100

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password (and Service Name).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password.
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing to use Bridged Mode.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing, IP Address, Subnet Mask, Gateway Address, and Domain Name System (DNS) IP Address (It is a fixed IP Address).
RFC1483 MER	VPI/VCI, VC-based/LLC-based multiplexing, IP Address, Subnet Mask, Gateway Address, and Domain Name System (DNS) IP Address.



Parameter	Description
VPI	VPI is a virtual path that determines the way an ATM cell should be routed. The VPI is an 8-bit (in UNI) or 12-bit (in NNI) number that is included in the header of an ATM cell. The valid range for the VPI is 0 to 255. Enter the VPI assigned by the ISP.
VCI	VCI is the label given to an ATM VC to identify it and determine its destination. The VCI is a 16-bit number that is included in the header of an ATM cell. The valid VCI range is 32 to 65535. Enter the VCI assigned by the ISP.
Encapsulation	Check with your ISP for the method of multiplexing.
Channel Mode	There are five kinds of channel modes you can select for an ADSL connection. Check with your ISP for the method of the ADSL connection.
Enable NAPT	Enable or disable NAPT, an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. When NAPT is enabled, the router will help to make all necessary IP address translations for the PC connected to the router to access the Internet.
Admin Status	Enable or disable the PVC channel setting.
User Name	Enter the username exactly as your ISP assigned it.
Password	Enter the password that your ISP has assigned to you.
Type	Continuous – The connection will be kept always on. If the connection is interrupted, the router will re-connect automatically. Connect on Demand – Only connects when you want to surf the Internet. “Idle Time” is set to stop the connection when the network traffic is not sending or receiving after an idle time. Manual – After you have selected this option, go to the Status screen and click “Connect.” The router will connect to the ISP. If you want to stop the connection, click “Disconnect.”

Ex.1017
CISCO SYSTEMS, INC. / Page 38 of 100

Idle Time (ms)	“Idle Time” is set to stop the connection when the network traffic is not sending or receiving after an idle time.
Type	Fixed IP – Set the static IP Address to the router. Enter the IP address your ISP has assigned. DHCP – To get the IP address from the ISP directly.
Local IP Address	Set the IP address obtained from your ISP.
Remote IP Address	Enter the remote IP address assigned by your ISP.
Subnet Mask	Enter the subnet mask assigned by your ISP.
Unnumbered	The IP Unnumbered configuration allows you to enable IP processing on a serial interface without assigning it an explicit IP address. When it is enabled, the router’s WAN IP address can “borrow” the IP address of another interface already configured on the router, which conserves network and address space. Check it if you want to assign the WAN IP address from other interface, such as a client’s IP address.
Default Route	When “Default Router” is enabled, all the packets for destinations not known by the router’s routing table are sent to the default route. By default, it is enabled.
Add/Modify	These buttons are for you to maintain the channel configuration settings.
Current ATM VC Table	The channel you have configured will be listed here. You can select the VC channel to Edit or Delete.
Delete Selected	If you want to delete a specific VC channel entry, check the “select” box of the VC channel you want to delete, then click “Delete Selected.”
Enable Auto-PVC Search	Check the box and click “Apply” to enable the auto PVC search function.
VPI	VPI is a virtual path that determines the way an ATM cell should be routed.
VCI	VCI is the label given to an ATM VC to identify it and determine its destination.
Add/Delete	These buttons are for you to maintain the Current Auto-PVC Table.

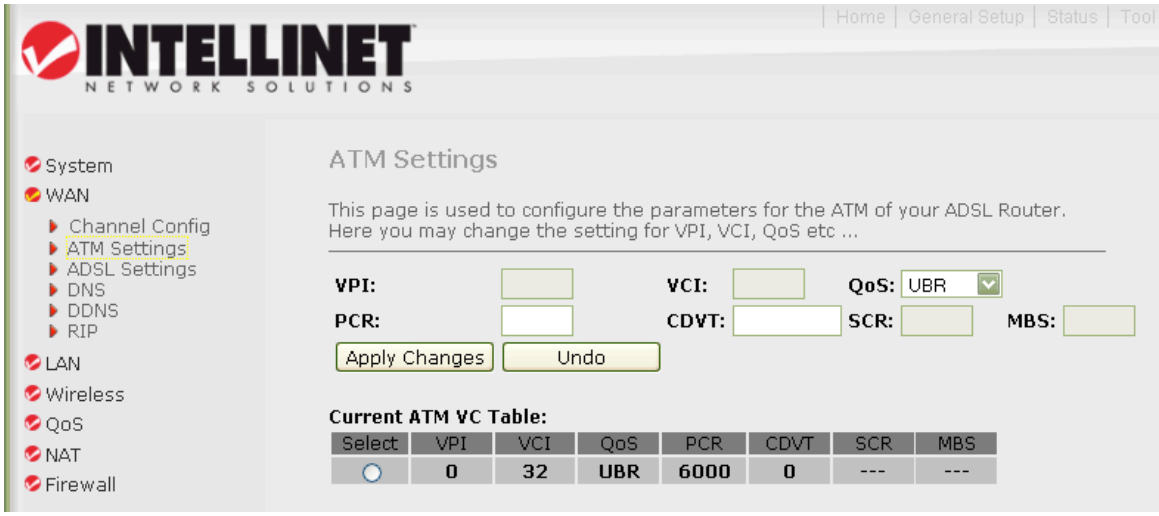
Ex.1017
CISCO SYSTEMS, INC. / Page 39 of 100

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.2.2 ATM Setting

The screen is for ATM PVC QoS parameters setting.



Parameter	Description
VPI	VPI is a virtual path that determines the way an ATM cell should be routed. The VPI is an 8-bit (in UNI) or 12-bit (in NNI) number that is included in the header of an ATM cell. The valid range for the VPI is 0 to 255. Enter the VPI assigned by the ISP.
VCI	VCI is the label given to an ATM VC to identify it and determine its destination. The VCI is a 16-bit number that

Ex.1017
CISCO SYSTEMS, INC. / Page 40 of 100

	is included in the header of an ATM cell. The valid VCI range is 32 to 65535. Enter the VCI assigned by the ISP.
QoS	UBR (Unspecified Bit Rate) – Select UBR for applications that are non-time sensitive, such as e-mail. CBR (Constant Bit Rate) – This class is used for emulating circuit switching. The cell rate is constant with time. Select CBR to specify fixed (always on) bandwidth for voice or data traffic. nrtVBR (non-real time Variable Bit Rate) – This class allows users to send traffic at a rate that varies with time depending on the availability of user information. Statistical multiplexing is provided to make optimum use of network resources. Multimedia e-mail is an example of nrtVBR. rtVBR (real time Variable Bit Rate) – This class is similar to nrtVBR but is designed for applications that are sensitive to cell-delay variation. Examples for real-time VBR are voice with speech activity detection (SAD) and interactive compressed video.
PCR	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the PCR (Peak Cell Rate). This is the maximum rate at which the sender can send cells.
CDVT	PCR generally is coupled with the CDVT (Cell Delay Variation Tolerance), which indicates how much jitter is allowable.
SCR	SCR (Sustain Cell Rate) is the average rate over a long interval, in the order of the connection lifetime.
MBS	MBS (Maximum Burst Size) refers to the maximum number of cells that can be sent at the peak rate. Enter the MBS, which is less than 65535.
Current ATM VC Table	The channel you have configured with regard to the ATM settings will be listed here.

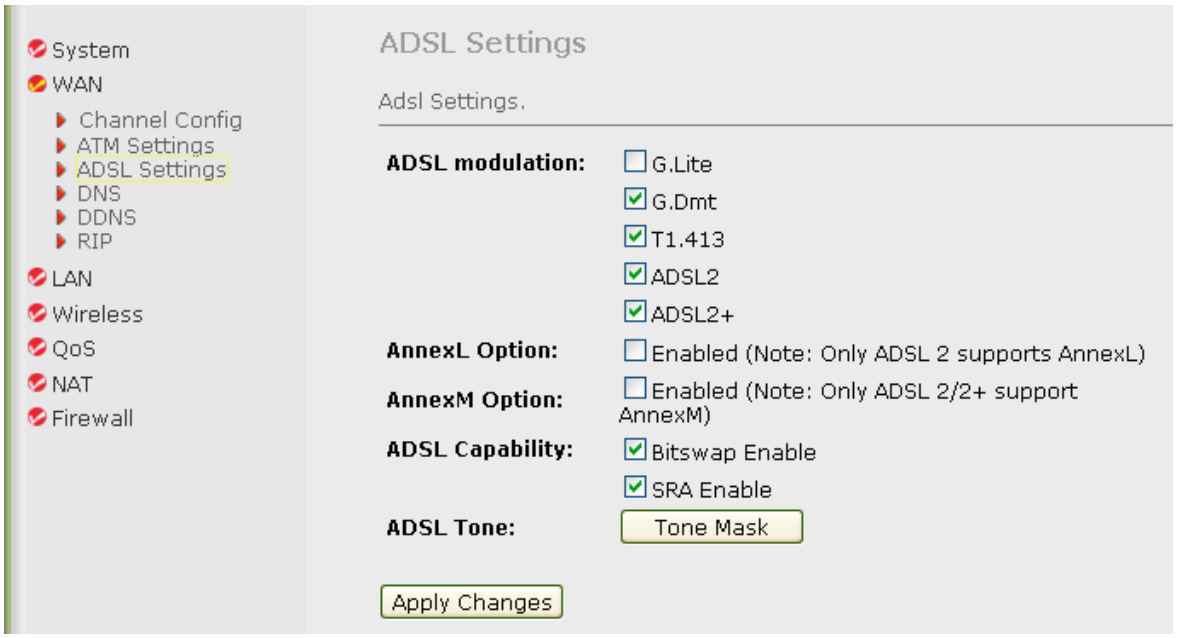
When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Ex.1017
CISCO SYSTEMS, INC. / Page 41 of 100

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.2.3 ADSL Setting

The screen allows you to select any combination of DSL modes.



Parameter	Description
ADSL modulation	Choose preferred ADSL standard protocols.
AnnexL Option	Enable/Disable ADSL2/ADSL2+ Annex L capability.
AnnexM Option	Enable/Disable ADSL2/ADSL2+ Annex M capability.
ADSL Capability	Bitswap Enable – Enable/Disable bitswap capability. SRA Enable – Enable/Disable SRA (seamless rate adaptation) capability.
ADSL Tone	Choose tones to be masked. The masked tones will not

Ex.1017
CISCO SYSTEMS, INC. / Page 42 of 100

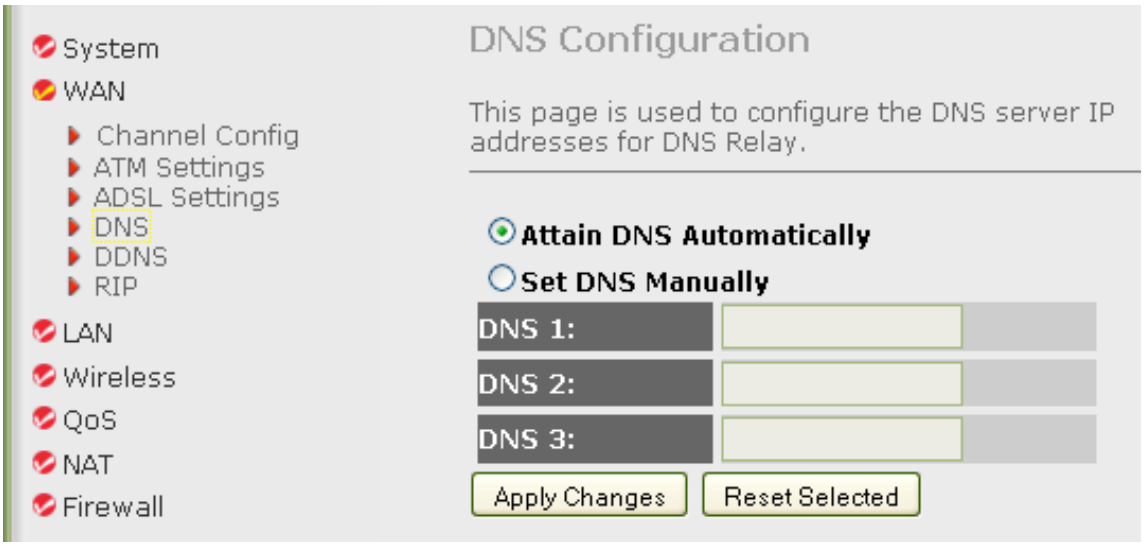
carry any data. Click “Tone Mask” to mask the tone number you have selected or all the tone numbers.

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.2.4 DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as “www.router.com,” a DNS server will find that name in its index and the matching IP address. This screen is used to select the way to obtain the IP addresses of the DNS servers.



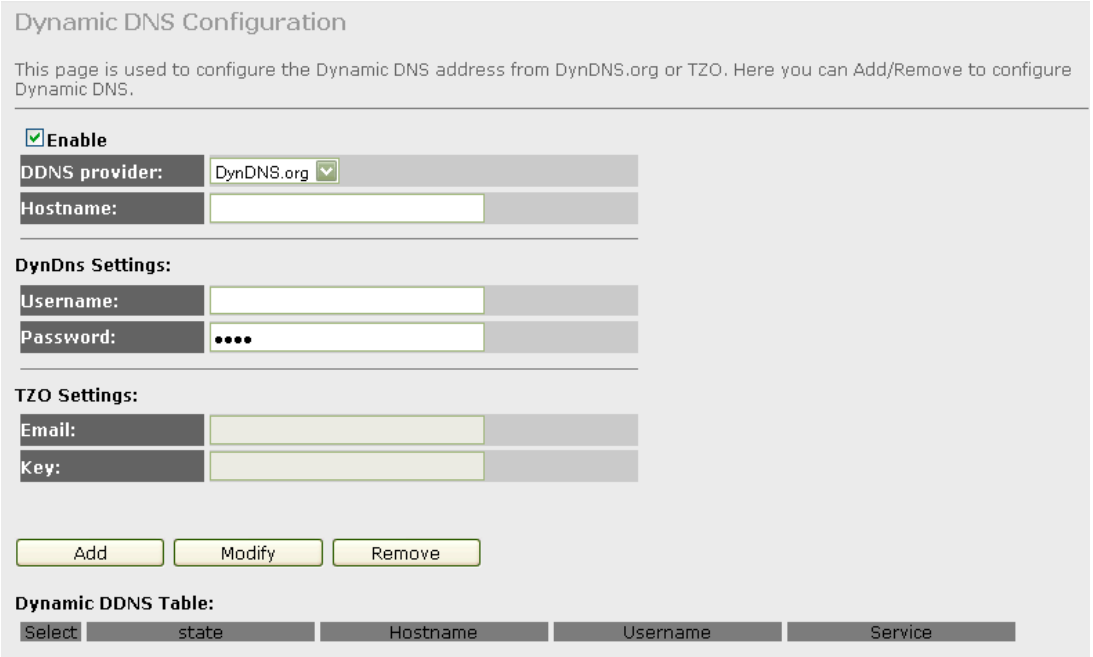
Parameter	Description
Attain DNS Automatically	Select this item if you want to use the DNS servers obtained from ISP.
Set DNS Manually	Select this item to specify up to three DNS IP addresses.

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.2.5 DDNS

Dynamic DNS (DDNS) allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers.



Ex.1017
CISCO SYSTEMS, INC. / Page 44 of 100

Parameter	Description
Enable	Check the box to enable DDNS function.
DDNS Provider	Select your DDNS service provider here. This router supports DynDNS and TZO service providers.
Host Name	Enter the domain name you've obtained from the DDNS service provider.
Username	Enter the username assigned by the DDNS service provider.
Password	Enter the password assigned by the DDNS service provider.
E-mail	Enter the e-mail account that your DDNS service provider assigned to you.
Key	Enter the password that your DDNS service provider assigned to you.
Add/Modify/Remove	These buttons are for you to maintain the DDNS table.
Dynamic DDNS Table	The DDNS you have configured will be added to the list.

When you finish, click "Apply Changes." You'll see the following message displayed on Web browser.

Click "Continue" to save the settings made and go back to the Web management interface; click "Apply" to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.2.6 RIP

RIP is an Internet protocol you can set up to share routing-table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line.

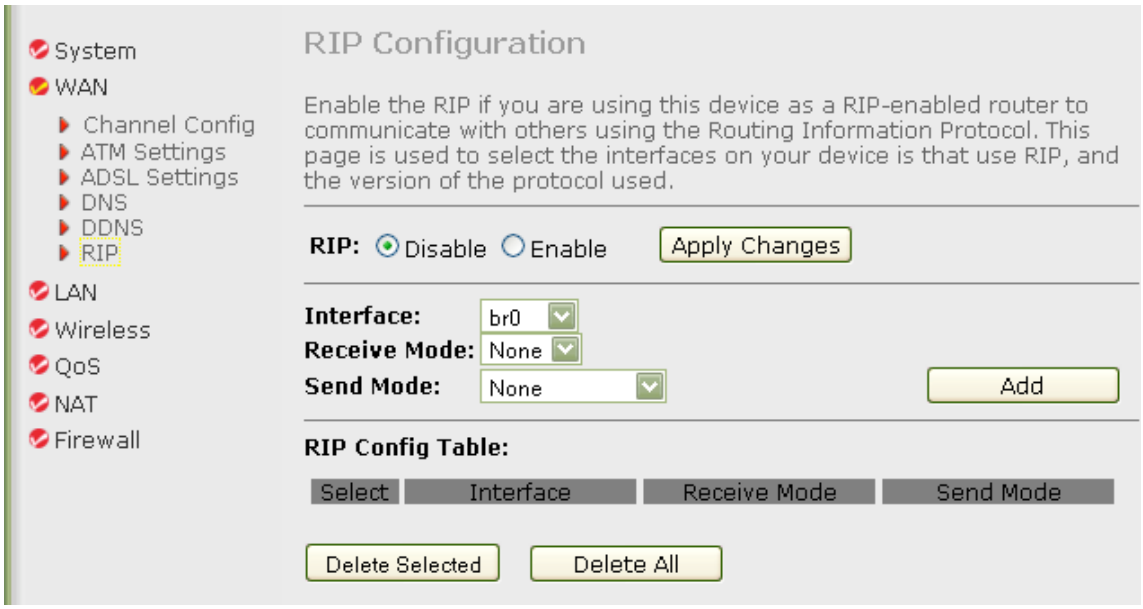
Most small home or office networks do not need to use RIP; they have only one router, such as this one, and one path to an ISP. In these cases, there is no need

Ex.1017
CISCO SYSTEMS, INC. / Page 45 of 100

to share routes because all Internet data from the network is sent to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC (other than this one). This router and the other router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.



Parameter	Description
RIP	Enable/disable the RIP feature.
Interface	Select the interface that you want to enable the RIP feature.
Receive Mode	Indicate the RIP version in which information must be passed to the DSL device in order for it to be accepted into its routing table.
Send Mode	Indicate the RIP version this interface will use when it sends its route information to other devices.

Ex.1017
CISCO SYSTEMS, INC. / Page 46 of 100

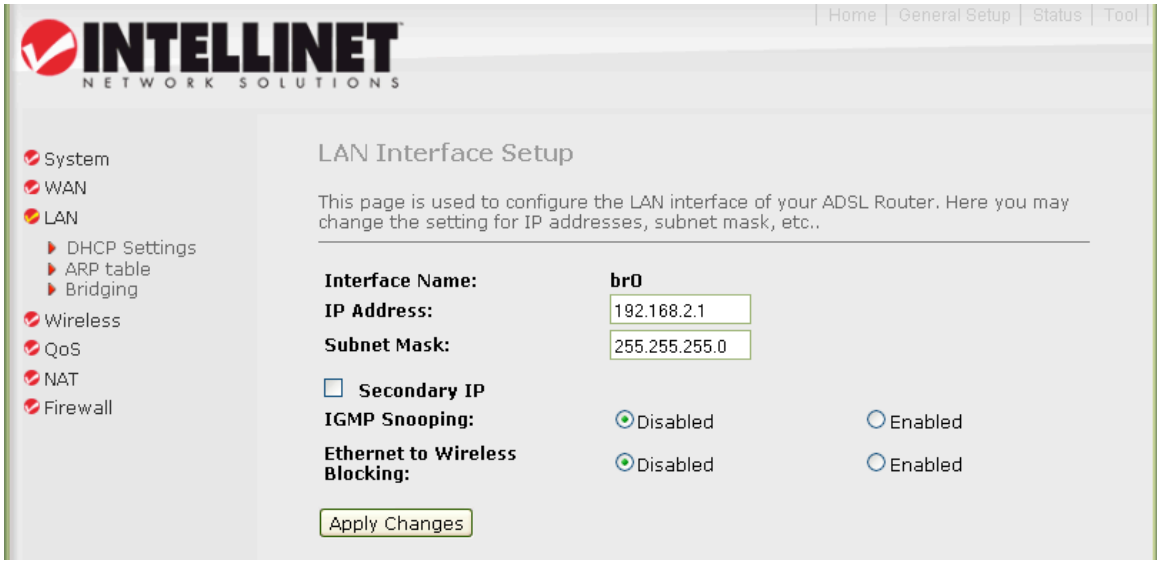
RIP Config Table	The RIP you have configured will be listed in the table. If you want to delete some settings, select the settings and click “Delete Selected.”

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.3 LAN

This screen is used to configure the LAN interface of this router. You can set IP address, subnet mask and IGMP Snooping.



Parameter	Description
Interface Name	The interface name is “br0.”
IP Address	Enter the IP address of the ADSL router for the local user to access the router’s Web screen. By default, the IP address is **192.168.2.1**.
Subnet Mask	Enter the subnet mask of the ADSL router. By default, the subnet mask is **255.255.255.0**.
Secondary IP	Assign a second IP address to the LAN.
IGMP Snooping	Enable/disable the IGMP snooping function for the multiple bridged LAN ports. When “IGMP Snoop” (Internet Group Management Protocol Snoop) is enabled, the router can make intelligent multicast forwarding decisions by examining the contents of each frame’s IP header. Without the function, the router will broadcast the multicast packets to each port and may create excessive traffic on the network and degrade the performance of the network.
Ethernet to Wireless Blocking	Enable/disable the “Ethernet to Wireless Blocking.” When this function is enabled, the traffic between Ethernet and wireless interfaces is not allowed.

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

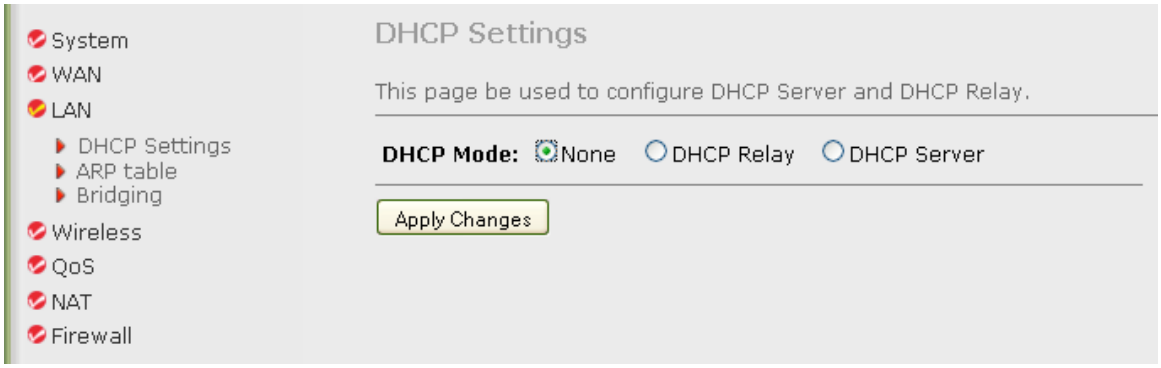
Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

Ex.1017
CISCO SYSTEMS, INC. / Page 48 of 100

5.2.3.1 DHCP Mode

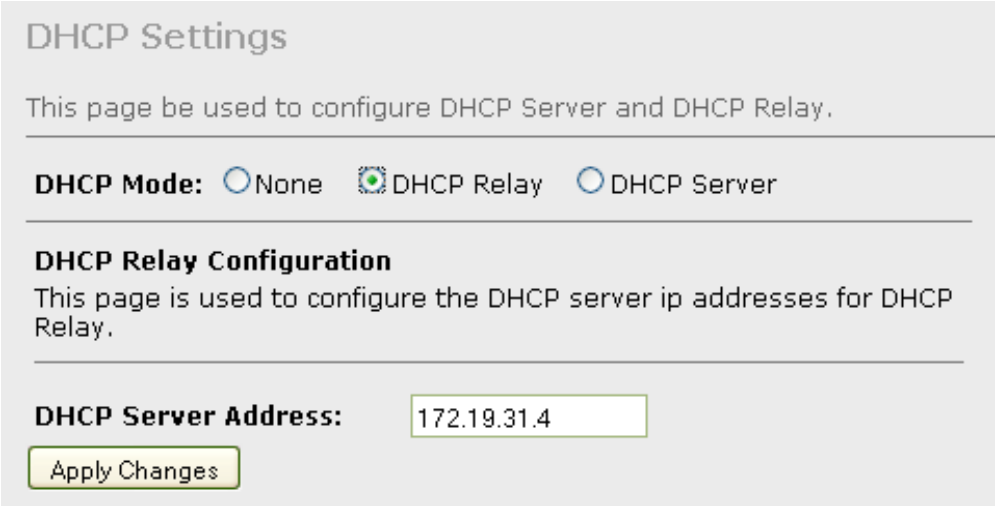
You can configure your network and the router to use the Dynamic Host Configuration Protocol (DHCP). This screen allows you to select the DHCP mode that this router will support.

There are two different DHCP modes: DHCP Server and DHCP Relay. When the router is acting as a DHCP server, configure it on the DHCP Server screen; while acting as a DHCP relay, you can set up the relay on the DHCP Relay screen.



5.2.3.2 DHCP Relay

Some ISPs perform the DHCP server function for their customers' home/small office network. In this case, you can configure this device to act as a DHCP relay agent. When a user's computer on your network requests Internet access, the router contacts your ISP to obtain the IP configuration, and then forwards that information to the computer.



Ex.1017
CISCO SYSTEMS, INC. / Page 49 of 100

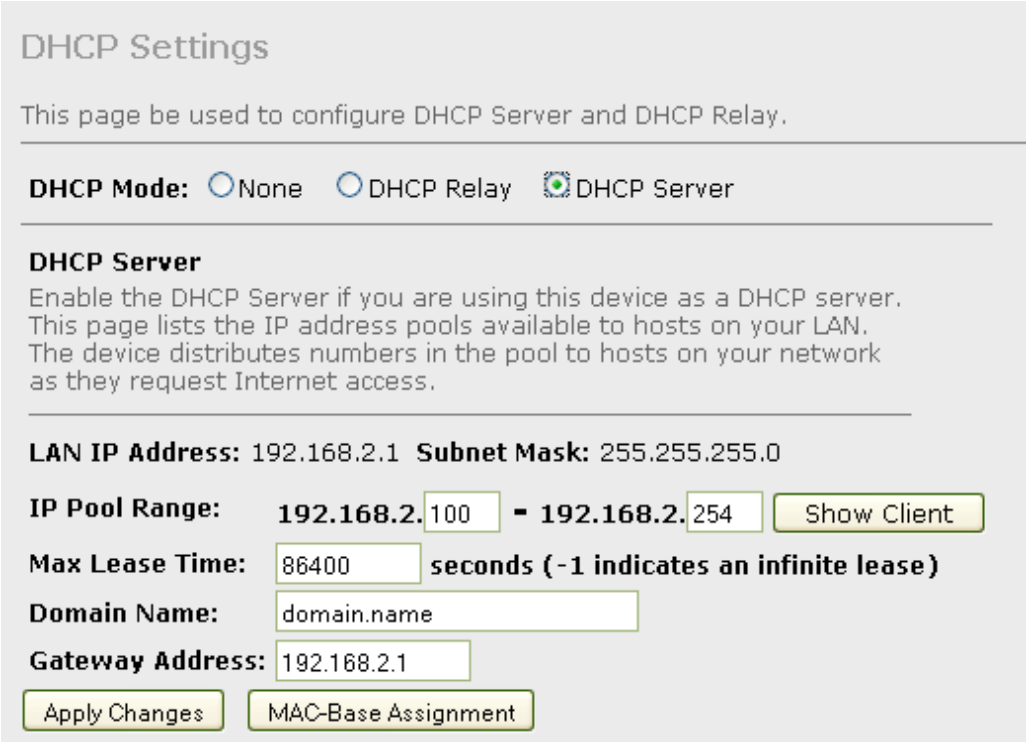
Parameter	Description
DHCP Server Address	Specify the IP address of your ISP's DHCP server. Requests for IP information from your LAN interface will be passed to the default gateway, which should route the request appropriately.

When you finish, click "Apply Changes." You'll see the following message displayed on Web browser.

Click "Continue" to save the settings made and go back to the Web management interface; click "Apply" to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.3.3 DHCP Server

When the DHCP server is enabled, the router will automatically give your LAN clients an IP address. If the DHCP is not enabled, then you'll need to manually set your LAN clients' IP addresses.



Parameter	Description
LAN IP Address	The current IP address of the router.
Subnet Mask	The current subnet mask of the router.
IP Pool Range	You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN clients. By default, the IP range is from 192.168.2.100 to 192.168.2.200.
Show Client	Click and a table is displayed, presenting the assigned IP address, MAC address and time expired for each DHCP leased client.
Subnet Mask	Enter the subnet mask for LAN clients.
Max Lease Time	In the Lease Time setting, you can specify the time period that the DHCP server lends an IP address to your LAN clients. The DHCP will change your LAN clients' IP address when this time threshold period is terminated.
Domain Name	A user-friendly name that refers to the group of hosts (subnet) that will be assigned addresses from this pool.
Gateway Address	The IP address of the router.
MAC Base Assignment	Click and you can assign a static IP address to the computer with the designated MAC address. The MAC address is the 12-digit hexadecimal number; for example, "00-d0-59-c6-12-43." The assigned IP address should be a unique IP address.

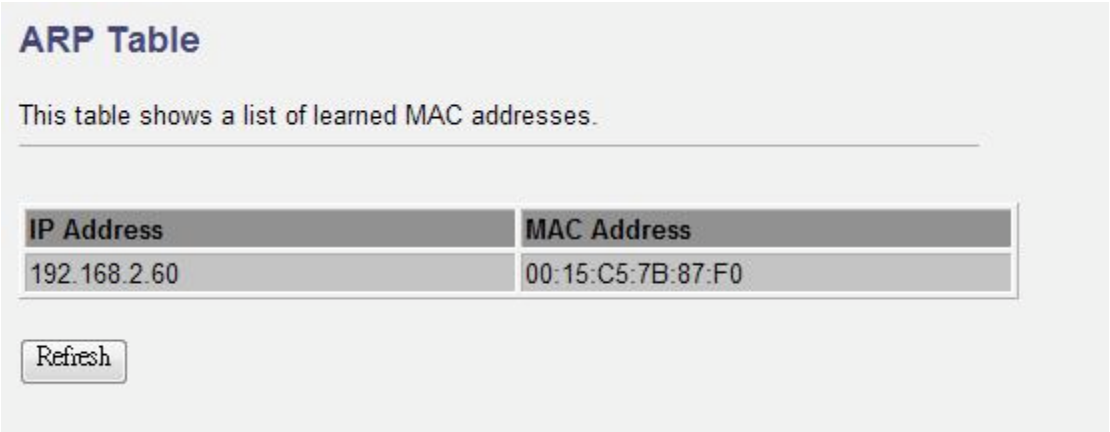
When you finish, click "Apply Changes." You'll see the following message displayed on Web browser.

Click "Continue" to save the settings made and go back to the Web management interface; click "Apply" to save the settings made and restart the router so the settings will take effect after it reboots.

Ex.1017
CISCO SYSTEMS, INC. / Page 51 of 100

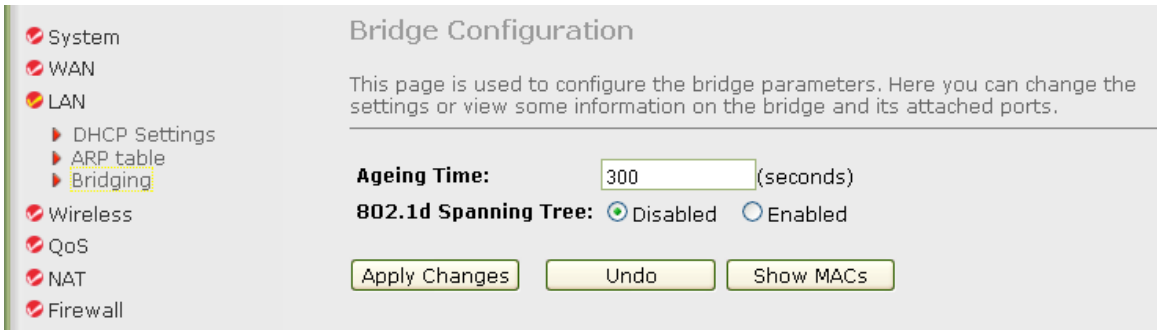
5.2.3.4 ARP Table

ARP is the Address Resolution Protocol. Its job is to match MAC addresses to IP addresses and vice versa (matching IP addresses to MAC addresses). This screen lists the IP addresses and the matched MAC addresses in the network.



5.2.3.5 Bridging

You can enable/disable the Spanning Tree Protocol and set the MAC address aging time on this screen.



Parameter	Description
Aging Time	Set the Ethernet address ageing time. After the aging time of not having seen a frame coming from a certain address, the bridge will time out (delete) and not forward the frame.
802.1d Spanning Tree	Enable/disable the Spanning Tree Protocol. When this feature is enabled, this router will use the Spanning Tree Protocol to prevent a network loop from forming in the network (LAN side).

Ex.1017
CISCO SYSTEMS, INC. / Page 52 of 100

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

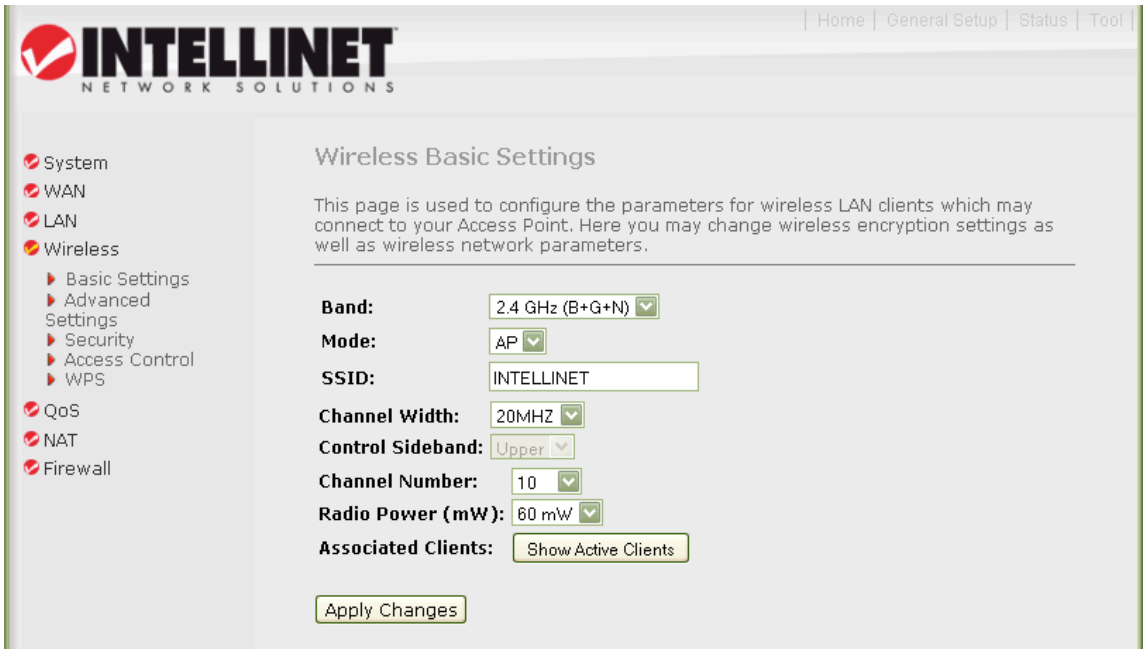
Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.4 Wireless

The router builds a wireless LAN and can let all IEEE 802.11b, IEEE 801.11g or IEEE 802.1n wireless stations connect to your intranet. It supports WEP, WPA and WPA2 encryption to enhance the security of your wireless network. It also supports WPS so you can easily set up the wireless connection between the router and other stations.

5.2.4.1 Basic Settings

This section provides the wireless network settings for your router. You can enable the wireless AP function here.



Parameter	Description
Disable Wireless LAN Interface	Check to deactivate the wireless function of the router. When this is activated, the router will not be an access point for other wireless clients to connect wirelessly.
Band	Select the radio band from one of the following options: • 2.4GHz(B): only allows 802.11b wireless network clients to connect to this router (maximum transfer rate is 11 Mbps). • 2.4 GHz (G): only allows 802.11g wireless network clients to connect to this router (maximum transfer rate is 54 Mbps). • 2.4 GHz (B+G): only allows 802.11b and 802.11g wireless network clients to connect to this router (maximum transfer rate is 11 Mbps for 802.11b clients; 54 Mbps for 802.11g clients). • 2.4 GHz (N): only allows 802.11n wireless network clients to connect to this router (maximum transfer rate is 150 Mbps). • 2.4 GHz (G+N): only allows 802.11g and 802.11n wireless network clients to connect to this router (maximum transfer rate is 54 Mbps for 802.11g clients; 150 Mbps for 802.11n clients). • 2.4 GHz (B+G+N): allows 802.11b, 802.11g and 802.11n wireless network clients to connect to this router (maximum transfer rate is 11 Mbps for 802.11b clients; 54 Mbps for 802.11g clients; 150 Mbps for 802.11n clients).
Mode	Set the router to act in AP, Client or WDS mode.
SSID	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. The default SSID of the router is “default.”
Channel Width	Sets the channel width of the wireless radio. Do not modify the default value if you don’t know what it is. The default setting is “Auto 20/40 MHz.”

Ex.1017
CISCO SYSTEMS, INC. / Page 54 of 100

Control Sideband	Select the upper band or lower band for your radio frequency. While “Upper” is selected, the channel options are from 5 to 11. While “Lower” is selected, the channel options are from 1 to 7.
Channel Number	This is the radio channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel. Select the country and designate a channel that the router will use. To let the router automatically find an available channel with the highest signal strength, select “Auto.”
Radio Power (mW)	Sets the maximum output power of the router. The higher the output power, the wider the coverage range.
Associated Clients	Click to see the wireless clients connected to the router.

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.4.2 Advanced Settings

This screen allows advanced users who have sufficient knowledge of wireless LANs to make configuration changes. These settings shouldn’t be changed unless you know exactly what will happen as a result.

Ex.1017
CISCO SYSTEMS, INC. / Page 55 of 100

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
Relay Blocking:	○ Enabled ◉ Disabled
Protection:	○ Enabled ◉ Disabled
Aggregation:	◉ Enabled ○ Disabled
Short GI:	○ Enabled ◉ Disabled

Apply Changes

Parameter	Description
Authentication Type	There are three authentication types: Open System, Shared Key and Auto. • Open System authentication is not required to be successful, as a client may decline to authenticate with any other particular client. • Shared Key is only available if the WEP option is implemented. Shared Key authentication supports authentication of clients as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in clear. Requires the use of the WEP privacy mechanism.

	• Auto is the default authentication algorithm. It will change its authentication type automatically to fulfill a client's requirement.
Fragmentation Threshold	Fragment Threshold specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance. Enter a value from 256 to 2346.
RTS Threshold	This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset "RTS Threshold" size, the RTS/CTS mechanism will not be enabled. The wireless router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.
Beacon Interval	This is the interval of time that this wireless router broadcasts a beacon, which is used to synchronize the wireless network. The range for the beacon period is 20 to 1024, with a default value of 100 (milliseconds).
Data Rate	This setting depends on the speed of your wireless network. You should select from a range of transmission speeds, or you can select "Auto" to have the wireless router automatically use the fastest possible data rate and enable the Auto-Fallback feature, which negotiates the best possible connection speed between the router and a wireless client. The default setting is "Auto."
Preamble Type	This defines the length of the CRC (Cyclic Redundancy Check) block for communication between the router and wireless stations. Make sure to select the appropriate preamble type. Note that high network traffic areas should use "Short Preamble." CRC is a common technique for detecting data transmission errors.
Broadcast SSID	If this option is enabled, the router will automatically

Ex.1017
CISCO SYSTEMS, INC. / Page 57 of 100

	transmit the network name (SSID) into open air at regular intervals. This feature is intended to allow clients to dynamically discover the router. If this option is disabled, the router will hide its SSID. When this is done, the clients cannot directly discover the router and MUST be configured with the SSID for access to the router. It is used to protect your network from being accessed easily.
Relay Blocking	When you enable this function, wireless clients will not be able to directly access other wireless clients.
Protection	This is also called CTS Protection. It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g/802.11n wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower.
Aggregation	This is used to join multiple data packets for transmission as a single unit to increase network efficiency.
Short GI	The 802.11n draft specifies two guard intervals: 400 ns (short) and 800 ns (long). Support of the 400 ns GI is optional for transmit and receive. Enabling this function will increase network efficiency.

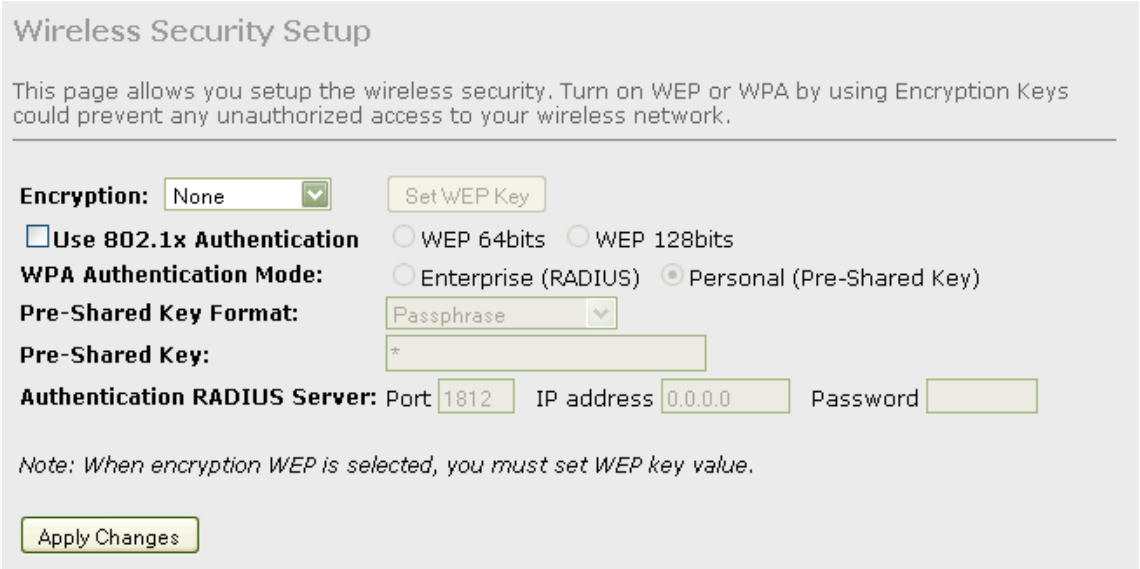
When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

Ex.1017
CISCO SYSTEMS, INC. / Page 58 of 100

5.2.4.3 Security

This router provides complete wireless LAN security functions, including WEP, IEEE 802.1x, IEEE 802.1x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can protect your wireless LAN from illegal access. Make sure your wireless stations use the same security function.



Parameter	Description
Encryption	Choose “None” to disable the encryption, or select “WEP,” “WPA(TKIP),” “WPA2(AES)” or “WPA2 Mixed” mode for security. When “WEP” is enabled, click “Set WEP Key” to choose the default key and set the four sets of WEP keys. • WEP is a lower level of security than WPA, and supports 64-bit and 128-bit key lengths to encrypt the wireless data. • WPA (TKIP) uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. • WPA2 (AES) uses the Advanced Encryption Standard (AES) for data encryption, which utilizes a symmetric 128-bit block data encryption. • WPA Mixed tells the router to support WPA (TKIP) and

Ex.1017
CISCO SYSTEMS, INC. / Page 59 of 100

	WPA2 (AES) for data encryption. The actual selection of the encryption methods will depend on the clients.
Use 802.1x Authentication	IEEE 802.1x is an authentication protocol. Every user must use a valid account to log in to this wireless router before accessing the wireless LAN. The authentication is processed by a RADIUS server. Check this box to authenticate a user by IEEE 802.1x.
WEP-64Bits	WEP is a lower level of security than WPA, and supports 64-bit and 128-bit key lengths to encrypt the wireless data. The longer key length will provide higher security. When “WEP-64Bits” is selected, you need to enter exactly 5 ASCII characters (“a-z” and “0-9”) or 10 hexadecimal digits (“0-9,” “a-f”) for each Key (1-4).
WEP-128Bits	When “WEP-128Bits” is selected, you need to enter exactly 13 ASCII characters (“a-z” and “0-9”) or 26 hexadecimal digits (“0-9,” “a-f”) for each Key (1-4).
WPA Authentication Mode	There are two types of authentication mode for WPA. • Enterprise (RADIUS) uses an external RADIUS server to perform user authentication. To use RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. Refer to the “Authentication RADIUS Server” setting below for RADIUS setting. • Personal (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved. To use WPA Pre-Shared Key, select the key format and enter a password in the “Pre-Shared Key Format” and “Pre-Shared Key” settings.
Pre-Shared Key Format	You can select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F,” “a-f” and “0-9” range) to be the Pre-shared Key. For example: Passphrase: ”iamguest” Hexadecimal Digits: “12345abcde”
Pre-Shared Key	Enter 8-63 characters as the “Pre-Shared Key.”
Authentication	Enter the port (default is 1812), the IP address and the

Ex.1017
CISCO SYSTEMS, INC. / Page 60 of 100

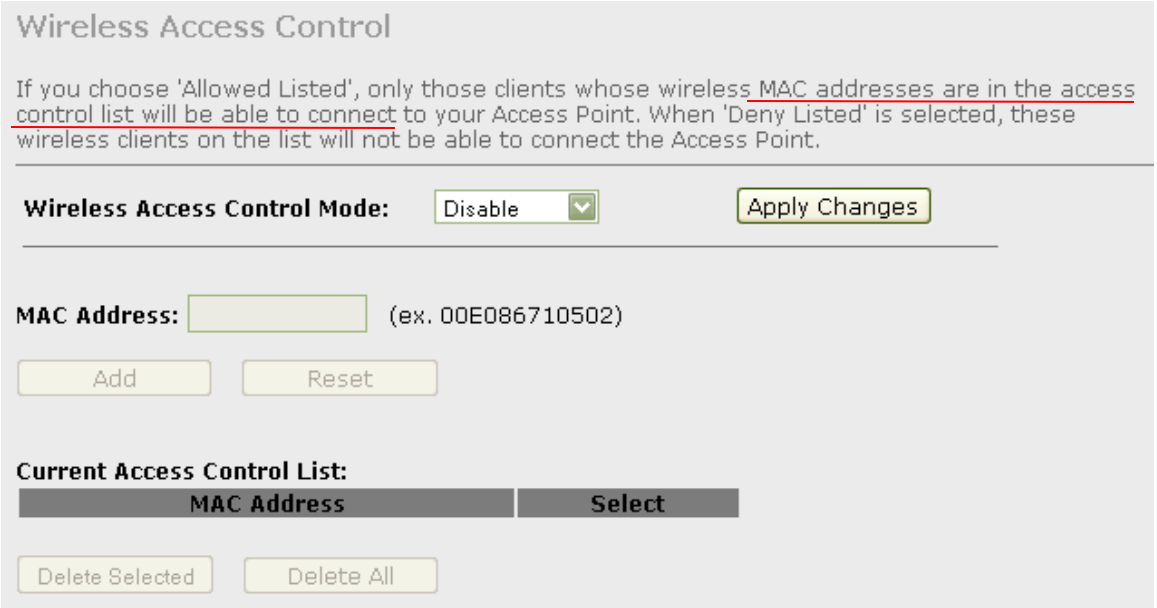
RADIUS Server	password of the external RADIUS server.

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.4.4 Access Control

This wireless router provides MAC Address Control, which prevents unauthorized MAC addresses from accessing your wireless network.



Parameter	Description
Wireless Access Control Mode	This router can prevent wireless clients from accessing the wireless network by checking the MAC address of the

Ex.1017
CISCO SYSTEMS, INC. / Page 61 of 100

	clients. If you enable this function, set the MAC address of the wireless clients that you want to filter. Disable disables this function. Allow Listed only allows the wireless clients with the MAC address you have specified access to the router. Deny Listed means the wireless clients with the MAC address you have specified will be denied access to the router.
MAC Address	Enter the MAC address of the wireless clients for the filtering control.
Current Access Control List	To remove a MAC address from the Current Access Control List, select it and click “Delete Selected.” To remove all MAC addresses from the table, just click “Delete All.” Click “Reset” to clear your current selections.

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

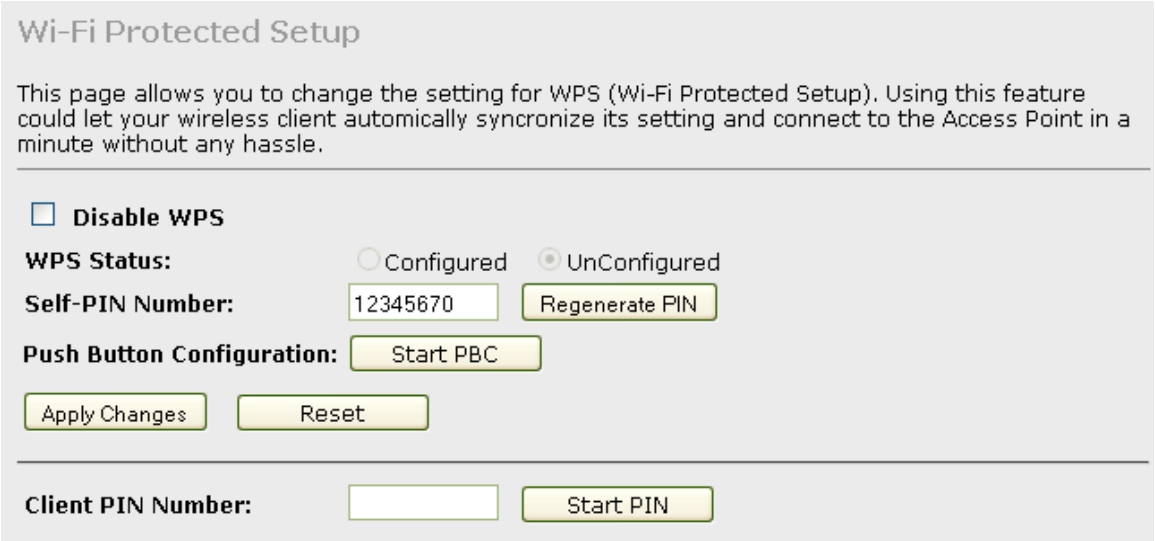
Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.4.5 WPS

Although home Wi-Fi networks have become more and more popular, users still have trouble with the initial setup of a network. This obstacle forces users to use an open security setting and increases the risk of eavesdropping. Wi-Fi Protected Setup (WPS) was designed to make it easier to set up security-enabled Wi-Fi networks and, subsequently, network management.

The biggest difference between WPS-enabled devices and legacy devices is that users do not need to know about SSID or channel and security settings, but they could still surf in a security-enabled Wi-Fi Network. This device supports both the Push Button and PIN methods for WPS, as described below.

Ex.1017
CISCO SYSTEMS, INC. / Page 62 of 100



Parameter	Description
Disable WPS	Check to disable Wi-Fi Protected Setup.
WPS Status	When the settings are factory defaults (out of the box), it is set to an open security and unconfigured state. “WPS Status” will display it as “UnConfigured.” If it already shows “Configured,” some registrars such as Vista WCN will not configure the router, and you’ll need to go to the Backup/Restore screen and click “Reset” to reload the factory default settings.
Self-PIN Number	“Self-PIN Number” is the router’s PIN. Whenever you want to change the PIN, click “Regenerate PIN” and “Apply Changes.” To create your own PIN, enter a four-digit PIN without checksum and click “Apply Changes.” However, this would not be recommended, since the registrar side needs to be supported with a four-digit PIN.
Regenerate PIN	Click to regenerate the Self-PIN Number.
Push Button Configuration	Clicking this button will invoke the PBC method of WPS. It is only used when the router acts as a registrar.
Start PBC	Click to start the Push Button method of WPS.
Reset	Click to restore the original values.
Client PIN Number	This is only used when users want their station to join the router’s network. The length of the PIN is limited to four

Ex.1017
CISCO SYSTEMS, INC. / Page 63 of 100

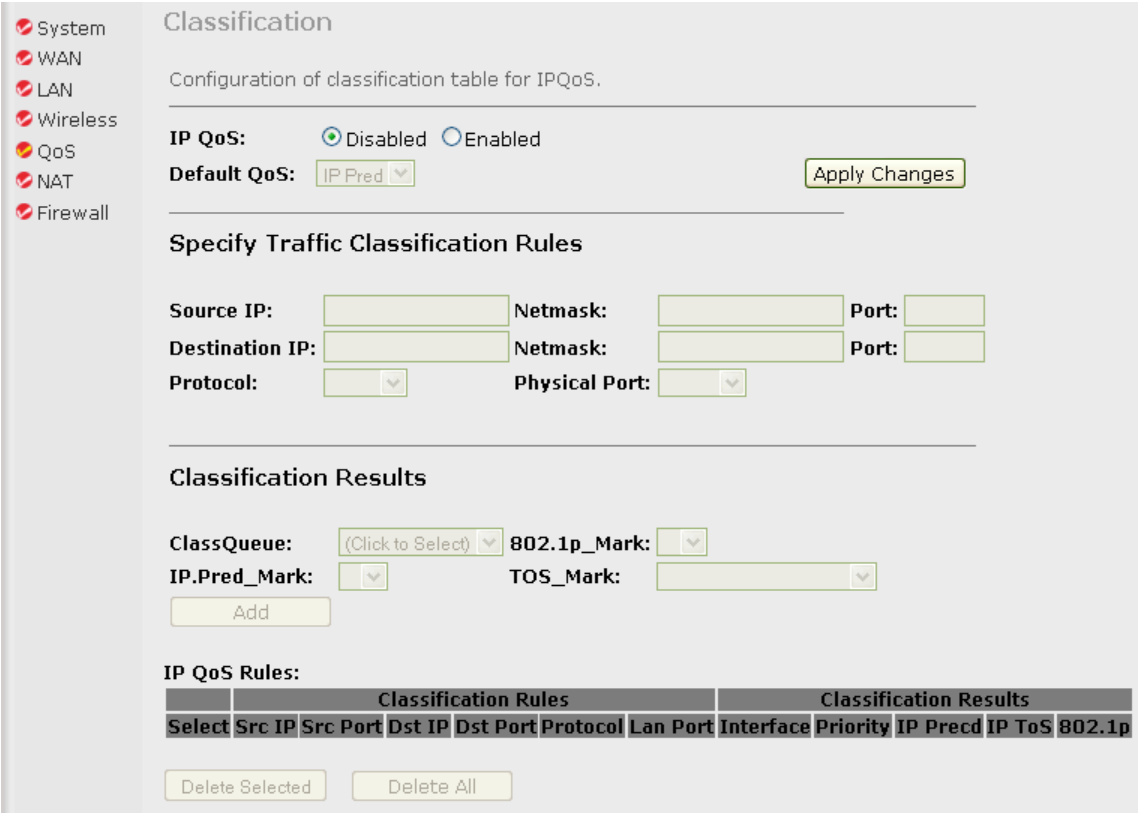
or eight numeric digits. If users enter an eight-digit PIN with checksum error, a warning message pops up. If users insist on this PIN, the router will take it.

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.5 QoS

The router supports the IP QoS feature, which can provide different priorities to different users or data flows.



Parameter	Description
IP QoS	Click the radio button to enable or disable the function.
Default QoS	Select the default mode of QoS from the menu. • IP Precedence: In QoS, a three-bit field in the ToS byte of the IP header (see RFC 791). Using IP Precedence, a network administrator can assign values from 0 (the default) to 7 to classify and prioritize types of traffic. • 802.1P: IEEE 802.1p is a three-bit field within an Ethernet frame header when using tagged frames on an 802.1 network. It specifies a priority value between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic.
Source IP	The IP address of the traffic source.
Source Netmask	The source IP netmask. This field is required if the source IP has been entered.
Source Port	The source port of the selected protocol. You cannot configure this field without entering the protocol first.
Destination IP	The IP address of the traffic destination.
Destination Netmask	The destination IP netmask. This field is required if the destination IP has been entered.
Destination Port	The destination port of the selected protocol. You cannot configure this field without entering the protocol first.
Protocol	The selections are TCP, UDP, ICMP and blank for none. This field is required if the source port or destination port has been entered.
Physical Port	The incoming ports. The selections include LAN ports, wireless port and blank for not applicable.
Outbound Priority	The priority level for the traffic that matches this classification rule. The possible selections are (in the descending priority): p0, p1, p2, p3.
802.1p	Select this field to mark the three-bit user-priority field in the 802.1p header of the packet that matches this classification rule. Note that this 802.1p marking is workable on a given PVC channel only if the VLAN tag is enabled in this PVC channel.

Ex.1017
CISCO SYSTEMS, INC. / Page 65 of 100

Precedence	Select this field to mark the IP precedence bits in the packet that match this classification rule.
TOS	The IP (Internet Protocol) uses the ToS (Type of Service) field to provide an indication of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting an IP datagram through a particular network.
IP QoS Rules	This table lists the rules you have configured. Click "Delete Selected" to delete the selected rules or click "Delete All" to delete all the rules.

When you finish, click "Apply Changes." You'll see the following message displayed on Web browser.

Click "Continue" to save the settings made and go back to the Web management interface; click "Apply" to save the settings made and restart the router so the settings will take effect after it reboots.

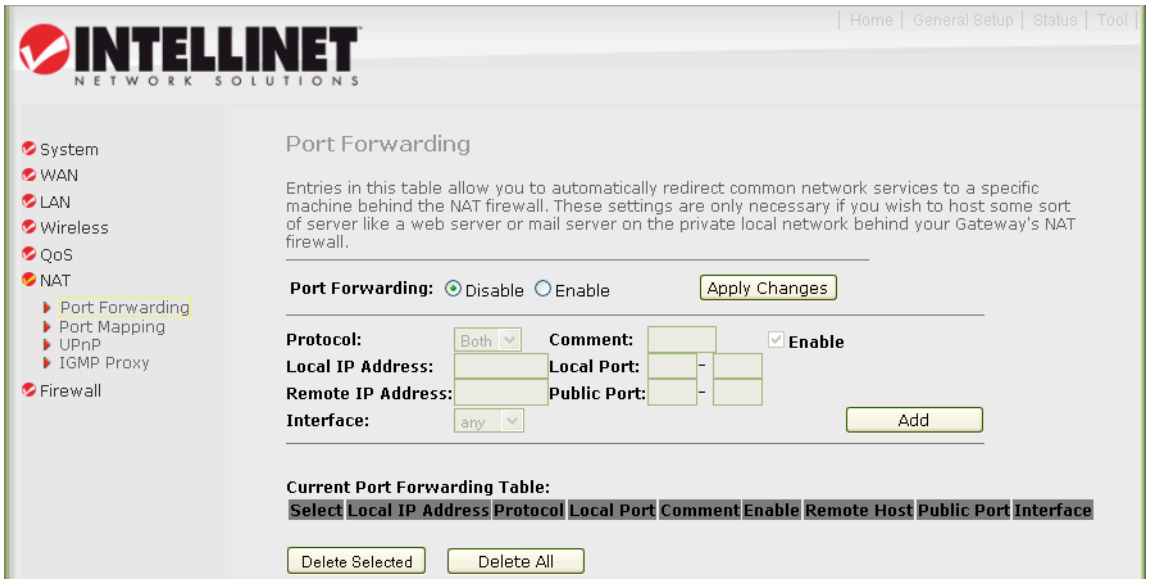
5.2.6 NAT (Network Address Translations)

NAT (network address translations) solve the problem of sharing a single IP address among multiple computers. Without NAT, all computers must be assigned with a valid Internet IP address to get connected to the Internet; but Internet service providers provide only a limited number of IP addresses to each user. Therefore, it's necessary to use NAT technology to share a single Internet IP address among multiple computers on local network so everyone can get connected.

Ex.1017
CISCO SYSTEMS, INC. / Page 66 of 100

5.2.6.1 Port Forwarding

Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet) to a particular LAN IP address. It helps you to host some servers behind the router's NAT firewall.



Parameter	Description
Port Forwarding	Check to enable or disable the port-forwarding feature.
Protocol	This is the protocol type to be forwarded. You can forward 'tCP" or "UDP" packets only, or you can select "Both" to forward both 'tCP" and "UDP" packets.
Comment	Enter any comments for the setting.
Enable	Check this item to enable this entry.
Local IP Address	IP address of your local server that will be accessed by the Internet.
Local IP Port	The destination port number that is made open for this application on the LAN side.
Remote IP Address	The source IP address from which incoming traffic is allowed. Leave blank for all.
Public Port	The destination port number that is made open for this application on the WAN side.
Interface	Select the WAN interface on which the port-forwarding rule is to be applied.
Current Port	To remove the port forwarding settings from the table,

Ex.1017
CISCO SYSTEMS, INC. / Page 67 of 100

Forwarding Table	select the items and click “Delete Selected.” To remove all settings, just click “Delete All.”

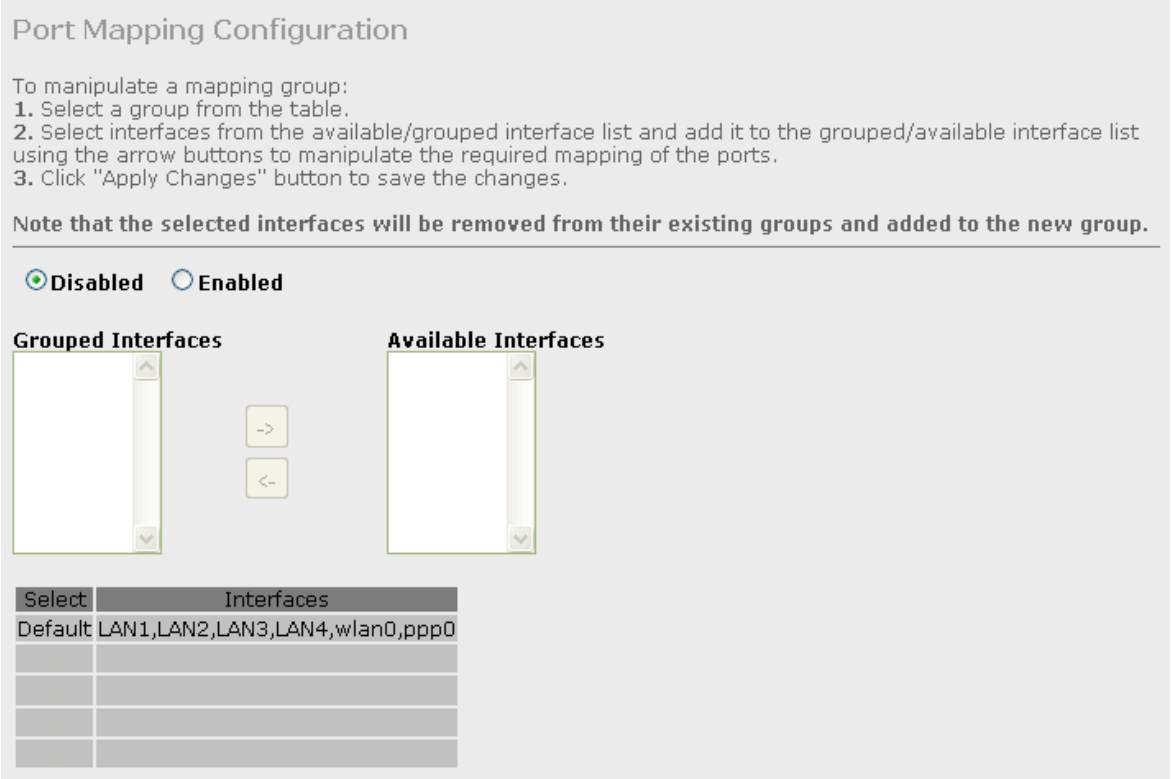
When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.6.2 Port Mapping

The router provides multiple interface groups. Up to five interface groups are supported, including one default group. The LAN and WAN interfaces could be included. Traffic coming from one interface of a group can only be flowed to the interfaces in the same interface group. Thus, the router can isolate traffic from group to group for some applications. By default, all the interfaces (LAN and WAN) belong to the default group, and the other four groups are all empty. It is possible to assign any interface to any one group.

Ex.1017
CISCO SYSTEMS, INC. / Page 68 of 100



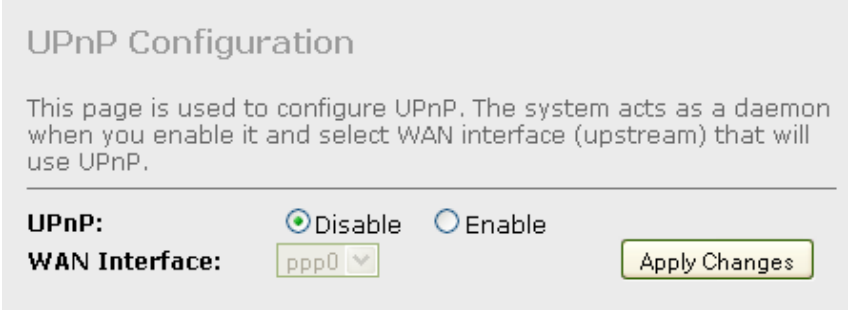
Parameter	Description
Disabled/Enabled	Click the radio button to enable or disable the feature. If disabled, all interfaces belong to the default group.
Interface groups	To manipulate a mapping group: 1. Select a group from the table. 2. Select interfaces from the available/grouped interface list and add to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.6.3 UPNP

When the UPnP function is enabled, the router can be detected by UPnP-compliant systems such as Windows XP. The router will be displayed in the Neighborhood of Windows XP, so you can directly double-click the router or right- click the router and select “Invoke” to configure the router through a Web browser.



Parameter	Description
UPnP	Enable or disable the UPnP feature.
WAN Interface	The upstream WAN interface is selected here. Select a WAN interface that will use UPnP from the drop-down menu.

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

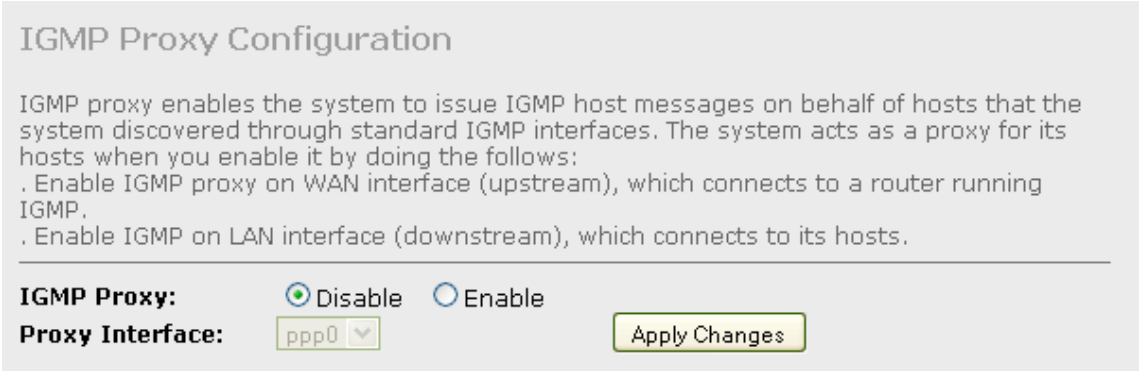
Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

Ex.1017
CISCO SYSTEMS, INC. / Page 70 of 100

5.2.6.4 IGMP Proxy

When IGMP Proxy (Internet Group Management Protocol Proxy) is enabled, the router can make intelligent multicast forwarding decisions by examining the contents of each frame's IP header. Without the function, the router will broadcast the multicast packets to each port and may create excessive traffic on the network and degrade the performance of the network.

The IGMP Proxy screen allows you to enable multicast on WAN and LAN interfaces. The LAN interface always serves as a downstream IGMP proxy, and you can configure one of the available WAN interfaces as the upstream IGMP proxy. Upstream is the interface used when IGMP requests from hosts are sent to the multicast router. Downstream is the interface used when data from the multicast router are sent to hosts in the multicast group database.



Parameter	Description
IGMP Proxy	Enable or disable the IGMP proxy feature.
Proxy Interface	The upstream WAN interface is selected here.

When you finish, click "Apply Changes." You'll see the following message displayed on Web browser.

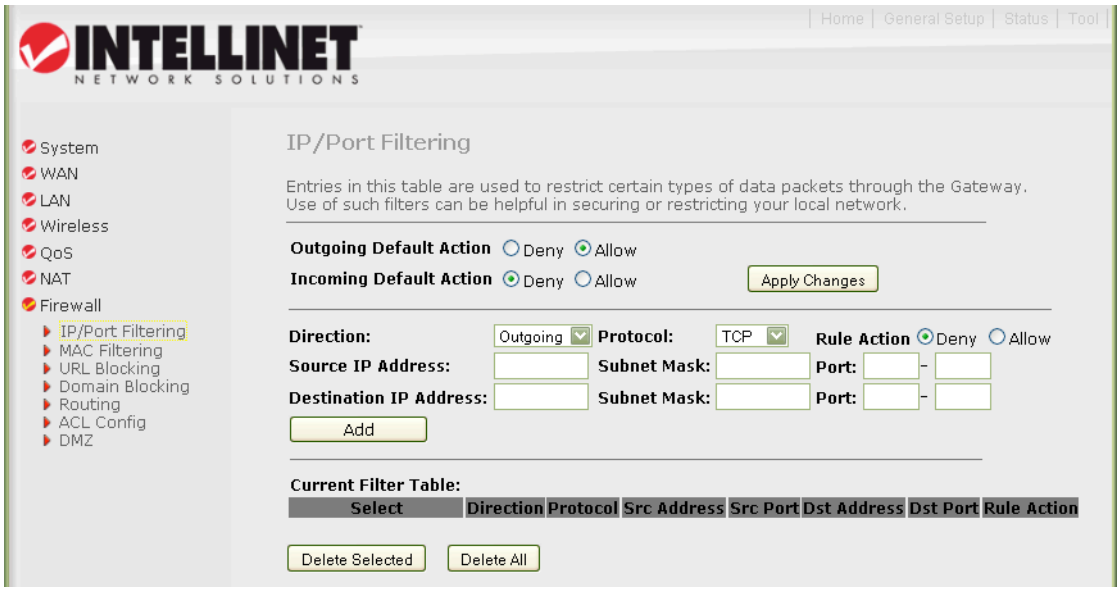
Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.7 Firewall

The Firewall section contains several features that are used to deny or allow traffic from passing through the router.

5.2.7.1 IP/Port Filtering

The IP/Port Filtering feature allows you to deny/allow specific services or applications in the forwarding path.



Parameter	Description
Outgoing Default Action	Specify the default action on the LAN-to-WAN (Traffic-to-Internet) forwarding path. Choose “Allow” to allow the IP addresses listed in the following table to connect to the Internet; choose “Deny” to deny the IP addresses listed in the following table from connecting to the Internet.
Incoming Default Action	Specify the default action on the WAN-to-LAN (Traffic-from-Internet) forwarding path. Choose “Allow” to allow the IP addresses listed in the following table to connect to the Internet; choose “Deny” to deny the IP addresses

Ex.1017
CISCO SYSTEMS, INC. / Page 72 of 100

	listed in the table from connecting to the Internet.
Direction	Select the traffic forwarding direction: outgoing or incoming.
Protocol	There are three options available: TCP, UDP and ICMP.
Rule Action	Deny or allow traffic when matching this rule.
Source IP Address	Enter the start IP address that will be monitored.
Subnet Mask	Enter the subnet mask based on the source IP address.
Port	LAN users use port numbers to distinguish one network application from another; for example, 21 is for FTP service. The port number range is from 0 to 65535. It is recommended that this option be configured by an advanced user.
Destination IP Address	Enter the destination IP address that will be monitored.
Subnet Mask	Enter the subnet mask based on the destination IP address.
Port	This is the port or port ranges that define the application.
Current Filter Table	To remove some IP/Port Filter settings from the Current Filter Table, select the items you want to remove in the list and click “Delete Selected.” To remove all the items from the table, click “Delete All.”

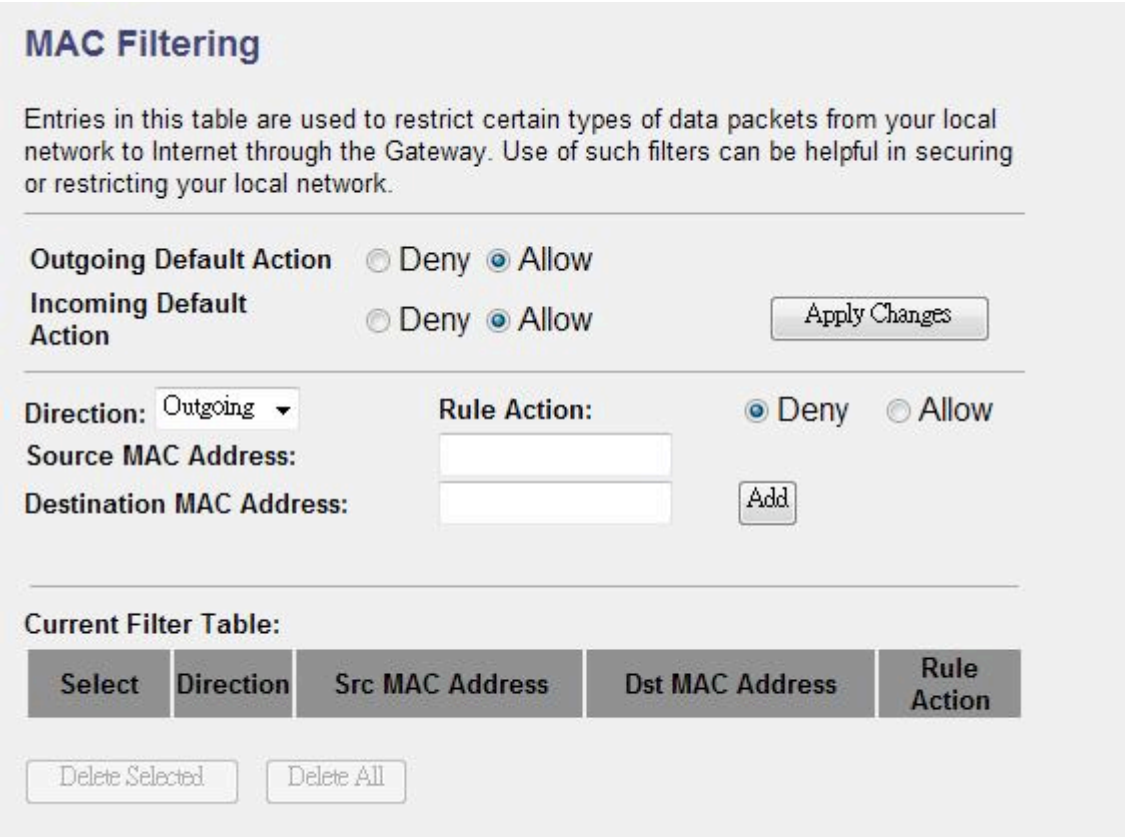
When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

Ex.1017
CISCO SYSTEMS, INC. / Page 73 of 100

5.2.7.2 MAC Filtering

The MAC Filtering feature allows you to define rules to allow or deny frames through the router based on source MAC address, destination MAC address and traffic direction.



Parameter	Description
Outgoing Default Action	Specify the default action on the LAN-to-WAN (Traffic-to-Internet) forwarding path. Choose “Allow” to allow the IP addresses listed in the following table to connect to the Internet; choose “Deny” to deny access.
Incoming Default Action	Specify the default action on the WAN-to-LAN (Traffic-from-Internet) forwarding path. Choose “Allow” to allow the IP addresses listed in the following table to connect to the Internet; choose “Deny” to deny access.
Direction	Traffic bridging/forwarding direction: outgoing or incoming.
Rule Action	Deny or allow traffic when matching this rule.

Ex.1017
CISCO SYSTEMS, INC. / Page 74 of 100

Source MAC Address	This must be in 12-digit hexadecimal format; for example, “00-d0-59-c6-12-43.”
Destination MAC Address	This must be in 12-digit hexadecimal format; for example, “00-d0-59-c6-12-50.”
Current Filter Table	To remove some filter rules from the Current Filter Table, select the MAC address you want to remove and click “Delete Selected.” To remove all settings, click “Delete All.”

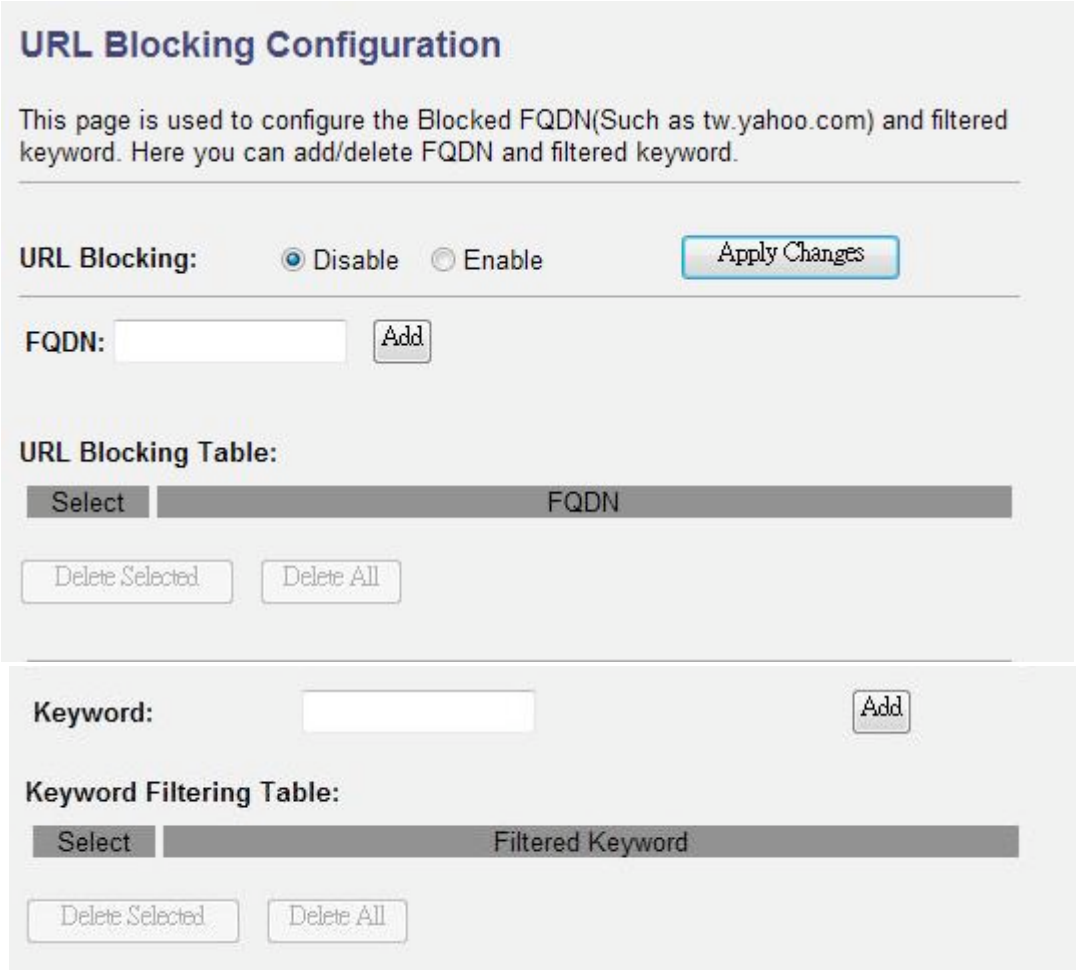
When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

Ex.1017
CISCO SYSTEMS, INC. / Page 75 of 100

5.2.7.3 URL Blocking

This screen is used to block some URL addresses or keywords.



Parameter	Description
URL Blocking	Enable or disable the URL Blocking function.
FQDN	Enter the FQDN which you want to block. A FQDN is a complete DNS name. For example, “www.yahoo.com.”
URL Blocking Table	The FQDN settings will be listed in the table. To delete some settings, select the settings and click “Delete Selected.” To remove all settings,click “Delete All.”
Keyword	Enter the keyword of the URL address you want to filter.
Keyword Filtering Table	The keyword settings will be listed in the table. To delete some keyword settings, select them and click “Delete Selected.” To remove all settings, click “Delete All.”

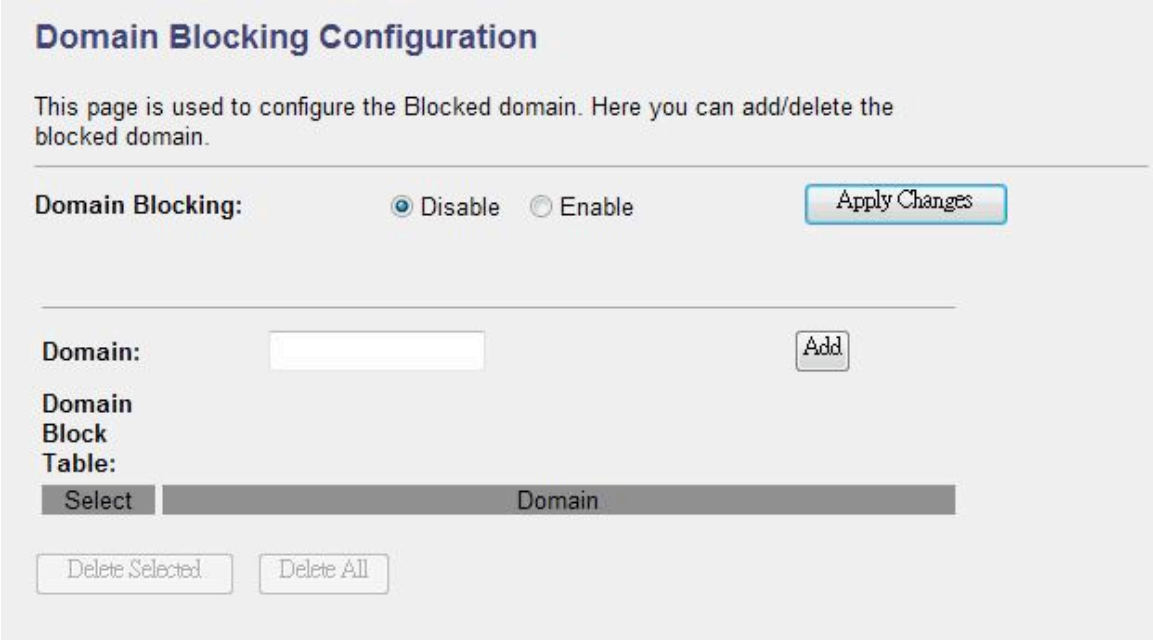
Ex.1017
CISCO SYSTEMS, INC. / Page 76 of 100

When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.7.4 Domain Blocking

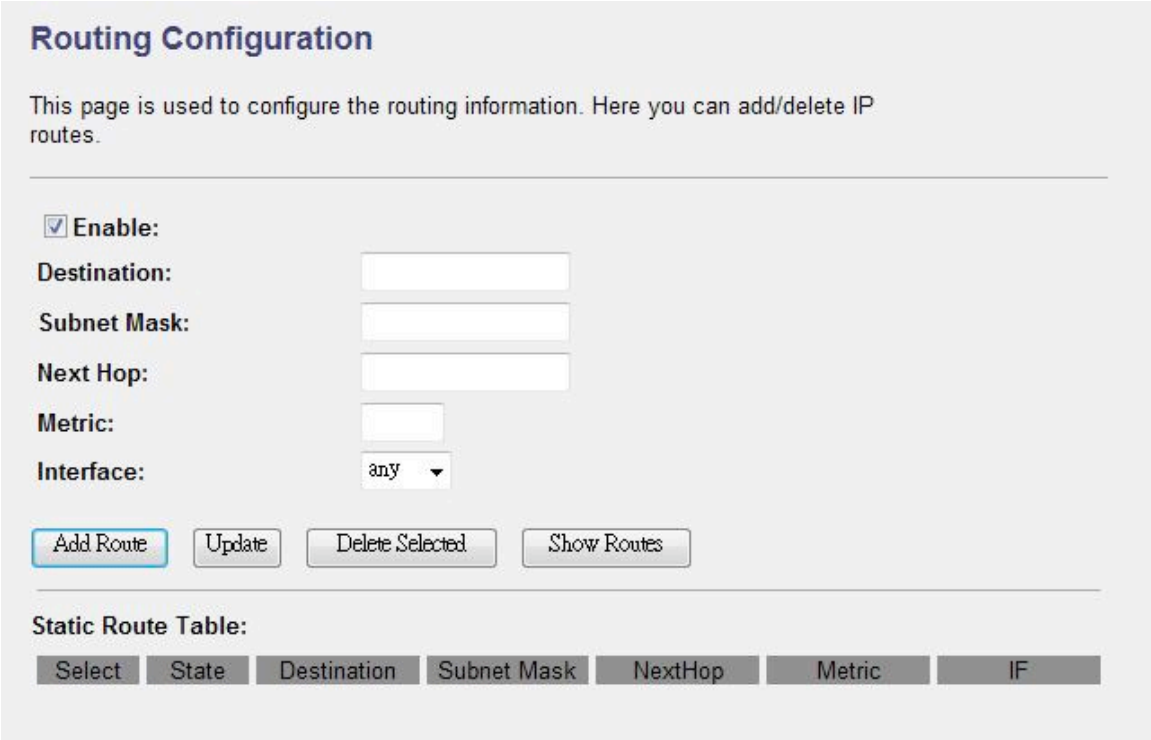
The firewall includes the ability to block access to specific domains based on string matches. For example, if the URL of the Martian Yahoo Web site is “ma.yahoo.com” and you enter “yahoo.com,” the firewall will block all the DNS queries with a “yahoo.com” string. So the host will be blocked from accessing all the URLs belonging to the “yahoo.com” domain. That means you can protect your computer, your house, your office and anything else that uses DNS from being able to service domains that you don’t want to load.



Parameter	Description
Domain Blocking	Check this item to enable the Domain Blocking feature.
Domain	The blocked domain. If the URL of the Mars Yahoo Web site is ma.yahoo.com, the domain can be yahoo.com.
Delete Selected/All	To delete a specific Domain Block entry, check the "Select" box of the Domain Block you want to delete, then click "Delete Selected." To remove all settings from the table, click "Delete All."

5.2.7.5 Routing Configuration

This screen enables you to define a specific route for your Internet and network data. Most users do not need to define routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN hosts and for the router provide the most appropriate path for all your Internet traffic. You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.



Parameter	Description
Enable	Check to enable the selected route or route to be added.

Ex.1017
CISCO SYSTEMS, INC. / Page 78 of 100

Destination	The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate the route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Subnet Mask	The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.
Next Hop	The IP address of the next hop through which traffic will flow toward the destination subnet.
Metric	Defines the number of hops between network nodes that data packets travel. The default value is 0, which means that the subnet is directly one hop away on the local LAN network.
Interface	The WAN interface to which a static routing subnet is to be applied.
Show Routes	Click to view the router's routing table.
Static Route Table	Click "Update" to update the selected destination route in the Static Route Table. Click "Delete Selected" to delete a selected destination route in the table.

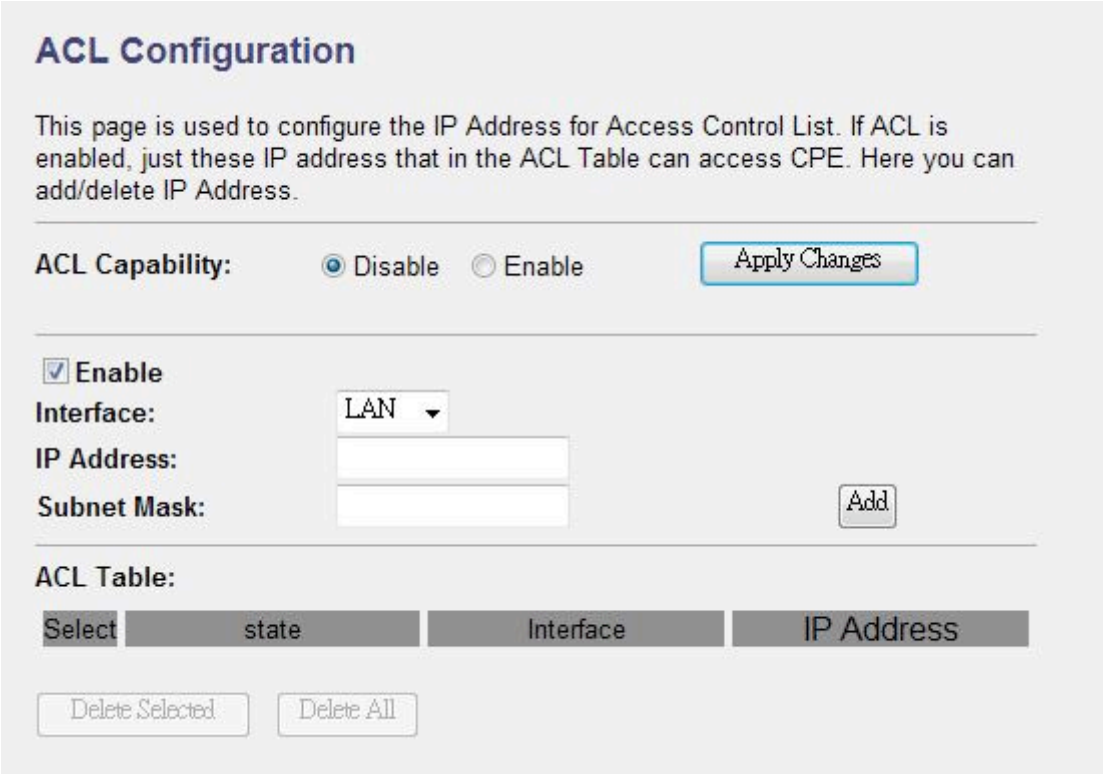
When you finish, click "Apply Changes." You'll see the following message displayed on Web browser.

Click "Continue" to save the settings made and go back to the Web management interface; click "Apply" to save the settings made and restart the router so the settings will take effect after it reboots.

Ex.1017
CISCO SYSTEMS, INC. / Page 79 of 100

5.2.7.6 ACL Configuration

The Access Control List (ACL) is a list of permissions attached to the router that specifies who is allowed to access this router. If ACL is enabled, all hosts cannot access this router except for the hosts with an IP address in the ACL table.



Parameter	Description
ACL Capability	Enable or disable the ACL function.
Enable	Check to enable this ACL entry.
Interface	Select the interface domain: LAN or WAN.
IP Address	Enter the IP address that is allowed to access the router.
Subnet Mask	Enter the subnet mask that is allowed to access the router.
ACL Table	The ACL settings will be listed here. Click “Delete Selected” to delete the settings you have selected. To remove all settings from the table, click “Delete All.”

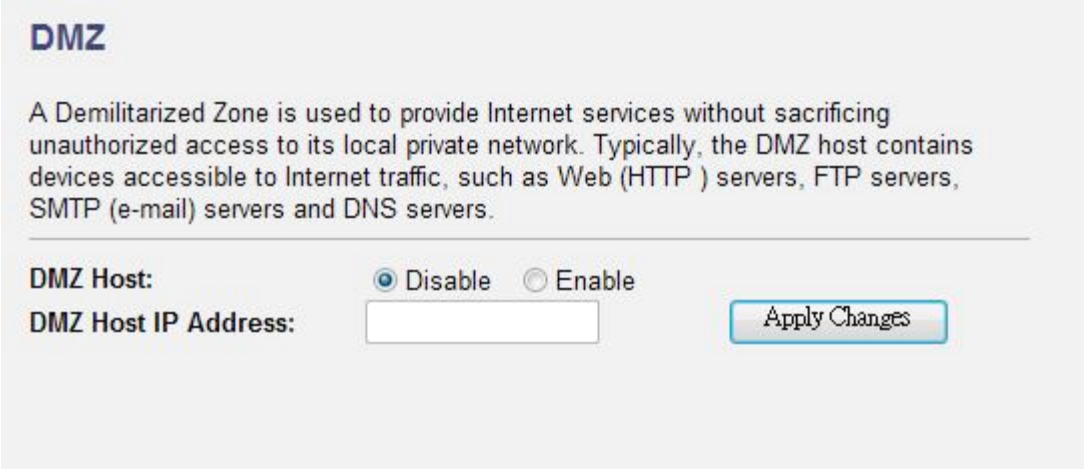
When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.2.7.7 DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the firewall and NAT algorithms, then passed to the DMZ Host.

For example, if you have a local client PC that cannot run an Internet application (e.g., games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host.



Parameter	Description
DMZ Host	Check the item to enable the DMZ function.
DMZ Host IP Address	Enter a static IP address to the DMZ host. This IP address will be exposed to the Internet.

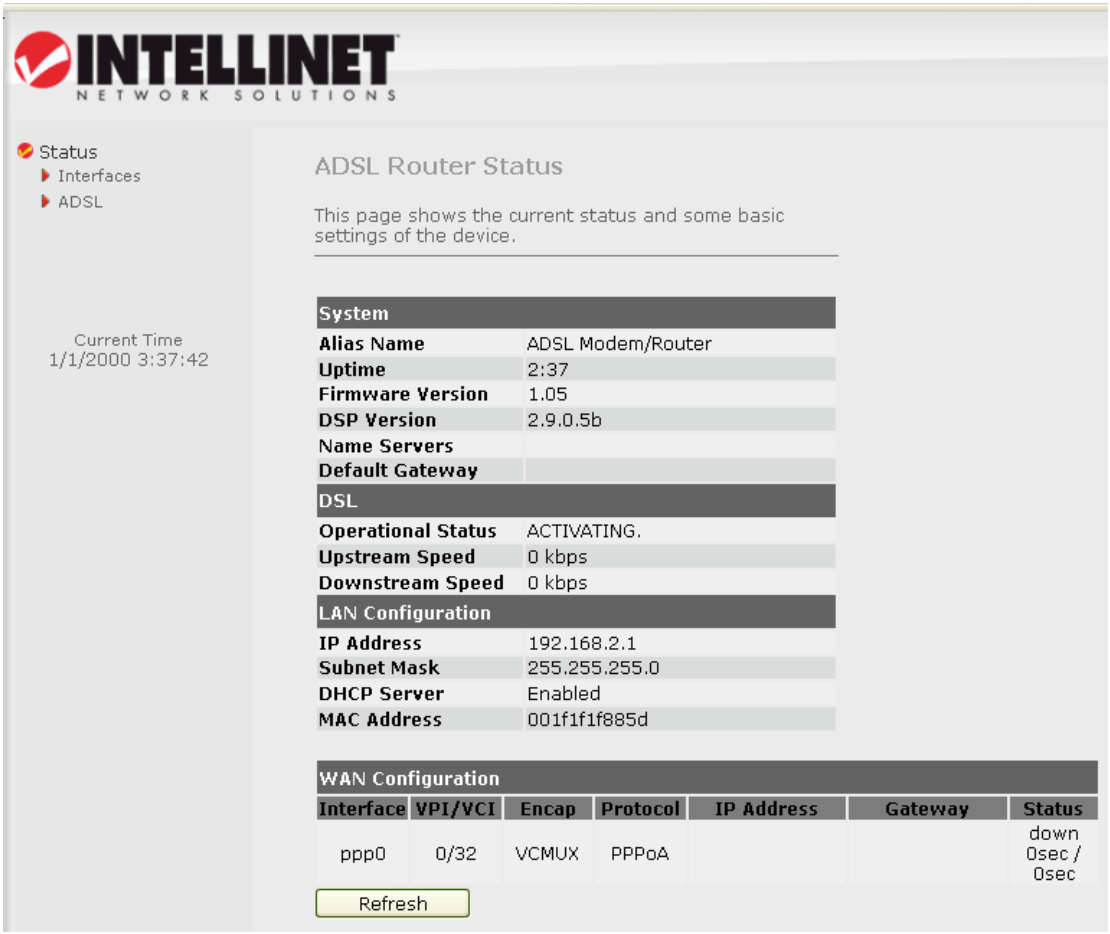
When you finish, click “Apply Changes.” You’ll see the following message displayed on Web browser.

Ex.1017
CISCO SYSTEMS, INC. / Page 81 of 100

Click “Continue” to save the settings made and go back to the Web management interface; click “Apply” to save the settings made and restart the router so the settings will take effect after it reboots.

5.3 Status

This screen displays the ADSL modem/router’s current status and settings. This information is read-only except for the PPPoE/PPPoA channel, for which you can connect/disconnect the channel on demand. Click “Refresh” to update the status function buttons on this screen.



5.3.1 Interface

You can view statistics on the processing of IP packets on the networking interfaces. You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems. To display statistics for any new data, click “Refresh.”

Statistics -- Interfaces

This page shows the packet statistics for transmission and reception regarding to network interface.

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
eth0	1302	0	0	1079	0	0
wlan0	13351	0	0	2131	0	0
0_33	0	0	0	0	0	0

Refresh Reset Statistics

Ex.1017
CISCO SYSTEMS, INC. / Page 83 of 100

5.3.2 ADSL

This screen shows the ADSL line statistic information.

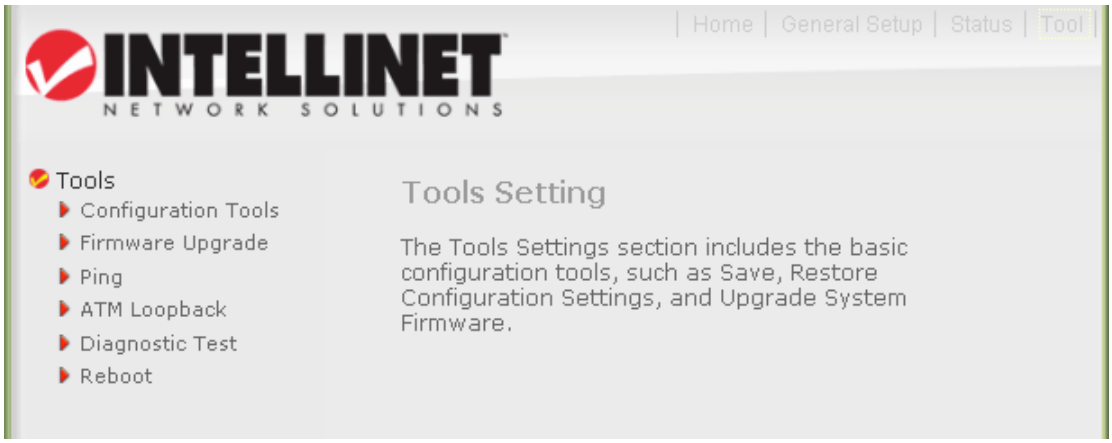
Statistics -- ADSL Line

Mode	
Latency	
Trellis Coding	Enable
Status	ACTIVATING.
Power Level	L0
Uptime	

	Downstream	Upstream
SNR Margin (dB)	0.0	0.0
Attenuation (dB)	0.0	0.0
Output Power (dBm)	0.0	0.0
Attainable Rate (Kbps)	0	0
Rate (Kbps)	0	0
K (number of bytes in DMT frame)		
R (number of check bytes in RS code word)		
S (RS code word size in DMT frame)		
D (interleaver depth)		
Delay (msec)		
FEC	0	0
CRC	0	0
Total ES	0	0
Total SES	0	0
Total UAS	0	0

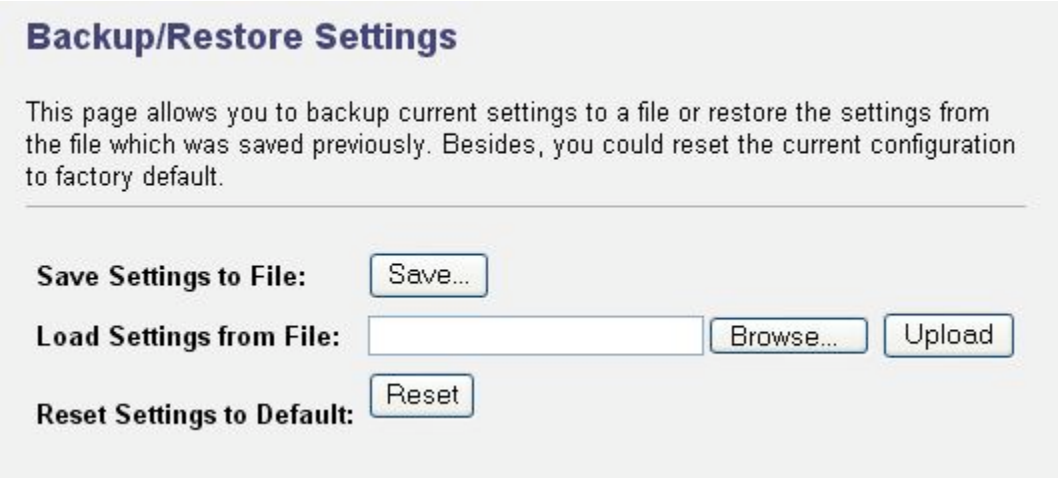
5.4 Tools

The Tools section includes the basic configuration tools, such as Back Up, Restore Configuration Settings, Upgrade System Firmware and Diagnostic Test.



5.4.1 Configuration Tools

This screen allows you to back up the current settings to a file or restore the settings from the file that was saved previously. You can also reset the current configuration to factory defaults.



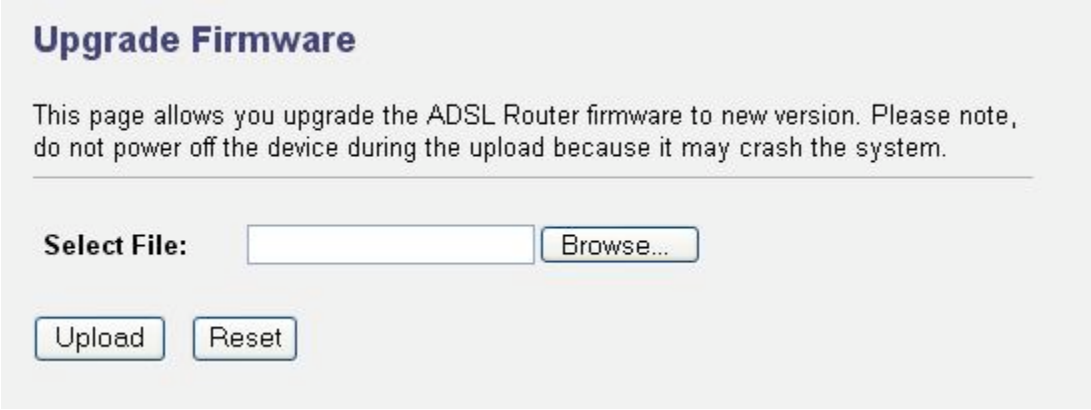
Parameter	Description
Save Settings to File	Click “Save” to save the router’s current configuration to a file named “config.bin” on your PC.

Load Settings from File	Click “Browse” to search for a file you saved before, and click “Upload” to restore the saved configuration.
Restore Settings to Default	Click “Reset” to force the router to perform a power reset and restore the original factory settings.

5.4.2 Firmware Upgrade

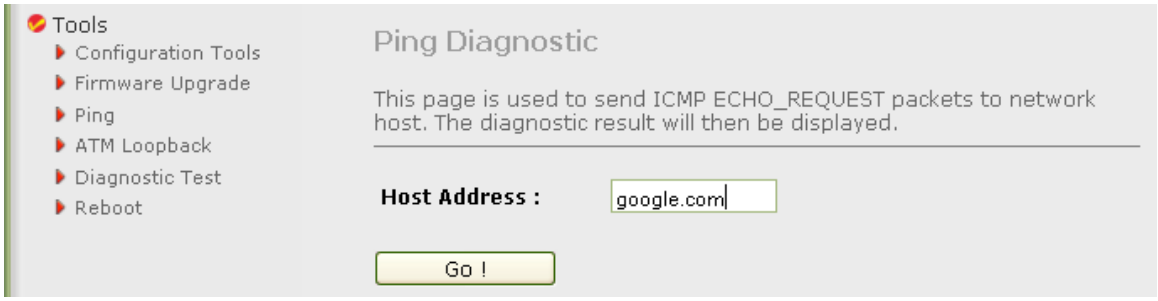
This screen allows you to upgrade the firmware for the router. Click “Browse” to select the firmware file and click “Upload” to start upgrading.

IMPORTANT! Do not turn off your router while this procedure is in progress.



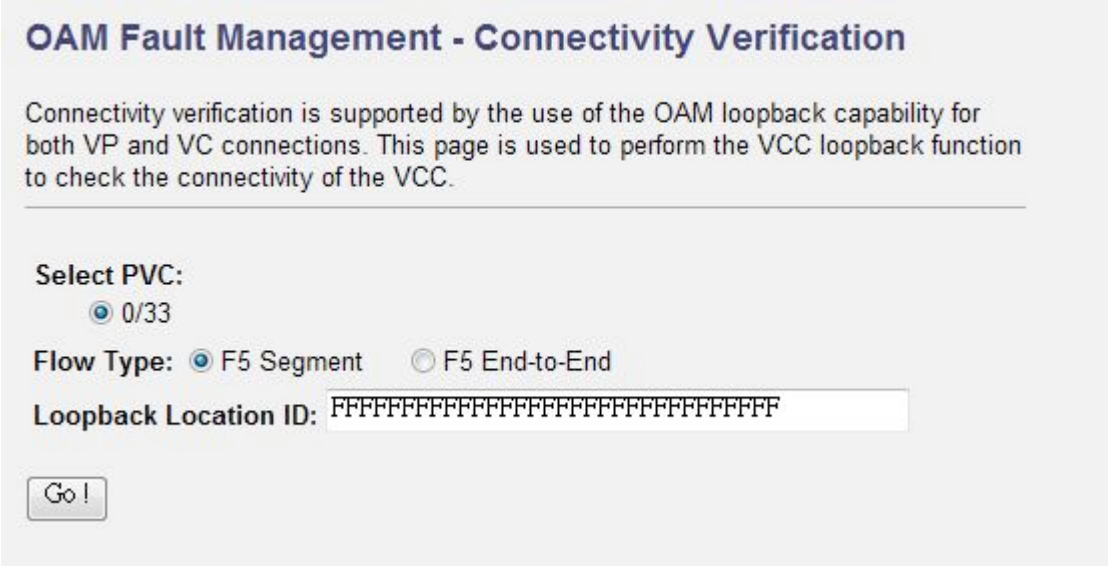
5.4.3 Ping

Once you have your router configured, you can send a ping command to the host you specify on this screen. To use it, you must enter the IP address of the host you are trying to communicate with in the “Host Address” field.



5.4.4 ATM Loopback

In order to isolate ATM interface problems, you can use ATM OAM loopback cells to verify connectivity between VP/VC endpoints, as well as segment endpoints within the VP/VC. This screen allows you to use ATM ping to test the reachability of a segment endpoint or a connection endpoint.



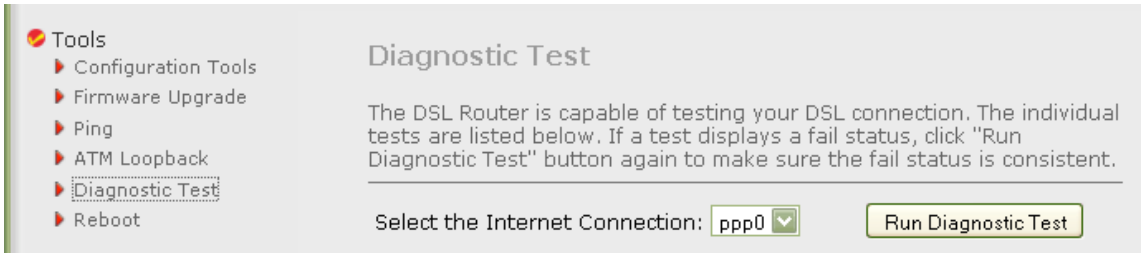
Parameter	Description
Select PVC	Select the PVC channel you want to do the loop-back diagnostic.
Flow Type	The ATM OAM flow type. The selection can be F5 Segment or F5 End-to-End. ATM uses F4 and F5 cell flows: • F4: used in VPs • F5: used in VCs
Loopback Location ID	The loop-back location ID field of the loop-back cell. The default value is all 1s (ones) to indicate the endpoint of the segment or connection.

Click “Go!” to save the setting to the configuration.

Ex.1017
CISCO SYSTEMS, INC. / Page 87 of 100

5.4.5 Diagnostic Test

The Diagnostic Test screen shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.



5.4.6 Reboot

Whenever you use the Web configuration to change system settings, the changes are initially placed in temporary storage. To save your changes for future use, you need to click “Commit and Reboot” to reboot the router. If you have encountered some problems during the configurations, press the “Reset” button on the rear panel of the router and hold it in for 10 seconds or more to reset default settings.

6 Troubleshooting

The LAN LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the Ethernet cable connections between your router and the computer or hub.
2	Check for faulty Ethernet cables.
3	Make sure your computer's Ethernet card is working properly.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

The ADSL LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the telephone wire and connections between router DSL port and the wall jack.
2	Make sure that the telephone company has checked your phone line and set it up for DSL service.
3	Reset your ADSL line to reinitialize your link to the DSLAM.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

I cannot access the Web management.

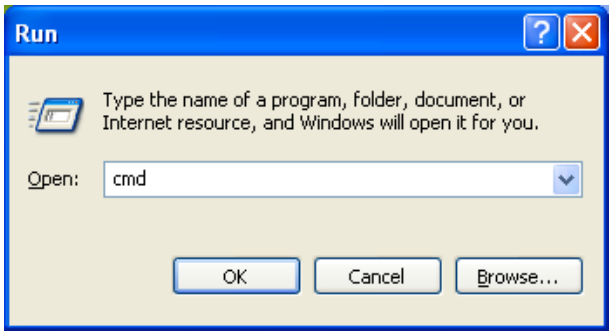
STEPS	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of router.
2	Your computer and the router's IP addresses must be on the same subnet for LAN access.
3	If you have changed router's LAN IP address, then enter the new one as the URL.

Ex.1017
CISCO SYSTEMS, INC. / Page 89 of 100

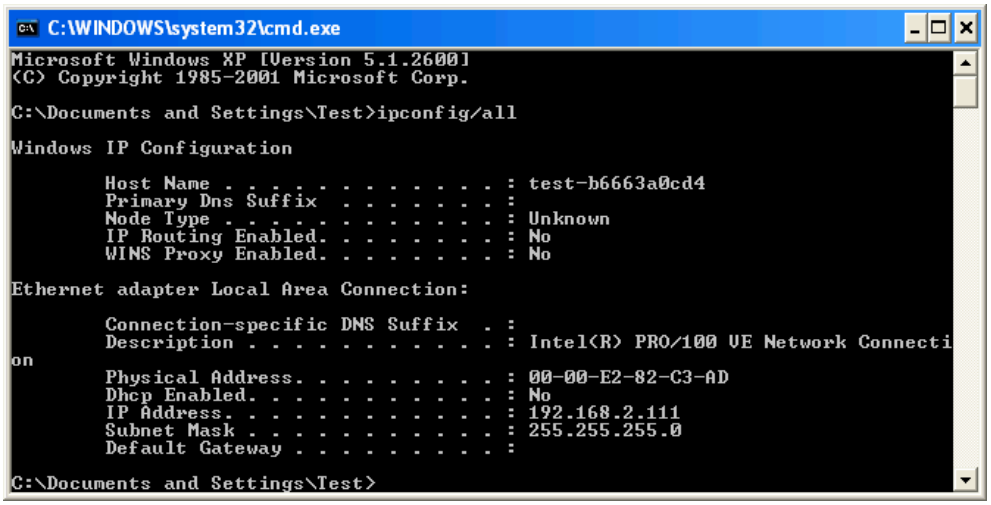
The following procedures will help you to check the current IP address setting of your computer. You can compare if your computer and the router's IP addresses are in the same subnet.

Step 1: Click "Start" and select "Run."

Step 2: Enter "cmd" in the "Open" text field and click "OK."



Step 3: Input "ipconfig/al"l and press <Enter> on your keyboard.



Your PC's IP address is 192.168.2.111.

The PC's subnet mask is 255.255.255.0.

Your PC's MAC address is the one listed as Physical Address (00-00-E2-82-C3-AD).

I forget my login username and/or password.

STEPS	CORRECTIVE ACTION
1	If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This will erase all custom configurations and restore all of the factory defaults, including the password.
2	Press and hold in the Reset/WPS button for over five seconds, then release it. When the Power LED begins to blink, the defaults have been restored.
3	The default username is “admin.” The default password is “1234.” The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper case.
4	It is highly recommended that you change the default username and password. Make sure you store the username and password in a safe place.

I cannot access the Web Management of the router after activating the ACL function.

STEPS	CORRECTIVE ACTION
1	When ACL is activated, you need to set the ACL rule for allowing some users to use some services. Check if you have set the rules. If not, all the users are forbidden to use any of service from the LAN or WAN.
2	If you cannot access the Web management of the router, press and hold in the Reset/WPS button over 5 seconds to restore to defaults.
3	After the router has restarted, log in to the router with the default IP address 192.168.2.1.

Ex.1017
CISCO SYSTEMS, INC. / Page 91 of 100

Initialization of the ADSL connection failed.

STEPS	CORRECTIVE ACTION
1	Check the cable connections between the ADSL port and the wall jack. The ADSL LED on the rear panel of the router should be on.
2	Check that the VPI, VCI, Type of Encapsulation and Type of Multiplexing settings are the same as what you collected from your ISP.
3	Restart the router. If you still have problems, you may need to verify your VPI, VCI, Type of Encapsulation and Type of Multiplexing settings with the ISP.

I cannot get a WAN IP address from the ISP.

STEPS	CORRECTIVE ACTION
1	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name.
2	The username and password apply to PPPoE and PPoA encapsulation only. Make sure that you have entered the correct Service Type, User Name and Password (be sure to use the correct case).

Internet connection disconnects.

STEPS	CORRECTIVE ACTION
1	Check the connection type.
2	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting.
3	Contact your ISP.

Ex.1017
CISCO SYSTEMS, INC. / Page 92 of 100

7 Glossary

10Base-T

It is an Ethernet standard for a local area network (LAN). 10Base-T uses a twisted pair cable with a maximum length of 100 meters.

AAL

ATM is an adaptation layer that defines the rules governing segmentation and reassembly of data into cells. Different AAL types are suited to different traffic classes.

ADSL

An asymmetric digital subscriber line is an asymmetrical data transmission technology with a high traffic rate downstream and a low traffic rate upstream. ADSL technology satisfies the bandwidth requirement of applications that demand “asymmetric” traffic, such as Web surfing, file downloads and video-on-demand (VOD).

ATM

Asynchronous transfer mode is a Layer 2 protocol supporting high-speed asynchronous data with advanced traffic management and quality-of-service features.

Bridge

A device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets; that is, to forward only certain traffic. Related devices are repeaters, which simply forward electrical signals from one cable to another, and full-fledged routers, which make routing decisions based on several criteria.

Default Gateway (Router)

Every non-router IP device needs to configure a default gateway’s IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out toward the destination.

DHCP

The Dynamic Host Configuration Protocol automatically gives every computer on your home network an IP address.

Ex.1017
CISCO SYSTEMS, INC. / Page 93 of 100

DNS Server IP Address

DNS stands for domain name system, which allows Internet servers to have a domain name (such as www.ADSLrouter.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing " ADSLrouter.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL

Digital line subscriber (DSL) technology provides high-speed access over twisted copper pair for connection to the Internet, LAN interfaces and DSL services such as video-on-demand, distance learning and video conferencing.

Ethernet

The standard for computer networks, Ethernet networks are connected by special cables and hubs or switches, and move data around at up to 10/100 million bits per second (Mbps).

FTP

The File Transfer Protocol is the Internet protocol (and program) used to transfer files between hosts.

Idle Timeout

Idle timeout is designed so that when there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

ISP

An Internet service provider is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

ISP Gateway Address

This is an IP address for the Internet router located at the ISP's office.

LAN

A local area network is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

Ex.1017
CISCO SYSTEMS, INC. / Page 94 of 100

MAC Address

MAC stands for media access control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is composed of two parts: 3 bytes of data that corresponds to the manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

NAT

A network address translator is defined by RFC 1631. It enables a LAN network to use one set of IP addresses for internal traffic. A NAT box located where the LAN meets the Internet provides the necessary IP address translation. This helps provide a sort of firewall and allows for a wider address range to be used internally without danger of conflict. Using the router's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port

Network clients (LAN PC) uses port numbers to distinguish one network application/protocol from another. Below is a list of common applications and protocol/port numbers.

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

Ex.1017
CISCO SYSTEMS, INC. / Page 95 of 100

PPP

PPP is the Point-to-Point-Protocol. The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

PPPoA (RFC 2364)

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. This document describes the use of ATM Adaptation Layer 5 (AAL5) for framing PPP encapsulated packets.

PPPoE (RFC 2516)

This document describes how to build PPP sessions and encapsulate PPP packets over Ethernet. PPP over Ethernet (PPPoE) provides the ability to connect a network of hosts over a simple bridging access device to a remote Access Concentrator.

Protocol

A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

PVC

A permanent virtual circuit is a connection-oriented, permanent leased-line circuit between end stations on a network over a separate ATM circuit.

RFC

Request for Comments is the document series, begun in 1969, that describes the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs.

RFC 1483

This is a multi-protocol encapsulation over AAL-5: two encapsulation methods for carrying network interconnect traffic over ATM AAL-5. The first method allows multiplexing of multiple protocols over a single ATM virtual circuit. The protocol of a carried PDU is identified by prefixing the PDU by an IEEE 802.2 Logical Link Control (LLC) header. The second method does higher-layer protocol multiplexing implicitly by ATM Virtual Circuits (VCs).

Router

A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms in order to choose the best route based on several criteria known as “routing metrics.”

Subnet Mask

A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g., 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP

Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocols. TCP performs proper error detection and error recovery, and thus is reliable. UDP, on the other hand, is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

VCI

A virtual circuit identifier is part of the ATM cell header. A VCI is a tag indicating the channel over which a cell will travel. The VCI of a cell can be changed as it moves between switches via signaling.

VPI

A virtual path identifier is part of the ATM cell header. A VPI is a conduit for a number of virtual circuits.

WAN

A wide area network is a network that connects computers located in geographically separate areas (e.g., different buildings, cities, countries). The Internet is a wide area network.

Web-based Management Graphical User Interface (GUI)

Many devices support a graphical user interface that is based on the Web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to control/configure or monitor the device being managed.

8 Specifications

Standards

• IEEE 802.3 (10Base-T Ethernet)
• IEEE 802.3u (100Base-TX Fast Ethernet)
• IEEE 802.11b (11 Mbps Wireless LAN)
• IEEE 802.11g (54 Mbps Wireless LAN)
• IEEE 802.11n Draft 2.0 (300 Mbps Wireless LAN)
• ADSL2+ (ITU G.992.5) up to 24 Mbps
• ADSL2 (ITU G.992.4) splitterless ADSL, up to 12 Mbps
• ADSL2 (ITU G.992.3) up to 12 Mbps
• ADSL (ITU G.992.2/G.Lite) up to 1.5 Mbps
• ADSL (ITU G.992.1/G.DMT) up to 8 Mbps
• ANSI T1.413, Issue 2 (Asymmetric DSL)

General

• LAN ports: 4 RJ45 10/100 Mbps data ports
• LAN ports with Auto MDI/MDI-X
• WAN port: 1 x RJ11 (ADSL)
• Flash: 2 MB
• Memory: 16 MB SDRAM
• Throughput max.: 24 Mbps downstream, 1 Mbps upstream
• Certifications: FCC Class B, CE, RoHS

Router

• Chipset: Realtek RTL8671BH + RTL8271B
• Supported WAN connection types:
  - PPP over Ethernet (RFC 2516)
  - PPP over AAL5 (RFC 2364)
  - Multiple protocols over AAL5 (RFC 1483/2684)
• NAT:
  - Port forwarding
  - DMZ (demilitarized zone)
• Firewall:
  - Access control based on MAC address

Ex.1017
CISCO SYSTEMS, INC. / Page 98 of 100

- URL filter
• Supports UPnP (Universal Plug and Play)
• Supports DHCP (client/server)
• Supports VPN PPTP, L2TP and IPsec passthrough

Wireless

• Chipset: Realtek RTL8192SU
• Wireless frequency range: 2.4 – 2.4835 GHz
• Modulation technologies:
- 802.11b: Direct Sequence Spread Spectrum (DSSS): DBPSK, DQPSK, CCK
- 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
- 802.11n: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
• Channels:
- USA & Canada: 11 channels
- Europe: 13 channels
- Japan: 14 channels
• Data rates:
- IEEE 802.11b (11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps)
- IEEE 802.11g (54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, 6 Mbps)
• Output power:
- OFDM: 15 dBm +/- 1.5 dBm (54 Mbps, 32 mW max.)
- OFDM: 13 dBm +/- 1.5 dBm (300 Mbps, 20 mW max.)
- CCK: 16 dBm +/- 1.5 dBm (11 Mbps, 40 mW max.)
• Wireless security:
- WEP encryption (64/128 bit)
- WPA TKIP
- WPA2 AES
- WPA2 mixed
- WPA RADIUS
- Client access control through media access control (MAC) filter
• Antennas:
- 2 fixed dipole antennas with 3 dBi gain each

- 2T2R MIMO mode (2 transmitter, 2 receiver)

LEDs

• Power
• WLAN
• WPS
• ADSL Link/Act
• LAN 1-4 Link/Act

Environmental

• Dimensions: 187 (W) x 100 (D) x 30 (H) mm (7.3 x 3.9 x 1.2 in.)
• Weight: 0.8 kg (1.7 lbs.)
• Operating temperature: 0 – 40°C (32 – 104°F)
• Operating humidity: 10 – 90% RH, non-condensing
• Storage temperature: 0 – 60°C (0 – 149°F)

Power

• External power adapter: 12 V DC, 1 A

Package Contents

• Wireless 300N ADSL 2+ Modem Router
• Quick installation guide
• Setup CD with user manual and setup wizard
• Power adapter
• Ethernet Cat5 RJ45 cable, 1.0 m (3 ft.)
• RJ11 telephone cable, 1.8 m (5.9 ft.)