

MC-4220

802.11n WLAN ADSL2+ Router

user's manual



MODECOM

Contest

Introduction	5
Device Requirements	5
Using this Document	6
Special messages	6
Getting to know the device	6
Parts Check	6
Front Panel	7
Rear Panel	9
Connecting your device	10
Configuring Ethernet PCs	11
Connecting the Hardware	11
Easy Setup	12
WAN Configuration:	12
Getting Started with the Web pages	17
Accessing the Web pages	17
Testing your Setup	19
Default device settings	19
Overview	20
Internet access settings	21
About Wireless ADSL2+ Router	22
Wireless Network	22
Basic Settings	22
Advanced Settings	24
Security	26
Access Control	31
Allow Listed	32
WPS	34
Operations of AP - AP being an enrollee	37
Operations of AP - AP being a registrar	44
Internet Access	49
Types of Internet Access	50
Configuring your PPPoE DSL connection	50
Configuring your PPPoA DSL connection	52
Configuring your Bridged DSL connection	53
Configuring your 1483 MER by DHCP	54
Configuring your 1483 MER by Fixed IP	55
ATM Settings	56
ADSL Settings	57
Local Network Configuration	58
Changing the LAN IP address and subnet mask	58
Adding the Secondary LAN IP address and subnet mask	61

DHCP Settings	63
DHCP Server Configuration	63
DHCP Relay Configuration	65
DHCP None Configuration	67
DNS Configuration	69
DHCP Server Configuration - Attain DNS Automatically	69
DHCP Server Configuration - Set DNS Manually	71
Overview of Dynamic DNS	73
Dynamic DNS Configuration – DynDNS.org	74
IP/Port Filtering	78
IP/Port Filtering	78
MAC Filtering	79
Configuring MAC filtering to Deny for outgoing access	79
Port Forwarding	81
Configuring Port Forwarding	81
Configuring custom applications	82
URL Blocking	89
Configuring URL Blocking of FQDN	89
Configuring URL Blocking of Keyword	91
Domain Blocking	93
Configuring Domain blocking	93
DMZ	95
Configuring DMZ	95
UPnP	97
Configuring UPnP	97
UPnP Control Point Software on Windows ME	99
UPnP Control Point Software on Windows XP with Firewall	99
RIP	101
ARP Table	103
ARP Table	103
Bridging	103
Bridging	103
Routing	104
Routing	104
SNMP	106
SNMP	106
Port Mapping	107
Port Mapping	107
IP QoS	109
IP QoS	109

Remote Access	110
Others	111
Diagnostic	111
Ping	111
ATM Loopback	113
ADSL	114
Diagnostic Test	115
Commit/Reboot	116
Commit/Reboot	116
Backup/Restore	117
Backup settings	117
Restore settings	118
Resetting to Defaults	118
Software Reset:	119
Password	120
Setting your username and password	120
Firmware Update	122
About firmware versions	122
Manually updating firmware	122
ACL Configuration	125
ACL Config	125
Time Zone	127
SNTP Server and SNTP Client Configuration settings	127
TR-069 Config	132
TR-069 Configuration	132
Statistics	133
Interfaces	133
ADSL	134
Configuring your Computers	135
Configuring Ethernet PCs	135
Assigning static Internet information to your PCs	138
IP Addresses, Network Masks, and Subnets	139
IP Addresses	139
Subnet masks	141
Troubleshooting	141
Troubleshooting Suggestions	142
Diagnosing Problem using IP Utilities	143
Glossary	145

Introduction

Congratulations on becoming the owner of the Wireless ADSL2+ Router. You will now be able to access the Internet using your high-speed DSL connection.

This User Guide will show you how to connect your Wireless ADSL2+ Router, and how to customize its configuration to get the most out of your new product.

Features

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

Features include:

- Internal DSL modem for high-speed Internet access
- 10/100Base-T Ethernet Router to provide Internet connectivity to all computers on your LAN
- Network address translation (NAT) functions to provide security for your LAN
- Network configuration through DHCP Server and DHCP Client
- Services including IP route and DNS configuration, RIP, and IP and DSL performance monitoring
- User-friendly configuration program accessed via a web browser
- User-friendly configuration program accessed via EasySetup program

Device Requirements

In order to use the Wireless ADSL2+ Router, you must have the following:

- DSL service up and running on your telephone line
- Instructions from your ISP on what type of Internet access you will be using, and the addresses needed to set up access
- One or more computers each containing an Ethernet card (10Base-T/100Base-T network interface card (NIC))
- For system configuration using the supplied a. web-based program: a web browser such as Internet Explorer v4 or later, or Netscape v4 or later. Note that version 4 of each browser is the minimum version requirement – for optimum display quality, use Internet Explorer v5, or Netscape v6.1 b. EasySetup program: Graphical User Interface



Note

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

Using this Document

Notational conventions

- Acronyms are defined the first time they appear in the text and also in the glossary.
- For brevity, the Wireless ADSL2+ Router is referred to as “the device”.
- The term *LAN* refers to a group of Ethernet-connected computers at one site.

Typographical conventions

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

Special messages

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



Note

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



Definition

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



Warning

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

Getting to know the device

Parts Check

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

1. Wireless ADSL2+ Router
2. CD-ROM containing the online manual and Easy Setup software
3. Power Supply
4. Ethernet Cable
5. Standard Phone Cable
6. Quick Installation Guide

Front Panel

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

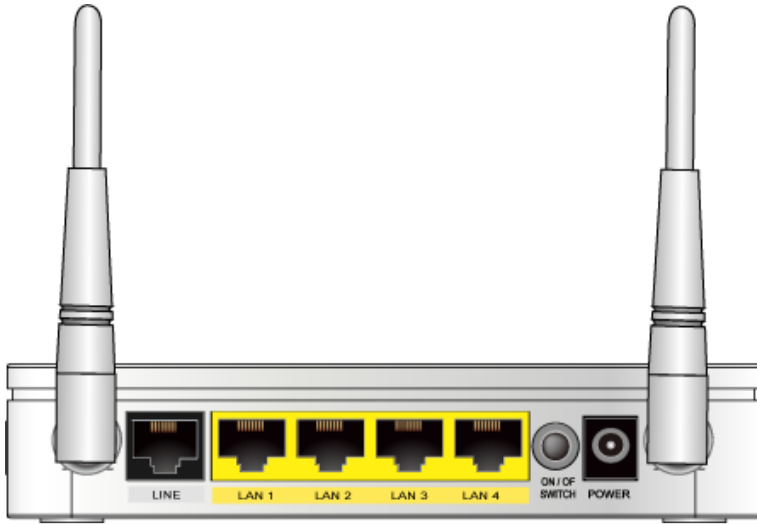


Front Panel and LEDs

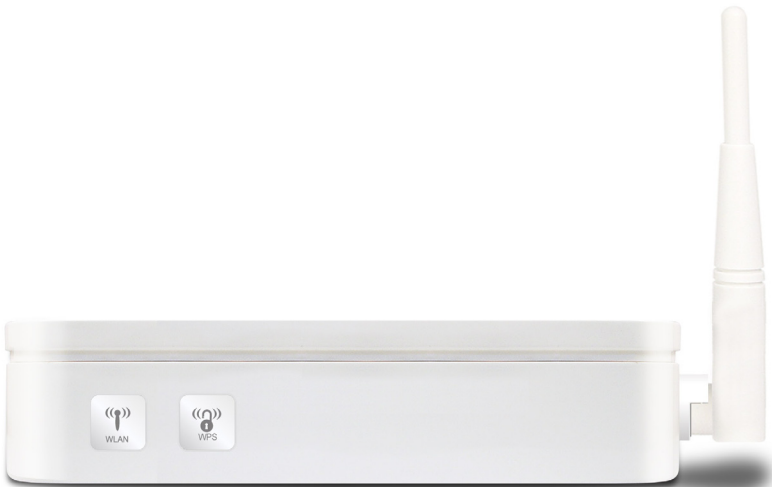
Label	Color	Function
POWER	green	On: device is powered on Off: device is powered off
DSL	green	On: DSL link reaches showtime, which means that your device has successfully connected to your ISP's DSL network. Off: DSL link not in showtime, your device has not successfully connected to your ISP's DSL network. Blink: Data being transmitted
INTERNET	green	On: PPP link established and active, which means that your device has successfully connected to your ISP's network. Off: No PPP link, your device has not successfully connected to your ISP's network. Blink: PPP link established and active
LAN 4/3/2/1	green	On: LAN link established and active Off: No LAN link Blink: Valid Ethernet packet being transferred
WLAN	green	Press this button for 5 seconds to Disable or Enable Wireless LAN.
WPS	green	Press this button for 3 seconds to Enable WPS function.

Rear Panel

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



Rear Panel Connections



Right Panel Connections

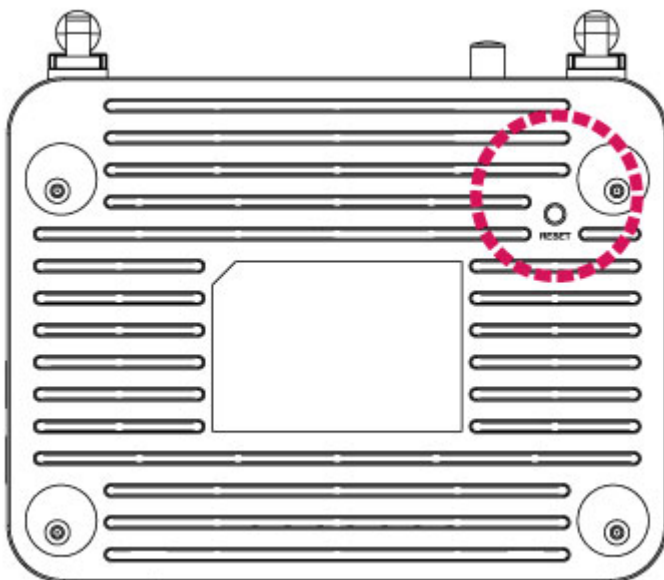


Figure 1: Bottom Side for Reset button

Label	Function
LINE	Connects the device to a telephone port in the wall of your home/office for DSL communication
RESET	Pressing this button restores the factory default configuration on your device
LAN 4/3/2/1	Connects the device via Ethernet to up to four PCs on your LAN
ANETENNA	ANETENNA
POWER	Connects to the supplied power cable
ON/OFF SWITCH	Power on/off the device
WLAN	Press this button for 5 seconds to Disable or Enable Wireless LAN.
WPS	Press this button for 3 seconds to Enable WPS function.

Connecting your device

This chapter provides basic instructions for connecting the Wireless ADSL2+ Router to a computer or LAN and to the Internet.

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

Configuring Ethernet PCs

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

Connecting the Hardware

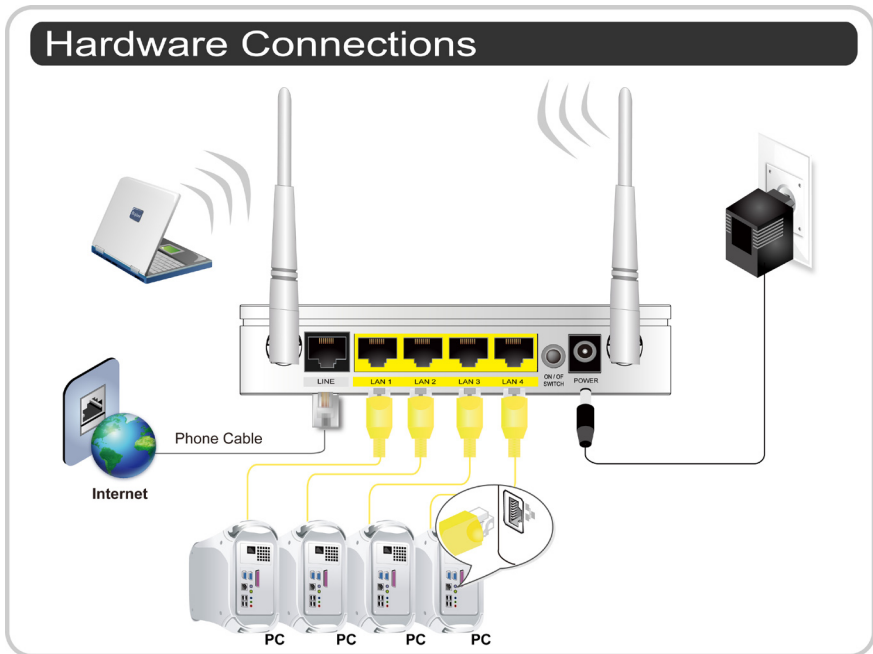
This section describes how to connect the device to the wall phone port, the power outlet and your computer(s) or network.



WARNING

Before you begin, turn the power off for all devices. These include your computer(s), your LAN hub/switch (if applicable), and the Wireless ADSL2+ Router.

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



Overview of Hardware Connections

Step 1. Connect the Telephone cable to ADSL line

Connect one end of the provided phone cable to the port labeled LINE on the rear panel of the device. Connect the other end to your wall phone port.

Step 2. Connect the Ethernet cable

Connect either a LAN hub or Ethernet computers directly to the device via Ethernet cable(s).

Note that the cables do not need to be crossover cables.

Step 3. Attach the power connector

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

Step 4. Power on the device

Press ON/OFF SWITCH to power on the device.

Step 5. Configure your Ethernet PCs

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

Next step

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

Easy Setup

For easy configuration, insert the CD into your CD-ROM drive.

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

WAN Configuration:

There are Four options of Protocol Modes on WAN Configuration: **PPPoA VC-Mux**, **PPPoE LLC**, **1483 Bridged IP LLC** and **1483 MER LLC Mode**.

PPPoE LLC / PPPoA VC-Mux

- After selecting the Protocol : *PPPoE LLC/ PPPoA VC-Mux*:
- Enter *VPI/VC/* which was given by Telecom or by your Internet Service Provider (ISP).
- Enter *Username/Password* which was given by Telecom or by your Internet Service Provider (ISP).
- Click *Setup*.

EASY SETUP 1.0 STANDARD

Wireless @DSL2+ Router

Set Internet Connection

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

The information from your Internet Service Provider. (ISP)

Protocol modes : PPPoE LLC

VPI / VCI : VPI 8 VCI 35

Please enter your ADSL Username and Password.

Username : 1234

Password : 1234

Show characters of Password

Setup Diagnose Exit

Easy setup configuration completed. Now you are ready to Surf the Internet!!!

Wireless @DSL2+ Router

Easy Setup completed.

This page shows the status of your connection

ADSL Status

ADSL Line Status : Pass

Internet Connect Status

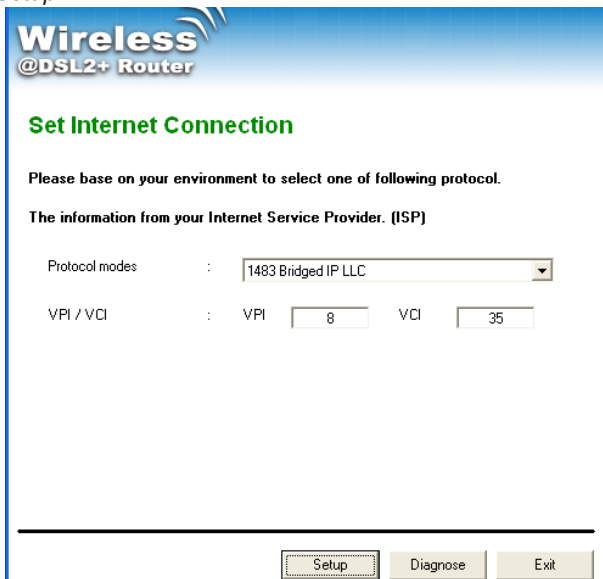
Internet Connection : Pass

The connection to the Internet Service is ready to use.
Clicking on Exit button to end this Easy Setup program.

Exit

1483 Bridged IP LLC

- After selecting the Protocol : 1483 Bridged IP LLC:
- Enter VPI/VCI which was given by Telecom or by your Internet Service Provider (ISP).
- Click *Setup*.



Wireless
@DSL2+ Router

Set Internet Connection

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

The information from your Internet Service Provider. (ISP)

Protocol modes : 1483 Bridged IP LLC

VPI / VCI : VPI 8 VCI 35

Setup Diagnose Exit

Easy setup configuration completed. Now you are ready to Surf the Internet!!!



Wireless
@DSL2+ Router

Easy Setup completed.

This page shows the status of your connection

ADSL Status

ADSL Line Status : Pass

ADSL 2+ Wireless Router setup successfully.
Clicking on Exit button to end this Easy Setup program.

Exit

1483 MER LLC Fixed IP

- After selecting the Protocol : 1483 MER LLC:
- Enter VPI/VCI which was given by Telecom or by your Internet Service Provider (ISP).
- From the Type ratio, click *Fixed IP*.
- Enter *Local IP Address / Subnet Mask / Remote IP Address* which was given by Telecom or by your Internet Service Provider (ISP).
- Click *Setup*.

Wireless @DSL2+ Router

Set Internet Connection

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

The information from your Internet Service Provider. (ISP)

Protocol modes : 1483 MER LLC

VPI / VCI : VPI 8 VCI 35

Type : Fixed IP DHCP

Local IP Address : 192 . 168 . 10 . 150

Subnet Mask : 255 . 255 . 255 . 0

Remote IP Address : 192 . 168 . 10 . 100

Setup Diagnose Exit

Easy setup configuration completed. Now you are ready to Surf the Internet!!!

Wireless @DSL2+ Router

Easy Setup completed.

This page shows the status of your connection

ADSL Status

ADSL Line Status : Pass

Internet Connect Status

Internet Connection : Pass

The connection to the Internet Service is ready to use.
Clicking on Exit button to end this Easy Setup program.

1483 MER LLC DHCP

- After selecting the Protocol : 1483 MER LLC:
- Enter VPI/VCI which was given by Telecom or by your Internet Service Provider (ISP).
- From the *Type* ratio, click *DHCP*.
- Click *Setup*.

Wireless
@DSL2+ Router

Set Internet Connection

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

The information from your Internet Service Provider. (ISP)

Protocol modes : 1483 MER LLC

VPI / VCI : VPI 8 VCI 35

Type : Fixed IP DHCP

Setup Diagnose Exit

Easy setup configuration completed. Now you are ready to Surf the Internet!!!

Wireless
@DSL2+ Router

Easy Setup completed.

This page shows the status of your connection

ADSL Status

ADSL Line Status : Pass

Internet Connect Status

Internet Connection : Pass

The connection to the Internet Service is ready to use.
Clicking on Exit button to end this Easy Setup program.

Exit

Getting Started with the Web pages

The Wireless ADSL2+ Router includes a series of Web pages that provide an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You can access it through your web browser from any PC connected to the device via the LAN ports.

Accessing the Web pages

- To access the Web pages, you need the following:
 - A PC or laptop connected to the LAN port on the device.
 - A web browser installed on the PC. The minimum browser version requirement is Internet Explorer v4 or Netscape v4. For the best display quality, use latest version of Internet Explorer, Netscape or Mozilla Firefox. From any of the LAN computers, launch your web browser, type the following URL in the web address (or location) box, and press [Enter] on your keyboard: **http://10.0.0.2**
- The Status homepage for the web pages is displayed:

Status

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

System						
Alias Name	MODECOM MC-4220 ADSL Router					
Uptime	2 min					
Firmware Version	2.0.0					
Customer Version	MC-4220-A0-4X32M_205rc3_STD_01_90724					
DSP Version	2.9.0.4i					
Name Servers						
Default Gateway						
DSL						
Operational Status	T1.413,SHOWTIME.					
Upstream Speed	896 kbps					
Downstream Speed	8064 kbps					
LAN Configuration						
IP Address	10.0.0.2					
Subnet Mask	255.255.255.0					
DHCP Server	Enabled					
MAC Address	00e04c867001					
WAN Configuration						
Interface	VPI/VCI	Encap	Protocol	IP Address	Gateway	Status
ppp0_vc0	8/35	LLC	PPPoE			down 0sec / 0sec <input type="button" value="Connect"/>

Homepage

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

A login screen is displayed:

Login screen

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

User Name: **admin**

Password: **administrator**



Note

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

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

This is the first page displayed each time you log in to the Web pages. This page contains links to the following pages:

- Addressing; links to the *Addressing* page that controls your device's network address. See *Addressing*.
- Internet Access; links to the *Internet Access* page that controls how your device connects to the Internet. See *Internet Access*.



Note

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

Testing your Setup

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

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

Table 1. LED Indicators

LED	Behavior
POWER	Solid green to indicate that the device is turned on. If this light is not on, check the power cable attachment.
ETH	Flashing on/off while the device is booting. After about 10-15 seconds, solid green to indicate that the device can communicate with your LAN.
Link	Flashing on/off while data is being transmitted. Solid green to indicate that the device has successfully established a connection with your ISP.
INTERNET	Flashing on/off while data is being transferred. Solid green when a valid IP address has been assigned to the device by the ISP.

If the LEDs illuminate as expected, test your Internet connection from a LAN computer. To do this, open your web browser, and type the URL of any external website. The LED labeled *INTERNET* should blink rapidly and then appear solid as the device connects to the site.

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

Default device settings

In addition to handling the DSL connection to your ISP, the DSL Modem can provide a variety of services to your network. The device is preconfigured with default settings for use with a typical home or small office network.

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



WARNING

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

Option	Default Setting	Explanation/Instructions
<i>LINE Port IP Address</i>	Unnumbered interface: 10.0.0.2 Subnet mask: 255.255.255.255	This is the temporary public IP address of the WAN port on the device. It is an unnumbered interface that is replaced as soon as your ISP assigns a 'real' IP address. See <i>Internet Access</i> .
<i>LAN Port IP Address</i>	Assigned static IP address: 10.0.0.2 Subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See <i>LAN</i> .
<i>DHCP (Dynamic Host Configuration Protocol)</i>	DHCP server enabled with the following pool of addresses: 10.0.0.33 through 10.0.0.254	The Wireless ADSL2+ Router maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in <i>Services -> DHCP Settings</i> .
<i>NAT (Network Address Translation)</i>	NAT enabled	Your computers' private IP addresses (see DHCP above) will be translated to your public IP address whenever the PCs access the Internet. See <i>Services -> Firewall</i> .

Overview

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

- details of the device's Internet access settings
- version information about your device

To display this page:

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

Status

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

System						
Alias Name	MODECOM MC-4220 ADSL Router					
Uptime	2 min					
Firmware Version	2.0.0					
Customer Version	MC-4220-A0-4X32M_205rc3_STD_01_90724					
DSP Version	2.9.0.4i					
Name Servers						
Default Gateway						
DSL						
Operational Status	T1.413,SHOWTIME.					
Upstream Speed	896 kbps					
Downstream Speed	8064 kbps					
LAN Configuration						
IP Address	10.0.0.2					
Subnet Mask	255.255.255.0					
DHCP Server	Enabled					
MAC Address	00e04c867001					
WAN Configuration						
Interface	VPI/VCI	Encap	Protocol	IP Address	Gateway	Status
ppp0_vc0	8/35	LLC	PPPoE			down 0sec / 0sec <input type="button" value="Connect"/>

Overview page

The information displayed on this page is explained in detail in the following sections.

Internet access settings

This section displays details of the settings that allow your device to access the Internet. These details include:

IP address and subnet mask:	The IP address and subnet mask assigned to your WAN interface. This address is used temporarily until your ISP assigns a real IP address (via DHCP or PPP – see Internet Access).
Default gateway:	The address of the ISP server through which your Internet connection will be routed.
DNS servers:	The Domain Name System (DNS) servers used by your ISP to map domain names to IP addresses.

Your ISP assigns all of these settings. In most cases, you **will not** need to make changes to these settings in order for your Internet connection to work. If your ISP does ask you to change any of these settings, follow the instructions for manually configuring your device in *Internet Access*.

About Wireless ADSL2+ Router

This section displays details of your device's hardware and firmware versions. If you need to contact your ISP's support team, they may need to know which hardware/firmware versions you are using in order to answer your query.

Your hardware version details contain information about the make and model of your device and its exact hardware components.

Your firmware version details contain information about the software program running on your device. From time to time, MODECOM may update or add new features to this firmware. They then make the latest updated version available to you via the Internet. For details of how to update your firmware, see *Admin -> Upgrade Firmware*.

Wireless Network

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

Basic Settings

This page contains all of the wireless basic settings. Most users will be able to configure the wireless portion and get it working properly using the setting on this screen.

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

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

Wireless Basic Settings

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

Disable Wireless LAN Interface

Band:

Mode:

SSID:

Channel Width:

Control Sideband:

Channel Number:

Radio Power (mW):

Associated Clients:

Wireless Network page

Field	Description
Disable Wireless LAN Interface	Enable/Disable the Wireless LAN Interface.
Band	Select the appropriate band from the list provided to correspond with your network setting.
Mode	Configure the Wireless LAN Interface to AP or AP + WDS mode
SSID	Specify the network name. Each Wireless LAN network uses a unique Network Name to identify the network. This name is called the Service Set Identifier (SSID). When you set up your wireless adapter, you specify the SSID. If you want to connect to an existing network, you must use the name for that network. If you are setting up your own network you can make up your own name and use it on each computer. The name can be up to 32 characters long and contain letters and numbers.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. You shall assign a different channel for each AP to avoid signal interference.
Radio Power (mW)	The maximum output power: 15mW, 30mW or 60mW.

Function Button	Description
Associated Clients	Show Active Wireless Client Table This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.
Apply Changes	Click to save the rule entry to the configuration.
Reset	Discard your changes and reload all settings from flash memory.

Advanced Settings

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

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

Wireless Advanced Settings

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

- Authentication Type:** Open System Shared Key Auto
- Fragment Threshold:** (256-2346)
- RTS Threshold:** (0-2347)
- Beacon Interval:** (20-1024 ms)
- Data Rate:**
- Preamble Type:** Long Preamble Short Preamble
- Broadcast SSID:** Enabled Disabled
- Relay Blocking:** Enabled Disabled
- Protection:** Enabled Disabled
- Aggregation:** Enabled Disabled
- Short GI:** Enabled Disabled

Field	Description
Authentication Type	<p>Open System: Open System authentication is not required to be successful while a client may decline to authenticate with any particular other client.</p> <p>Shared Key: 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. Requiring the use of the WEP privacy mechanism.</p> <p>Auto: Auto is the default authentication algorithm. It will change its authentication type automatically to fulfill client's requirement.</p>
Fragment Threshold	<p>When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium.</p> <p>The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages.</p> <p>This value should remain at its default setting of 2346. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the "Fragment Threshold" value within the value range of 256 to 2346. Setting this value too low may result in poor network performance. Only minor modifications of this value are recommended.</p>
RTS Threshold	<p>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 ADSL modem (or AP) 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.</p>
Beacon Interval	<p>The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1024. A beacon is a packet broadcast by the ADSL modem (or AP) to synchronize the wireless network. The default is 100.</p>
Data Rate	<p>The rate of data transmission should be set depending on the speed of your wireless network. You should select from a range of transmission speeds, or you can select Auto to have the ADSL modem (or AP) automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the AP and a wireless client. The default setting is Auto.</p>
Function Button	Description
Apply Changes	Click to save the rule entry to the configuration.

Security

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

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

Wireless Security Setup

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

Encryption:

Use 802.1x Authentication
 WEP 64bits WEP 128bits

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

Pre-Shared Key Format:

Pre-Shared Key:

Authentication RADIUS Server:

Port IP address Password

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

Field	Description
Encryption	<p>There are 4 types of security to be selected. To secure your WLAN, it's strongly recommended to enable this feature.</p> <p>WEP: Make sure that all wireless devices on your network are using the same encryption level and key. Click Set WEP Key button to set the encryption key.</p> <p>WPA (TKIP): WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP utilized a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.</p> <p>WPA2 (AES): WPA2, also known as 802.11i, uses Advanced Encryption Standard (AES) for data encryption. AES utilized a symmetric 128-bit block data encryption.</p> <p>WAP2 Mixed: The AP supports WPA (TKIP) and WPA2 (AES) for data encryption. The actual selection of the encryption methods will depend on the clients.</p>

Set WEP Key	Configure the WEP Key
Use 802.1x Authentication	Check it to enable 802.1x authentication. This option is selectable only when the “Encryption” is choose to either None or WEP. If the “Encryption” is WEP, you need to further select the WEP key length to be either WEP 64bits or WEP 128bits.
WPA Authentication Mode	There are 2 types of authentication mode for WPA. WPA-RADIUS: WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. Please refer to “Authentication RADIUS Server” setting below for RADIUS setting. The WPA algorithm is selected between TKIP and AES, please refer to “WPA cipher Suite” below. Pre-Shared Key: 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 key format and enter a password in the “Pre-Shared Key Format” and “Pre-Shared Key” setting respectively. Please refer to “Pre-Shared Key Format” and “Pre-Shared Key” setting below.
Pre-Shared Key Format	PassPhrase: Select this to enter the Pre-Shared Key secret as user-friendly textual secret. Hex (64 characters): Select this to enter the Pre-Shared Key secret as hexadecimal secret.
Pre-Shared Key	Specify the shared secret used by this Pre-Shared Key. If the “Pre-Shared Key Format” is specified as PassPhrase, then it indicates a passphrase of 8 to 63 bytes long; or if the “Pre-Shared Key Format” is specified as PassPhrase, then it indicates a 64-hexadecimal number.
Authentication RADIUS Server	If the WPA-RADIUS is selected at “WPA Authentication Mode”, the port (default is 1812), IP address and password of external RADIUS server are specified here.
Function Button	Description
Apply Changes	Click to save the rule entry to the configuration.

WEP + Encryption Key

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

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

Encryption: 

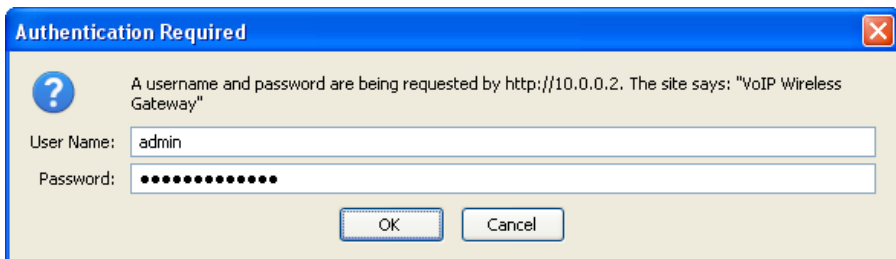
- Click *Set WEP Key* button.

Set WEP Key

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

User Name: **admin**

Password: **administrator**



- From the *Key Length* drop-down list, select *64-bit* or *128-bit* setting.
- From the *Key Format* drop-down list, select *ASCII (5 characters)*, *Hex (10 characters)*, *ASCII (13 characters)* or *Hex (26 characters)* setting.
- From the *Default Tx Key* drop-down list, select a *key is used for encryption*.
- Enter the *Encryption Key* value depending on selected ASCII or Hexadecimal.
- Click *Apply Changes* button.

Wireless WEP Key Setup

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

SSID TYPE: Root VAP0 VAP1 VAP2 VAP3

Key Length: 64-bit ▼

Key Format: ASCII (5 characters) ▼

Default Tx Key: Key 1 ▼

Encryption Key 1: *****

Encryption Key 2: *****

Encryption Key 3: *****

Encryption Key 4: *****

Apply Changes Close Reset

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

Change setting successfully!

OK

WEP + Use 802.1x Authentication

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

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

Encryption: ▼

- Check the option of *Use 802.1x Authentication*.
- Click on the ratio of *WEP 64bits* or *WEP 128bits*.

Use 802.1x Authentication WEP 64bits WEP 128bits

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

Authentication RADIUS Server: Port IP address
 Password

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

Change setting successfully!

OK

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

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

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

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

Encryption:

WPA(TKIP) ▼

Encryption:

WPA2(AES) ▼

Encryption:

WPA2 Mixed ▼

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

WPA Authentication Mode:

Enterprise (RADIUS) Personal (Pre-Shared Key)

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

Pre-Shared Key Format:

Passphrase ▼

Pre-Shared Key Format:

Hex (64 characters) ▼

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

Pre-Shared Key:

0123456789

5. Click on *Apply Changes* button to confirm and return.

Apply Changes

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

Change setting successfully!

OK

WPA/WPA2/WPA2 Mixed + Enterprise (RADIUS)

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

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

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

Encryption:

WPA(TKIP) ▼

Encryption:

WPA2(AES) ▼

Encryption:

WPA2 Mixed ▼

Click on the radio of *Enterprise (RADIUS)*.

WPA Authentication Mode:

Enterprise (RADIUS) Personal (Pre-Shared Key)

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

Authentication RADIUS Server:

Port

1812

IP address

10.0.0.100

Password

••••

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

Change setting successfully!

OK

Access Control

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

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

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

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

Wireless Access Control

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

Wireless Access Control Mode:

Disable



Apply Changes

MAC Address:

(ex. 00E086710502)

Add

Reset

Current Access Control List:

MAC Address

Select

Delete Selected

Delete All

Allow Listed

1. If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point.
2. From the Wireless Access Control Mode drop-down list, select Allowed Listed setting.
3. Enter the *MAC Address*.
4. Click *Add* button.

Wireless Access Control Mode:

Allow Listed



Apply Changes

MAC Address:

(ex. 00E086710502)

Add

Reset

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

Change setting successfully!

OK

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

Current Access Control List:

MAC Address	Select
00:1d:09:a2:52:f9	<input type="checkbox"/>

Delete Selected

Delete All

Deny Listed

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

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

2. Enter the *MAC Address*.

3. Click *Add* button.

Wireless Access Control Mode:

Deny Listed ▼

Apply Changes

MAC Address: (ex. 00E086710502)

Add

Reset

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

Change setting successfully!

OK

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

Current Access Control List:

MAC Address	Select
00:1d:09:a2:52:f9	<input type="checkbox"/>

Delete Selected

Delete All

WPS

Introduction of WPS

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

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

Supported WPS features

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

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

If those unsupported modes are enforced by users, WPS will be disabled.

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

AP mode

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

AP as Enrollee

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

AP as Registrar

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

AP as Proxy

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

Infrastructure-Client mode

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

Instructions of AP's and Client's operations

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

This device supports Push Button method and PIN method for WPS. The following sub-paragraphs will describe the function of each item. The webpage is as below. To access the *Wireless Network WPS* page:

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

Wi-Fi Protected Setup

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

Disable WPS

WPS Status:

Configured UnConfigured

Self-PIN Number:

12345670

Regenerate PIN

Push Button Configuration:

Start PBC

Apply Changes

Reset

Client PIN Number:

Start PIN

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

Push Button Configuration	“Self-PIN Number” is AP’s PIN. Whenever users want to change AP’s PIN, they could click “Regenerate PIN” and then click “Apply Changes”. Moreover, if users want to make their own PIN, they could enter four-digit PIN without checksum and then click “Apply Changes”. However, this would not be recommended since the registrar side needs to be supported with four-digit PIN.
Push Button Configuration	Clicking this button will invoke the PBC method of WPS. It is only used when AP acts as a registrar.
Client PIN Number	It is only used when users want their station to join AP’s network. The length of PIN is limited to four or eight numeric digits. If users enter eight-digit PIN with checksum error, there will be a warning message popping up. If users insist on this PIN, AP will take it.
Function Button	Description
Regenerate PIN	Click to regenerate the Self-PIN Number.
Start PBC	Click to start the Push Button method of WPS.
Apply Changes	Click to commit changes.
Reset	It restores the original values.
Start PIN	Click to start the PIN method of WPS.

Operations of AP - AP being an enrollee

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

1. From the left-hand *Wireless* -> *WPS* menu. The following page is displayed:
2. Make sure AP is in un-configured state.

Wi-Fi Protected Setup

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

Disable WPS

WPS Status:

Configured UnConfigured

Self-PIN Number:

12345670

Regenerate PIN

Push Button Configuration:

Start PBC

Apply Changes

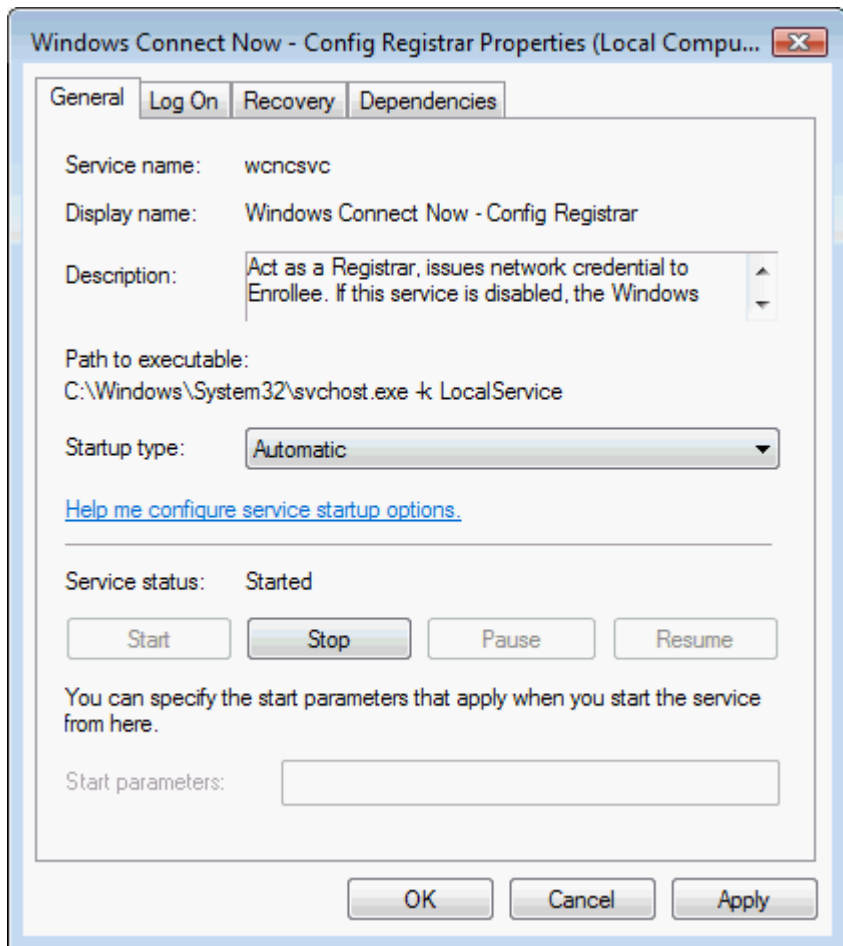
Reset

Client PIN Number:

Start PIN

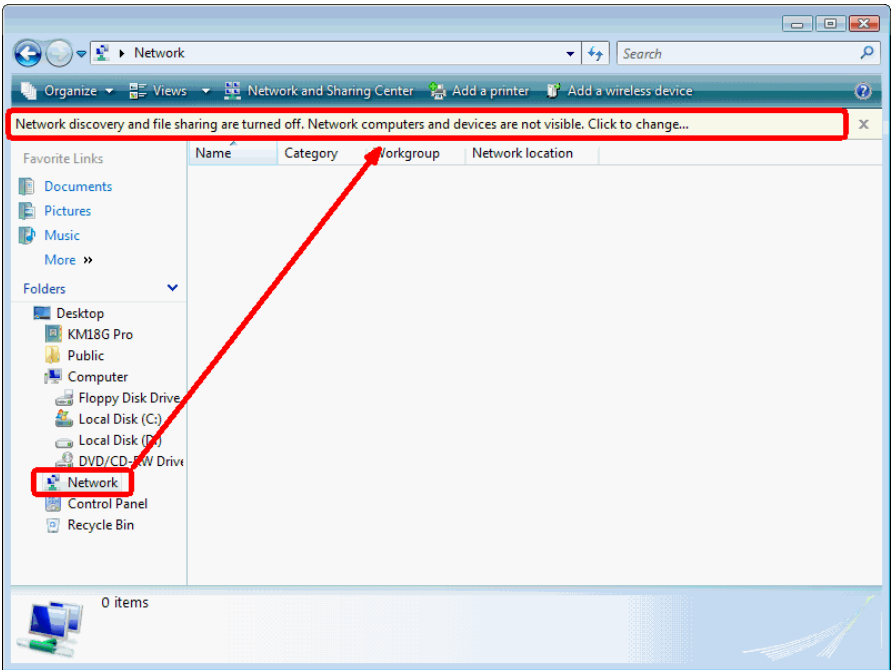
3. Plug the Ethernet cable into AP's LAN port and make sure the IP connection is valid with Vista.

4. Make sure WCN is enabled. Users may need to enable it at the first time. They could open the "Control Panel", click "Classic View", open "Administrative Tools", double click "Services", , a User Account Control pop up and click "Continue", edit properties of "Windows Connect Now", choose the "Startup type" with "Automatic" and click "Start".

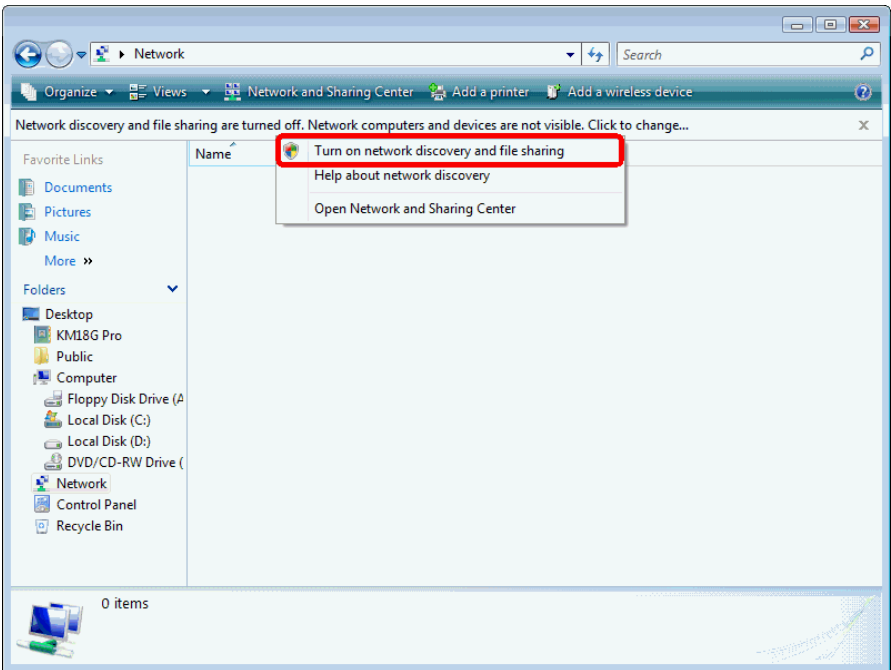


5. If the previous steps are done, open Windows Explorer. Go to the Network section.

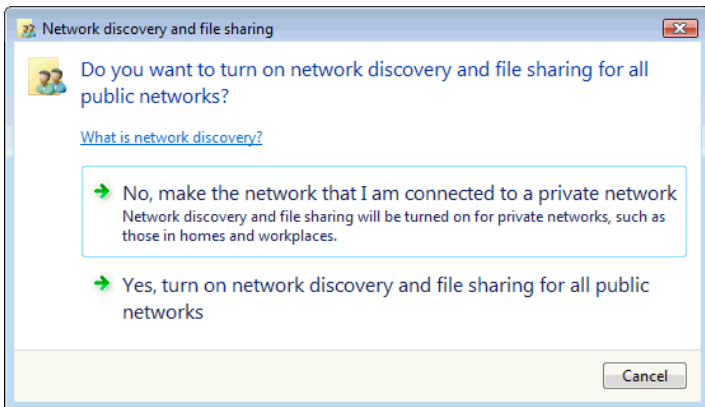
6. Click on "Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to Change..."



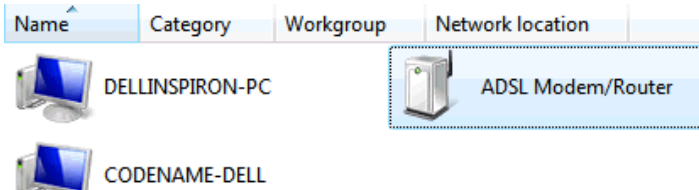
7. Click on "Turn on network discovery and file sharing"



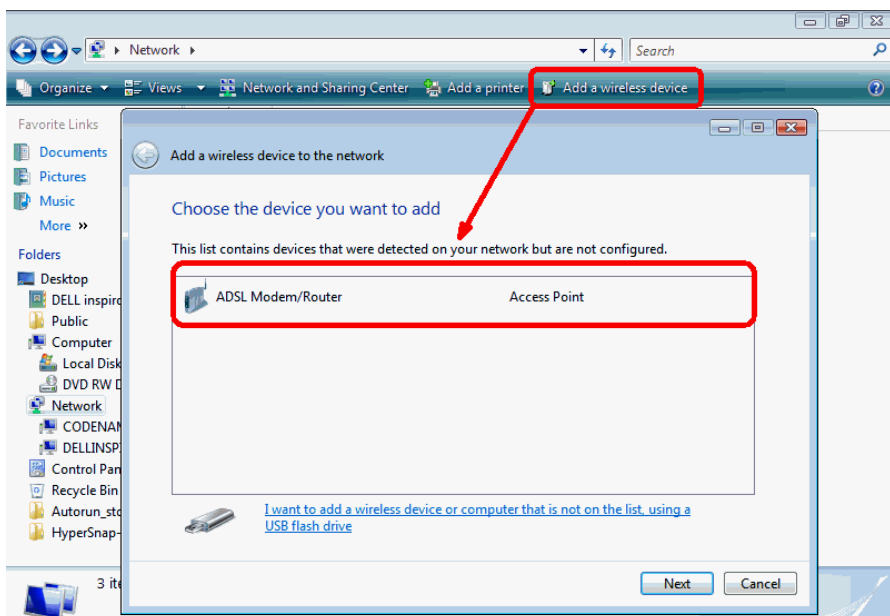
8. Click on “No, make the network that I am connected to a private network”



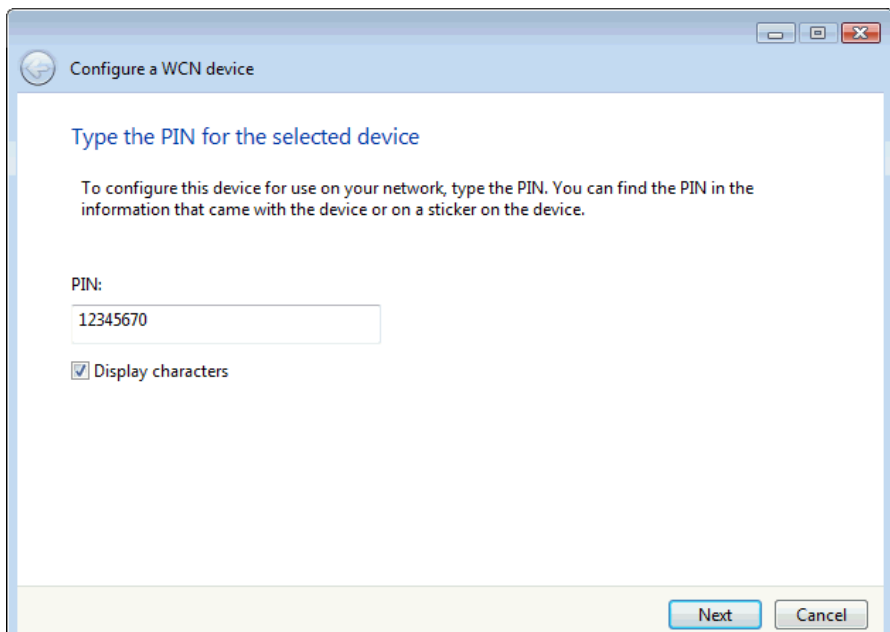
9. AP's icon will show up. Double click on it.



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



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



Configure a WCN device

Type the PIN for the selected device

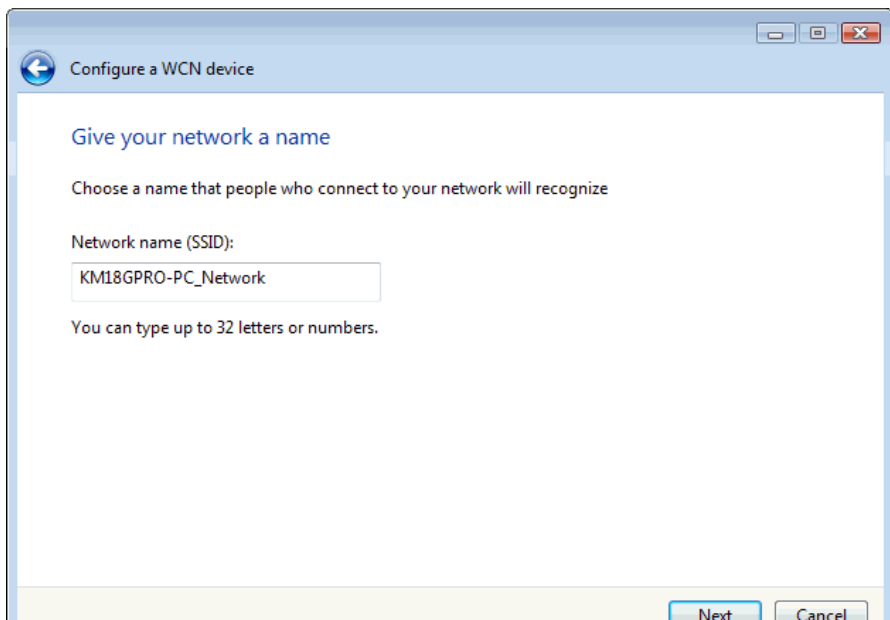
To configure this device for use on your network, type the PIN. You can find the PIN in the information that came with the device or on a sticker on the device.

PIN:

Display characters

Next Cancel

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



Configure a WCN device

Give your network a name

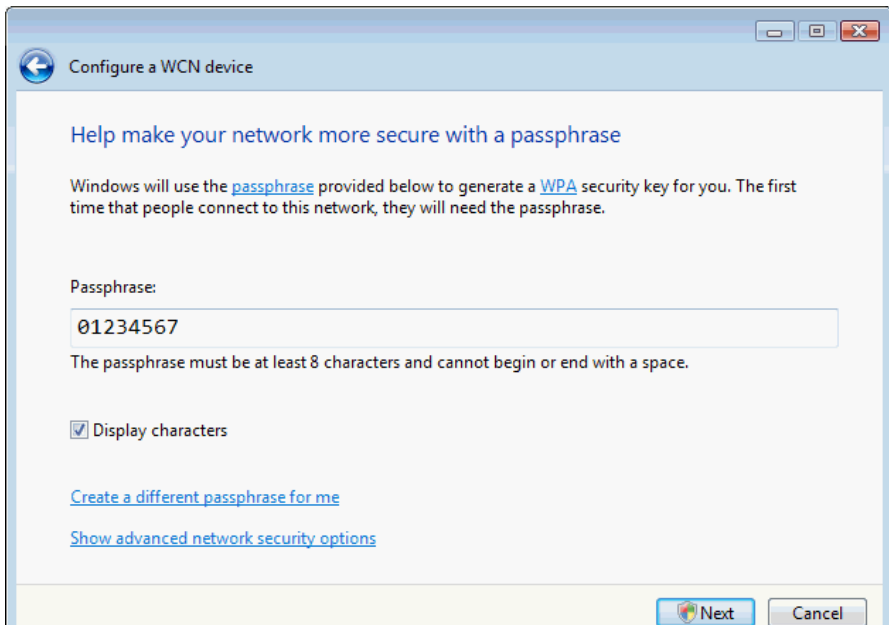
Choose a name that people who connect to your network will recognize

Network name (SSID):

You can type up to 32 letters or numbers.

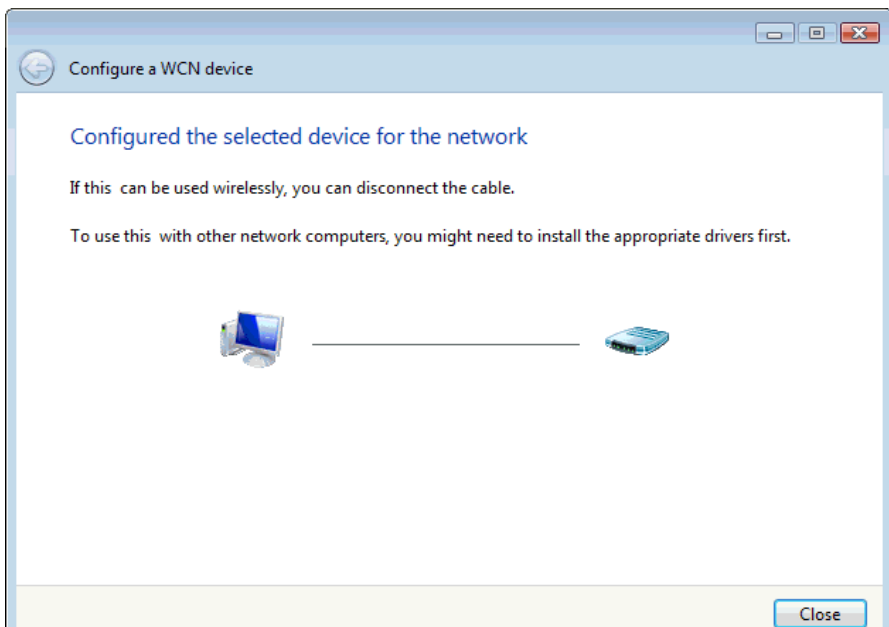
Next Cancel

13. Enter the Passphrase and then click Next.



14. A User Account Control screen pops up, click Continue.

15. AP is successfully configured by WCN.



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

Wi-Fi Protected Setup

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

Disable WPS

WPS Status:

Configured UnConfigured

Self-PIN Number:

12345670

Regenerate PIN

Push Button Configuration:

Start PBC

Apply Changes

Reset

Current Key Info:

Authentication	Encryption	Key
WPA PSK	TKIP	C7Un2aEccjPyhkr01CTDX3

Client PIN Number:

Start PIN

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

Wireless Basic Settings

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

Disable Wireless LAN Interface

Band:

2.4 GHz (B+G) ▼

Mode:

AP ▼

Network Type:

Infrastructure ▼

SSID:

KM18GPRO-PC_Network

Channel Number:

11 ▼

Associated Clients:

Show Active Clients

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode
(Acting as AP and client simultaneously)

SSID of Extended Interface:

Apply Changes

Reset

Operations of AP - AP being a registrar

AP mode

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

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

Wi-Fi Protected Setup

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

Disable WPS

WPS Status:

Configured UnConfigured

Self-PIN Number:

12345670

Regenerate PIN

Push Button Configuration:

Start PBC

Apply Changes

Reset

Client PIN Number:

19953533

Start PIN

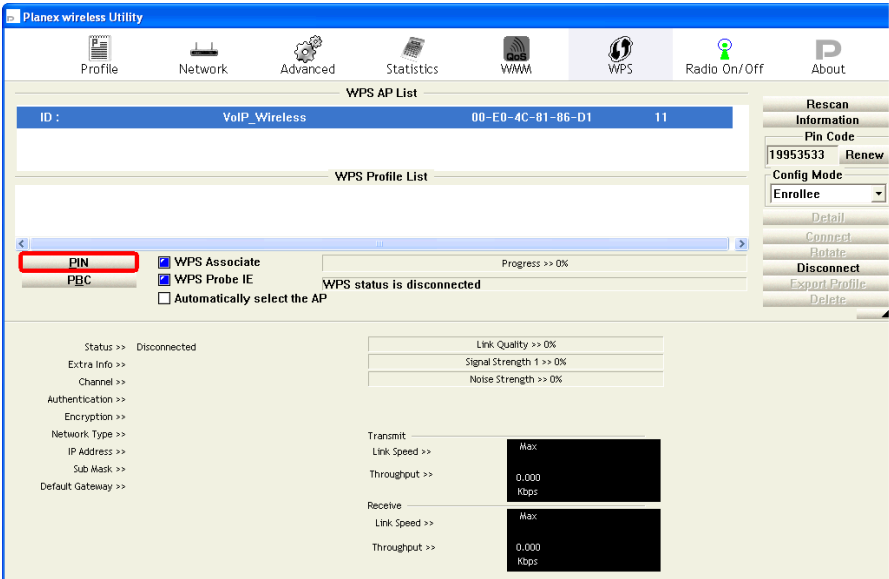
5. Users must start the PIN method on the station side within two minutes.

Applied client's PIN successfully!

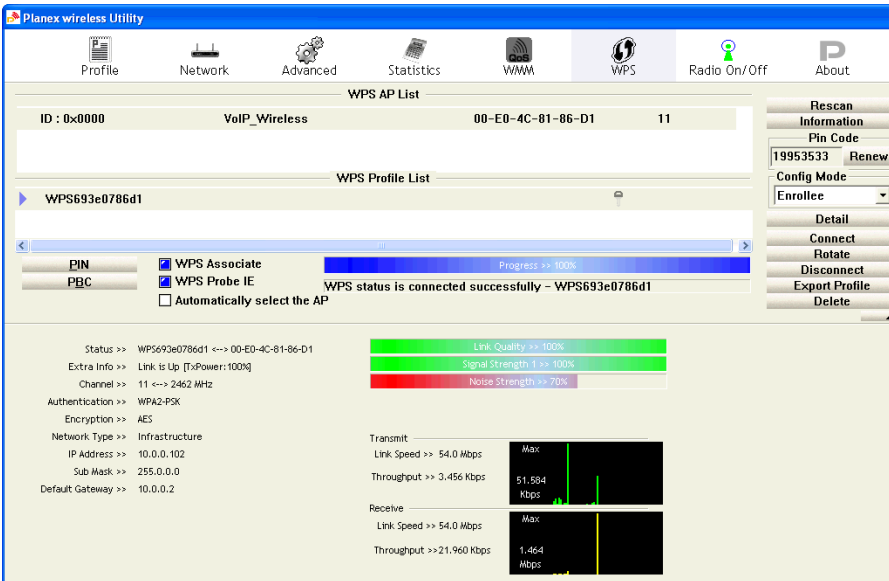
You have to run Wi-Fi Protected Setup in client within 2 minutes.

OK

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



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



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

Wi-Fi Protected Setup

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

Disable WPS

WPS Status: Configured UnConfigured

Self-PIN Number:

Push Button Configuration:

Current Key Info:

Authentication	Encryption	Key
WPA PSK	TKIP	3b82fe8b3dad5d965d4a0e

Client PIN Number:

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

Push Button method

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

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

1. From the left-hand *Wireless* -> *WPS* menu. The following page is displayed:
2. Make sure AP is in un-configured state.
3. Click *Start PBC*.

Wi-Fi Protected Setup

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

Disable WPS

WPS Status: Configured UnConfigured

Self-PIN Number:

Push Button Configuration:

Client PIN Number:

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

Start PBC successfully!

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

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

The screenshot displays the Planex wireless Utility interface for WPS configuration. At the top, navigation tabs include Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The main area is titled 'WPS AP List' and shows a single entry with ID: VoIP_Wireless, MAC: 00-E0-4C-81-86-D1, and SSID: 11. Below this is the 'WPS Profile List' section, which is currently empty. A selection menu at the bottom left shows 'PIN' selected and highlighted with a red box, with 'PBC' also visible. To the right of this menu, there are checkboxes for 'WPS Associate' (checked), 'WPS Probe IE' (checked), and 'Automatically select the AP' (unchecked). A status indicator shows 'WPS status is disconnected' and 'Progress >> 0%'. On the far right, a 'Rescan Information' sidebar shows 'Pin Code: 19953533' and 'Enrollee' mode. The bottom section of the page displays various network statistics, including 'Link Quality >> 0%', 'Signal Strength 1 >> 0%', 'Noise Strength >> 0%', and 'Throughput >> 0.000 Kbps' for both Transmit and Receive directions.

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

The screenshot shows the 'Planex wireless Utility' interface with the 'WPS' tab selected. The 'WPS AP List' shows a single entry for 'WPS693e0786d1'. The 'WPS Profile List' also shows this profile. The 'WPS status' is 'connected successfully - WPS693e0786d1'. The 'WPS Associate' checkbox is checked, and the 'WPS Probe IE' checkbox is also checked. The 'Automatically select the AP' checkbox is unchecked. The 'Progress' bar is at 100%. The 'Link Quality' is 100%, 'Signal Strength' is 100%, and 'Noise Strength' is 70%. The 'Transmit' section shows 'Link Speed >> 54.0 Mbps' and 'Throughput >> 3.454 Kbps'. The 'Receive' section shows 'Link Speed >> 54.0 Mbps' and 'Throughput >> 21.960 Kbps'. The 'Status' section shows 'WPS693e0786d1 <-> 00-E0-4C-81-86-D1', 'Link is Up [TxPower:100%]', 'Channel >> 11 <-> 2462 Mhz', 'Authentication >> WPA2-PSK', 'Encryption >> AES', 'Network Type >> Infrastructure', 'IP Address >> 10.0.0.102', 'Sub Mask >> 255.0.0.0', and 'Default Gateway >> 10.0.0.2'. The 'Rescan Information' section shows 'Pin Code 19953533', 'Renew', 'Config Mode', 'Enrollee', and 'Detail' options.

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

Wi-Fi Protected Setup

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

Disable WPS

WPS Status:

Configured UnConfigured

Self-PIN Number:

12345670

Regenerate PIN

Push Button Configuration:

Start PBC

Apply Changes

Reset

Current Key Info:

Authentication	Encryption	Key
WPA PSK	TKIP	3b82fe8b3dad5d965d4a0e

Client PIN Number:

Start PIN

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

Internet Access

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

Your device needs the following address information in order to access the Internet:

ATM PVC	<p>To configure ATM PVC, enter the VPI and VCI provided by ISP. Select the Service Type Index, Service Category and enter the following information:</p> <ul style="list-style-type: none"> • Peak Cell Rate • Sustainable Cell Rate • Maximum Burst Size
Connection Type	<p>To configure the connection type, select the protocol and encapsulation type as indicated by ISP. Supported Protocol types are:</p> <ul style="list-style-type: none"> • RFC1483 Bridged • RFC1483 MER • PPPoE • PPPoA • RFC1483 Routed <p>Supported Encapsulation types are:</p> <ul style="list-style-type: none"> • VCMUX • LLC/SNAP
WAN IP Settings	<p>To configure WAN IP settings, enter the information as indicated by ISP. Enable/Disable the Access Concentrator option. Either enter the WAN IP or select the option to automatically obtain IP address.</p> <p>Check as applicable the following two options:</p> <ul style="list-style-type: none"> • Enable NAT • Add default Route

- Broadband Username and Password
- To configure Broadband Username and Password, enter the user name and password details. Also set the session establishment condition as one of the following:
- Continuous
 - Connect on demand. Enter the minutes after which the session must be disconnected, if no activity takes place.
 - Manual. Enter the minutes after which the session must be disconnected, if no activity takes place.

In most cases, you **will not** need to configure your device with these addresses because your ISP is likely to use an Internet access type which automatically assigns addresses to your device. For more information, see *Types of Internet Access*.

Types of Internet Access

The types of Internet access available are as follows:

- PPP Internet access – your device uses a Point to Point Protocol (PPP) to carry data between your ISP and your computer. To use PPP Internet access, you must enter a PPP login username and password the first time to log on. The IP addresses required to access your ISP's Internet service are automatically configured.

Your device supports PPPoE (over Ethernet).

- PPP Internet access – your device uses a Point to Point Protocol (PPP) to carry data between your ISP and your computer. To use PPP Internet access, you must enter a PPP login username and password the first time to log on. The IP addresses required to access your ISP's Internet service are automatically configured.

Your device supports PPPoA (over ATM).

- Bridged Internet access – your device uses a Bridge mode with your PPPoE Client Software to carry data between your ISP and your computer. To use Bridged Internet access with your PPPoE Client Software, you must enter a PPP login username and password the first time to log on. The IP addresses required to access your ISP's Internet service are automatically configured.

Your device supports RFC 1483 Bridged Mode).

Configuring your PPPoE DSL connection

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

Your ISP may also tell you to set unique path and circuit numbers (called VPI and VCI) in order to connect your device to the ISP's Internet service. In most cases, your device will use default settings, so you may not need to enter these values.



Your ISP will provide you with the login details and VPI/VCI values necessary to set up a PPP login account.

Note

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

1. From the left-hand *WAN* menu, click on *Channel Config*. The following page is displayed:
2. Enter VCI and VPI setting determined by your ISP.
3. Select the Encapsulation determined by your ISP.
4. From the *Channel Mode* drop-down list, select *PPPoE* setting.
5. Enter *User Name/Password* provided by your ISP. Type them in the relevant boxes.
6. If you are happy with your settings, click *Add*

WAN Configuration

This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router.

VPI: VCI: Encapsulation: LLC VC-Mux Channel Mode:
 Enable NAPT: Admin Status: Enable Disable

PPP Settings: User Name: Password:
 Type: Idle Time (min):

WAN IP Settings: Type: Fixed IP DHCP
 Local IP Address: Remote IP Address:
 Subnet Mask: Unnumbered
 Default Route: Disable Enable

Current ATM VC Table:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IP Addr	Remote IP	Subnet Mask	User Name	DRoute	Status	Actions
<input type="radio"/>	vc0	br1483	5	35	LLC							Enable	

Enable Auto-PVC Search
 VPI: VCI:

Current Auto-PVC Table:

PVC	VPI	VCI
-----	-----	-----

7. Your configuration is complete.
8. Now you are ready to Surf the Internet !!!

Configuring your PPPoA DSL connection

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

Your ISP may also tell you to set unique path and circuit numbers (called VPI and VCI) in order to connect your device to the ISP's Internet service. In most cases, your device will use default settings, so you may not need to enter these values.



Note

Your ISP will provide you with the login details and VPI/VCI values necessary to set up a PPP login account.

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

- From the left-hand *WAN* menu, click on *Channel Config*. The following page is displayed:
- Enter VCI and VPI setting determined by your ISP.
- Select the Encapsulation determined by your ISP.
- From the *Channel Mode* drop-down list, select *PPPoE* setting.
- Enter *User Name/Password* provided by your ISP. Type them in the relevant boxes.
- If you are happy with your settings, click **Add**

WAN Configuration

This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router.

VPI: <input type="text" value="0"/>	VCI: <input type="text" value="36"/>	Encapsulation: <input type="radio"/> LLC <input checked="" type="radio"/> VC-Mux	Channel Mode: <input type="text" value="PPPoA"/>
Enable NAPT: <input type="checkbox"/>	Admin Status: <input checked="" type="radio"/> Enable <input type="radio"/> Disable		
PPP Settings: User Name: <input type="text" value="1234"/>		Password: <input type="password" value="••••"/>	
Type: <input type="text" value="Continuous"/>	Idle Time (min): <input type="text"/>		

WAN IP Settings:

Type:	<input checked="" type="radio"/> Fixed IP	<input type="radio"/> DHCP
Local IP Address:	<input type="text"/>	Remote IP Address: <input type="text"/>
Subnet Mask:	<input type="text"/>	Unnumbered <input type="checkbox"/>
Default Route:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable

Add

Modify

Current ATM VC Table:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IP Addr	Remote IP	Subnet Mask	User Name	DRoute	Status	Actions
<input type="radio"/>	vc0	br1483	5	35	LLC							Enable	

Delete Selected

Enable Auto-PVC Search Apply

VPI: VCI: Add Delete

Current Auto-PVC Table:

PVC	VPI	VCI
-----	-----	-----

- Your configuration is complete.
- Now you are ready to Surf the Internet !!!

Configuring your Bridged DSL connection

- From the left-hand *WAN* menu, click on *Channel Config*. The following page is displayed:
- Enter VCI and VPI setting determined by your ISP.
- Select the Encapsulation determined by your ISP.
- From the *Channel Mode* drop-down list, select *1483 Bridged* setting.
- If you are happy with your settings, click Add

WAN Configuration

This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router.

VPI: VCI: Encapsulation: LLC VC-Mux Channel Mode: ▼

Enable NAPT: Admin Status: Enable Disable

PPP Settings: User Name: Password:

Type: Idle Time (min):

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address: Remote IP Address:

Subnet Mask: Unnumbered

Default Route: Disable Enable

Current ATM VC Table:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IP Addr	Remote IP	Subnet Mask	User Name	DRoute	Status	Actions
<input type="radio"/>	vc0	br1483	5	35	LLC							Enable	

Delete Selected

Enable Auto-PVC Search Apply

VPI: VCI: Add Delete

Current Auto-PVC Table:

PVC	VPI	VCI
-----	-----	-----

- Now you can load your PPPoE Client Software onto your PC.
- Now you can load your PPPoE Client Software with *user name* and *password* which determined by your ISP onto your PC.

Configuring your 1483 MER by DHCP

- From the left-hand *WAN* menu, click on *Channel Config*. The following page is displayed:
- Enter VCI and VPI setting determined by your ISP.
- Select the Encapsulation determined by your ISP.
- From the *Channel Mode* drop-down list, select *1483 MER* setting.
- From the *Type* ratio, click *DHCP*.
- If you are happy with your settings, click Add

WAN Configuration

This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router.

VPI: VCI: Encapsulation: LLC VC-Mux Channel Mode:

Enable NAPT: Admin Status: Enable Disable

PPP Settings: User Name: Password:

Type: Idle Time (min):

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address: Remote IP Address:

Subnet Mask: Unnumbered

Default Route: Disable Enable

Current ATM VC Table:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IP Addr	Remote IP	Subnet Mask	User Name	DRoute	Status	Actions
<input type="radio"/>	vc0	br1483	5	35	LLC							Enable	

Enable Auto-PVC Search

VPI: VCI:

Current Auto-PVC Table:

PVC	VPI	VCI
-----	-----	-----

- Your configuration is complete.
- Now you are ready to Surf the Internet !!!

Configuring your 1483 MER by Fixed IP

- From the left-hand *WAN* menu, click on *Channel Config*. The following page is displayed:
- Enter VCI and VPI setting determined by your ISP.
- Select the Encapsulation determined by your ISP.
- From the *Channel Mode* drop-down list, select *1483 MER* setting.
- From the *Type* ratio, click *Fixed IP*.
- Enter *Local IP Address*, *Subnet Mask* and *Remote IP Address* which was given by Telecom or by your Internet Service Provider (ISP).
- If you are happy with your settings, click Add

WAN Configuration

This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router.

VPI: VCI: Encapsulation: LLC VC-Mux Channel Mode: ▼

Enable NAPT: Admin Status: Enable Disable

PPP Settings: User Name: Password:

Type: Idle Time (min):

WAN IP Settings:

Type: Fixed IP DHCP

Local IP Address: Remote IP Address:

Subnet Mask: Unnumbered

Default Route: Disable Enable

Add

Current ATM VC Table:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IP Addr	Remote IP	Subnet Mask	User Name	DRoute	Status	Actions
<input type="radio"/>	vc0	br1483	5	35	LLC							Enable	

Enable Auto-PVC Search

VPI: VCI:

Current Auto-PVC Table:

PVC	VPI	VCI
-----	-----	-----

- Your configuration is complete.
- Now you are ready to Surf the Internet !!!

ATM Settings

- The page is for ATM PVC QoS parameters setting. The DSL device support 4 QoS mode —CBR/rt-VBR/nrt-VBR/UBR.
- From the left-hand WAN menu, click on *Channel Config*. The following page is displayed:

ATM Settings

This page is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for VPI, VCI, QoS etc ...

VPI: VCI: QoS:

PCR: CDVT: SCR: MBS:

Current ATM VC Table:

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
<input type="radio"/>	5	35	UBR	6000	0	---	---

Field	Description
VPI	Virtual Path Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table.
VCI	Virtual Channel Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table. The VCI, together with VPI, is used to identify the next destination of a cell as it passes through to the ATM switch.

QoS	Quality of Server, a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. The four QoS options are: -UBR (Unspecified Bit Rate): When UBR is selected, the SCR and MBS fields are disabled. -CBR (Constant Bit Rate): When CBR is selected, the SCR and MBS fields are disabled. -nrt-VBR (non-real-time Variable Bit Rate): When nrt-VBR is selected, the SCR and MBS fields are enabled. -rt-VBR (real-time Variable Bit Rate): When rt-VBR is selected, the SCR and MBS fields are enabled.
PCR	Peak Cell Rate, measured in cells/sec., is the cell rate which the source may never exceed.
SCR	Sustained Cell Rate, measured in cells/sec., is the average cell rate over the duration of the connection.
MBS	Maximum Burst Size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the peak cell rate.
Function Button	Description
Apply Changes	Set new PVC OoS mode for the selected PVC. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.
Undo	Discard your settings.

ADSL Settings

The ADSL setting page allows you to select any combination of DSL training modes.

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

ADSL Settings

Adsl Settings.

ADSL modulation:

- G.Lite
 G.Dmt
 T1.413
 ADSL2
 ADSL2+

AnnexL Option: (Note: Only ADSL 2 supports AnnexL)

- Enabled

AnnexM Option: (Note: Only ADSL 2/2+ support AnnexM)

- Enabled

ADSL Capability:

- Bitswap Enable
 SRA Enable

ADSL Tone:

Tone Mask

Apply Changes

Field	Description
ADSL modulation	Choose preferred xdsl standard protocols. G.lite : G.992.2 Annex A G.dmt : G.992.1 Annex A T1.413 : T1.413 issue #2 ADSL2 : G.992.3 Annex A ADSL2+ : G.992.5 Annex A
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.

Function Button	Description
Tone Mask	Choose tones to be masked. Mased tones will not carry any data.
Apply Changes	Click to save the setting to the configuration and the modem will be retrained.

Local Network Configuration

The *Addressing* page displays information about your LAN IP address and allows you to change the address and subnet mask assigned to your device.



Note

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

Changing the LAN IP address and subnet mask

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

LAN Interface Setup

This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP addresses, subnet mask, etc..

Interface Name:	br0
IP Address:	<input type="text" value="10.0.0.2"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<input type="checkbox"/> Secondary IP	
<input type="button" value="Apply Changes"/>	

From the left-hand *Services* menu, click on *DHCP Settings*.

DHCP Settings

This page be used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address:	10.0.0.2	Subnet Mask:	255.255.255.0
IP Pool Range:	<input type="text" value="10.0.0.33"/> - <input type="text" value="10.0.0.254"/>	<input type="button" value="Show Client"/>	
Subnet Mask:	<input type="text" value="255.255.255.0"/>		
Max Lease Time:	<input type="text" value="86400"/> seconds (-1 indicates an infinite lease)		
Domain Name:	<input type="text" value="domain.name"/>		
Gateway Address:	<input type="text" value="10.0.0.2"/>		
<input type="button" value="Apply Changes"/>		<input type="button" value="MAC-Base Assignment"/>	

Change the *IP Pool Range* and then click *Apply Changes* button.

DHCP Settings

This page be used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 10.0.0.2 **Subnet Mask:** 255.255.255.0

IP Pool Range: -

Subnet Mask:

Max Lease Time: **seconds (-1 indicates an infinite lease)**

Domain Name:

Gateway Address:

Change setting successfully! Click *OK* button.

Change setting successfully!

From the left-hand *LAN* menu, click on *LAN*.

Type a new IP Address and Subnet Mask.

Click *Apply Changes*.

LAN Interface Setup

This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP addresses, subnet mask, etc..

Interface Name: **br0**

IP Address:

Subnet Mask:

Secondary IP

The primary IP address is being changed to 10.0.0.2 netmask 255.255.255.0. Then Please go to <http://10.0.0.2> to continue. Your browser communicates with the web server via the LAN connection, and changing the IP address may disrupt this.

You may also need to renew your DHCP lease:

Windows 95/98

- a. Select **Run...** from the **Start** menu.
- b. Enter **winiptcfg** and click **OK**.
- c. Select your ethernet adaptor from the pull-down menu
- d. Click **Release All** and then **Renew All**.
- e. **Exit** the winipcfg dialog.

Windows NT/Windows 2000/Windows XP

- a. Bring up a command window.
- b. Type **ipconfig /release** in the command window.
- c. Type **ipconfig /renew**.
- d. Type **exit** to close the command window.

Linux

- a. Bring up a shell.
- b. Type **pump -r** to release the lease.
- c. Type **pump** to renew the lease.



Note

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

From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

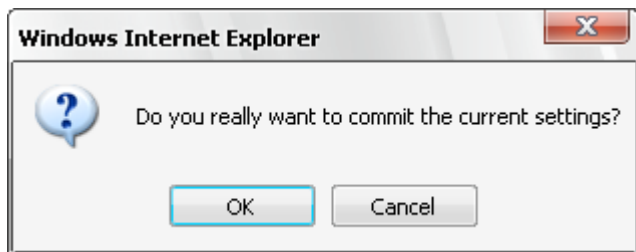
Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

Commit/Reboot page

Click on *OK*.



The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Adding the Secondary LAN IP address and subnet mask

- From the left-hand *LAN* menu, click on *LAN*.
- Check on *Secondary IP*.
- Type the Secondary IP Address and Subnet Mask.
- Click *Apply Changes*.

LAN Interface Setup

This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP addresses, subnet mask, etc..

Interface Name:	br0
IP Address:	<input type="text" value="10.0.0.2"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<input checked="" type="checkbox"/> Secondary IP	
IP Address:	<input type="text" value="10.0.0.4"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<input type="button" value="Apply Changes"/>	

- Change setting successfully! Click *OK* button.

Change setting successfully!

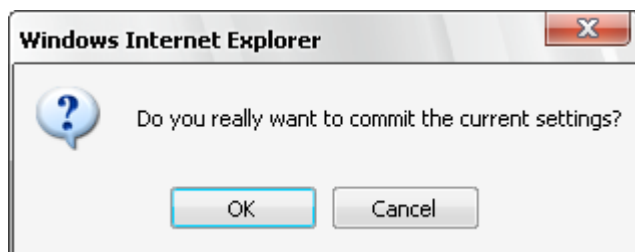
- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

Commit/Reboot page

- Click on *OK*.



- The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

DHCP Settings

You can configure your network and DSL device to use the Dynamic Host Configuration Protocol (DHCP). This page provides DHCP instructions for implementing it on your network by selecting the role of DHCP protocol that this device wants to play.

There are two different DHCP roles that this device can act as: DHCP Serve and DHCP Relay. When acting as DHCP server, you can setup the server parameters at the **DHCP Server** page; while acting as DHCP Relay, you can setup the relay at the **DHCP Relay** page.

DHCP Server Configuration

- From the left-hand *Services* menu, click on *DHCP Settings*.
- From *Services* check ratio, click on *DHCP Server Mode*.
- Type a new IP Pool Range, Subnet Mask, Max Lease Time, Domain Name and Gateway Address.
- Click on *Apply Changes*.

DHCP Settings

This page be used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 10.0.0.2 **Subnet Mask:** 255.255.255.0

IP Pool Range: -

Subnet Mask:

Max Lease Time: **seconds (-1 indicates an infinite lease)**

Domain Name:

Gateway Address:

Field	Description
IP Pool Range	Specify the lowest and highest addresses in the pool.
Max Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the device using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or a new IP is issued by the DHCP server. The amount of time is in units of seconds. The default value is 86400 seconds (1 day). The value -1 stands for the infinite lease.
Domain Name	A user-friendly name that refers to the group of hosts (subnet) that will be assigned addresses from this pool.

Function Button	Description
Show Client	This shows the assigned IP address, MAC address and time expired for each DHCP leased client.

Apply Changes	Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.
Undo	Discard your changes.

- Change setting successfully! Click *OK* button.

Change setting successfully!

OK

- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

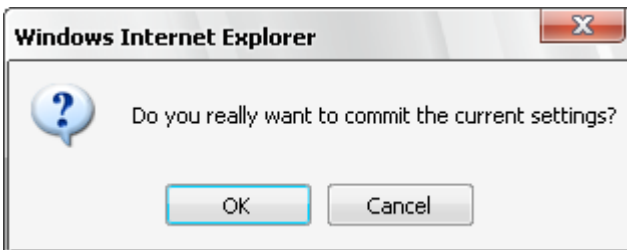
Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

Commit/Reboot page

- Click on *OK*.



- The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

DHCP Relay Configuration

- From the left-hand *Services* menu, click on *DHCP Settings*.
- From *Services* check ratio, click on *DHCP Relay Mode*.
- Type DHCP server IP Addresses for DHCP Relay.
- Click on *Apply Changes*.

DHCP Settings

This page be used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

DHCP Relay Configuration

This page is used to configure the DHCP server ip addresses for DHCP Relay.

DHCP Server Address:

192.168.10.100

Apply Changes

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

Function Button	Description
Apply Changes	Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

- Change setting successfully! Click *OK* button.

Change setting successfully!

A rectangular button with a thin blue border and the text "OK" in black.

- You need to renew your DHCP lease:

Windows 95/98

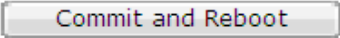
- a. Select **Run...** from the **Start** menu.
- b. Enter **winipcfg** and click **OK**.
- c. Select your ethernet adaptor from the pull-down menu
- d. Click **Release All** and then **Renew All**.
- e. **Exit** the winipcfg dialog.

Windows NT/Windows 2000/Windows XP

- a. Bring up a command window.
- b. Type **ipconfig /release** in the command window.
- c. Type **ipconfig /renew**.
- d. Type **exit** to close the command window.

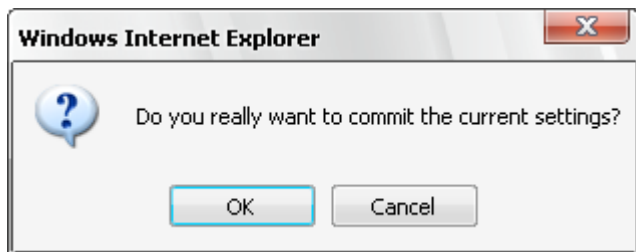
Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

A rectangular button with a grey gradient and a thin border, containing the text "Commit and Reboot".

Commit/Reboot page

- Click on *OK*.



- The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

DHCP None Configuration

- From the left-hand *Services* menu, click on *DHCP Settings*.
- From *Services* check ratio, click on *None Mode*.
- Click on *Apply Changes*.

DHCP Settings

This page be used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

Apply Changes

Function Button	Description
Apply Changes	Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

- Change setting successfully! Click *OK* button.

Change setting successfully!



- You need to renew your DHCP lease:

Windows 95/98

- a. Select **Run...** from the **Start** menu.
- b. Enter **wiipcfg** and click **OK**.
- c. Select your ethernet adaptor from the pull-down menu
- d. Click **Release All** and then **Renew All**.
- e. **Exit** the wiipcfg dialog.

Windows NT/Windows 2000/Windows XP

- a. Bring up a command window.
- b. Type **ipconfig /release** in the command window.
- c. Type **ipconfig /renew**.
- d. Type **exit** to close the command window.

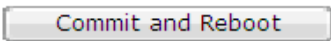
Linux

- a. Bring up a shell.
- b. Type **pump -r** to release the lease.
- c. Type **pump** to renew the lease.

- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

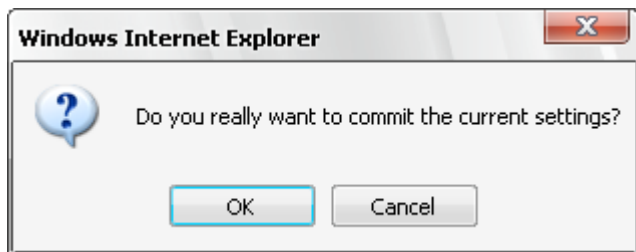
Commit/Reboot

This page is used to commit changes to system memory and reboot your system.



Commit/Reboot page

- Click on *OK*.



- The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

DNS Configuration

There are two submenus for the DNS Configuration: **DNS Server** and **Dynamic DNS**

DHCP Server Configuration - Attain DNS Automatically

- From the left-hand *Services* menu, click on *DNS -> DNS Server*.
- From check ratio, click on *Attain DNS Automatically*.
- Click on *Apply Changes*.

DNS Configuration

This page is used to configure the DNS server IP addresses for DNS Relay.

Attain DNS Automatically

Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Apply Changes

Reset Selected

Field	Description
Attain DNS Automatically	Select this item if you want to use the DNS servers obtained by the WAN interface via the auto-configuration mechanism.
Set DNS Manually	Select this item to configure up to three DNS IP addresses.

Function Button	Description
Apply Changes	Set new DNS relay configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.
Reset Selected	Discard your changes.

- Change setting successfully! Click *OK* button.

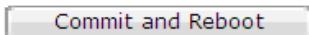
Change setting successfully!



- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

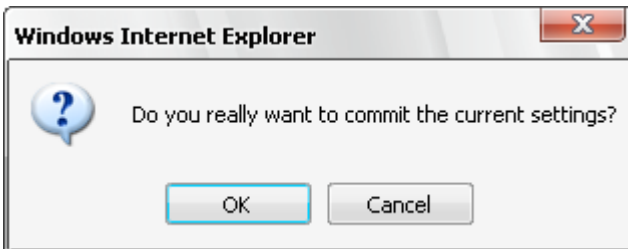
Commit/Reboot

This page is used to commit changes to system memory and reboot your system.



Commit/Reboot page

- Click on *OK*.



The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

DHCP Server Configuration - Set DNS Manually

- From the left-hand *Services* menu, click on *DNS -> DNS Server*.
- From check ratio, click on *Attain Set DNS Manually*.
- Enter the IP Address of DNS.
- Click on *Apply Changes*.

DNS Configuration

This page is used to configure the DNS server IP addresses for DNS Relay.

Attain DNS Automatically

Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Field	Description
Attain DNS Automatically	Select this item if you want to use the DNS servers obtained by the WAN interface via the auto-configuration mechanism.
Set DNS Manually	Select this item to configure up to three DNS IP addresses.

Function Button	Description
Apply Changes	Set new DNS relay configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.
Reset Selected	Discard your changes.

- Change setting successfully! Click *OK* button.

Change setting successfully!

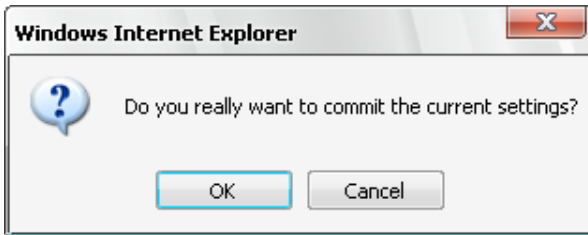
- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

Commit/Reboot page

- Click on *OK*.



- The System is Restarting ...
System rebooting, Please wait ... 57

The System is Restarting ...

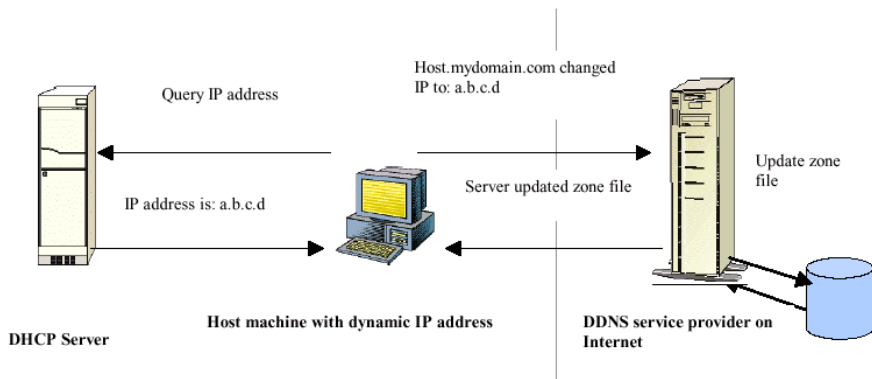
The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Overview of Dynamic DNS

If some host has a dynamic IP address that keeps changing frequently, it is difficult to keep updating the IP record that is associated with the domain name of this host in the zone files. This will result in non-accessibility of this host on the Internet. Dynamic DNS service allows to keep mapping of a dynamic IP address of such host to a static hostname. Dynamic DNS services are provided by many websites. The host needs

to register with some website and get a domain name. When the IP address of the host changes, it just needs to send a message to the website that's providing dynamic DNS service to this host. For this to work, an automated update client needs to be implemented. These update clients send update messages to the servers whenever there is some change in the IP address of that host. Then, the server updates the entries for that host and replies back with some return code.



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

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

Registering With Dynamic DNS Service Provider

Currently, Wireless ADSL2+ Router supports two Dynamic DNS service providers, www.tzo.com and www.dyndns.com. To use their Dynamic DNS service, you first need to visit the Web site of a service provider and register. While registering, you need to provide your username, password, and hostname as mandatory parameters. A service provider may also prompt you to fill some optional parameters.

Configuring IP Interfaces

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



Note

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

Dynamic DNS Configuration – DynDNS.org

- From the left-hand *Services* menu, click on *DNS -> Dynamic DNS*.
- Check the *Enable* check box.
- From *DDNS provider* drop-down list, select *DynDNS.org*.
- Enter the *Hostname*.
- Enter the *Username*.
- Enter the *Password*.
- Click *Add* button.

Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.

Enable:
DDNS provider:
Hostname:

DynDns Settings:

Username:
Password:

TZO Settings:

Email:
Key:

Field	Description
Enable	Check this item to enable this registration account for the DNS server.
DDNS provider	There are two DDNS providers to be selected in order to register your device with: DynDNS and TZO . A charge may occurs depends on the service you select.

Hostname	Domain name to be registered with the DDNS server.
Username	User-name assigned by the DDNS service provider.
Password	Password assigned by the DDNS service provider.

Function Button	Description
Add	Click Add to add this registration into the configuration.
Modify	Click Modify to modify this registration into the configuration.
Remove	Select an existing DDNS registration by clicking the radio button at the Select column of the Dynamic DNS Table . Click Remove button to remove the selected registration from the configuration.

- Configure Dynamic DNS setting successfully!

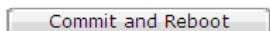
Dynamic DDNS Table:

Select	state	Hostname	Username	Service
<input type="radio"/>	Enable	golden0909.dyndns.org	golden0909	dyndns

- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

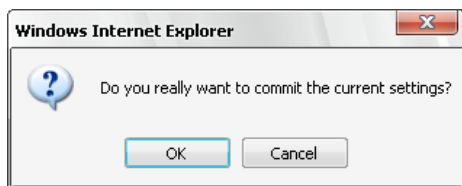
Commit/Reboot

This page is used to commit changes to system memory and reboot your system.



Commit/Reboot page

- Click on OK.



- The System is Restarting ...

System rebooting. Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

- Dynamic DNS Configuration – TZO
- From the left-hand *Services* menu, click on *DNS -> Dynamic DNS*.
- Check the *Enable* check box.
- From *DDNS provider* drop-down list, select *TZO*.

- Enter the *Hostname*, *Email* and *Password*.
- Click *Add* button.

Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.

Enable:

DDNS provider:

Hostname:

DynDns Settings:

Username:

Password:

TZO Settings:

Email:

Key:

Field	Description
Enable	Check this item to enable this registration account for the DNS server.
DDNS provider	There are two DDNS providers to be selected in order to register your device with: DynDNS and TZO . A charge may occurs depends on the service you select.
Hostname	Domain name to be registered with the DDNS server.
Email	Email that applied for the DDNS service provider.
Key	Key assigned by the DDNS service provider.

Function Button	Description
Add	Click Add to add this registration into the configuration.
Modify	Click Modify to modify this registration into the configuration.
Remove	Select an existing DDNS registration by clicking the radio button at the Select column of the Dynamic DNS Table . Click Remove button to remove the selected registration from the configuration.

- Configure Dynamic DNS setting successfully!

Dynamic DDNS Table:

Select	state	Hostname	Username	Service
<input type="radio"/>	Enable	golden0909.dyndns.org	golden0909	dyndns

- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

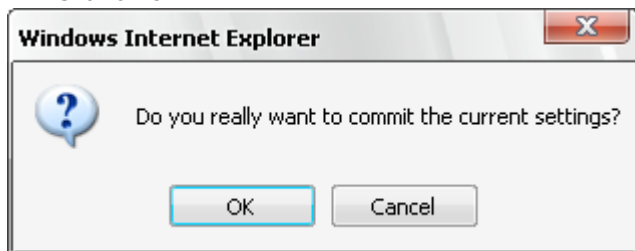
Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

Commit/Reboot page

- Click on *OK*.



- The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

IP/Port Filtering

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

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

IP/Port Filtering

- From the left-hand *Services* menu, click on *Firewall -> IP/Port Filtering*.

IP/Port Filtering

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

Outgoing Default Action Deny Allow
Incoming Default Action Deny Allow

Direction: **Protocol:** **Rule Action** Deny Allow
Source IP Address: **Subnet Mask:** **Port:** -
Destination IP Address: **Subnet Mask:** **Port:** -

Current Filter Table:

Select	Direction	Protocol	Src Address	Src Port	Dst Address	Dst Port	Rule Action
--------	-----------	----------	-------------	----------	-------------	----------	-------------

Fields on the first setting block	Description
Outgoing Default Action	Specify the default action on the LAN to WAN forwarding path.
Incoming Default Action	Specify the default action on the WAN to LAN forwarding path.

Function Button	Description
Apply Changes	Click to save the setting of default actions to the configuration.

Fields on the second setting block	Description
Rule Action	Deny or allow traffic when matching this rule.
Direction	Traffic forwarding direction.
Protocol	There are 3 options available: TCP, UDP and ICMP.
Source IP Address	The source IP address assigned to the traffic on which filtering is applied.
Source Subnet Mask	Subnet-mask of the source IP.
Source Port	Starting and ending source port numbers.
Destination IP Address	The destination IP address assigned to the traffic on which filtering is applied.
Destination Subnet Mask	Subnet-mask of the destination IP.
Destination Port	Starting and ending destination port numbers.

Function Button	Description
Apply Changes	Click to save the rule entry to the configuration.

Delete Selected	Delete selected filtering rules from the filter table. You can click the checkbox at the Select column to select the filtering rule.
Delete All	Delete all filtering rules from the filter table.

MAC Filtering

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

Configuring MAC filtering to Deny for outgoing access

- From the left-hand *Services* menu, click on *Firewall -> MAC Filtering*.
- From the *Direction* drop-down list, select *Outing* setting
- From the *Rule Action* check ratio, select *Deny*
- Enter the MAC Address that you want to deny for outgoing access in the *Source MAC Address*
- Click *Add*

MAC Filtering

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

Outgoing Default Action Deny Allow
Incoming Default Action Deny Allow

Direction: **Rule Action** Deny Allow

Source MAC Address:

Destination MAC Address:

- Configure MAC filtering setting successfully!

Current Filter Table:

Select	Direction	Src MAC Address	Dst MAC Address	Rule Action
<input type="checkbox"/>	Outgoing	00-0c-29-23-f1-4c	-----	Deny

Fields on the first setting block

Description

Outgoing Default Action

Specify the default action on the LAN to WAN bridging/forwarding path.

Incoming Default Action	Specify the default action on the WAN to LAN bridging/forwarding path.
-------------------------	--

Function Button	Description
-----------------	-------------

Apply Changes	Click to change the setting of default actions to the configuration.
---------------	--

Fields on the second setting block	Description
------------------------------------	-------------

Rule Action	Deny or allow traffic when matching this rule.
Direction	Traffic bridging/forwarding direction.
Source MAC Address	The source MAC address. It must be xxxxxxxxxxxx format. Blanks can be used in the MAC address space and are considered as don't care.
Destination MAC Address	The destination MAC address. It must be xxxxxxxxxxxx format. Blanks can be used in the MAC address space and are considered as don't care.

Function Button	Description
-----------------	-------------

Delete Selected	Delete selected filtering rules from the filter table. You can click the checkbox at the Select column to select the filtering rule.
Delete All	Delete all filtering rules from the filter table.

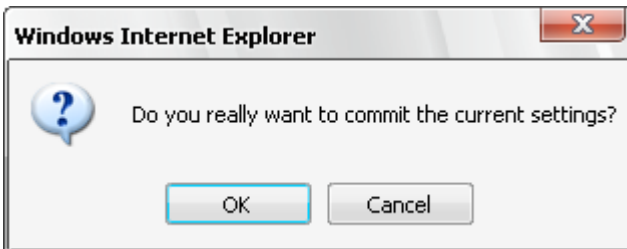
- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

- Click on *OK*.



- The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Port Forwarding

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

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

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

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

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

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

Configuring Port Forwarding

Certain network games, chat or file sharing software do not work with your default Port Forwarding setting. Your device knows the port, protocol and trigger information needed to allow access to the common applications listed below, but by default, access to them is disabled.

Application	TCP port number	UDP port number	Trigger required?
E-mail	110, 25	N/A	false
News	119	N/A	false
MSN Messenger	1863	N/A	false
Yahoo! Instant Messenger	5050 5055 5100	N/A	false
AOL Instant Messenger	5190	N/A	false

Application	TCP port number	UDP port number	Trigger required?
Internet Relay Chat (IRC)	194	194	false
	1720	N/A	true
Netmeeting (h323)	N/A	1719	true
	1731	N/A	false
	522	N/A	false
Real Audio	544 7070	544 6770	false
Ping	N/A (ICMP)	N/A (ICMP)	false
Web connections (HTTP, HTTPS)	80, 443	N/A	false
	51210	N/A	true
DialPad	N/A	51200	false
	N/A	51201	true
FTP	21	N/A	false
Telnet	23	N/A	false
Secure shell (SSH)	22	N/A	false
Windows Media Services	1755	1755	false
Gnutella	6346	N/A	false
Kazaa	1214	N/A	false
Windows Terminal Server	3389	N/A	false
DNS	N/A	53	false
PPTP	1723	1723	false
Internet Key Exchange	N/A	500	false
LDAP	389	N/A	false
GRE	N/A (GRE)	N/A (GRE)	false
Databeam (T.120)	1503	N/A	false

You can enable access to a common application from a specific PC on your network.

If you want to allow access to an application that is **not** included on the above list of common applications, you can create and enable a *custom* application.

Configuring custom applications

If you want to enable access to an application that does not appear on your device's default list of common applications you can create a custom application.

In order to create a custom application, you must know:

- the protocol used by the application (e.g., TCP, UDP and so on)
- the primary port or range of ports used by the application
- whether the application requires a trigger, and if so, the secondary port or range of ports used by the application
- the address translation type used by the trigger

Your application provider or games manufacturer should provide you with these details.

Port Forwarding for FTP

In this example configuration, a custom application called *FTP Server* using TCP port 21 is created.

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

Port Forwarding

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

Port Forwarding: Disable Enable

Protocol: Comment: Enable
 Local IP Address: Local Port: -

 Remote IP Address: Public Port: -

 Interface:

Current Port Forwarding Table:

Select	Local IP Address	Protocol	Local Port	Comment	Enable	Remote Host	Public Port	Interface
--------	------------------	----------	------------	---------	--------	-------------	-------------	-----------

- From the *Port Forwarding* check ratio, check on *Enable*
- Click *Apply Changes*
- Type the Local IP Address for your FTP Server.
- Enter the range of Local Port for your FTP Server.
- Select *any* from the *Interface* drop-down list.
- Click *Apply*

Port Forwarding

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

Port Forwarding: Disable Enable

Protocol: Comment: Enable
 Local IP Address: Local Port: -

 Remote IP Address: Public Port: -

 Interface:

Fields on the first setting block	Description
Enable Port Forwarding	Check this item to enable the port-forwarding feature.
Protocol	There are 3 options available: TCP, UDP and Both.
Enable	Check this item to enable this entry.
Local IP Address	IP address of your local server that will be accessed by Internet.
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 the incoming traffic is allowed. Leave blank for all.
External 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.

Function Button	Description
Apply Changes	Click to change the setting of default actions to the configuration.
Delete Selected	Delete the selected port forwarding rules from the forwarding table. You can click the checkbox at the Select column to select the forwarding rule.
Delete All	Delete all forwarding rules from the forwarding table.

Current Port Forwarding Table:

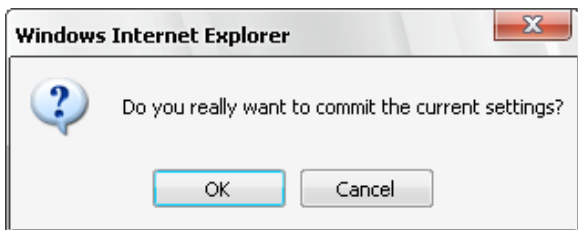
Select	Local IP Address	Protocol	Local Port	Comment	Enable	Remote Host	Public Port	Interface
<input type="checkbox"/>	10.0.0.33	TCP	21	FTP	Enable		----	ppp0

- Configure Port Forwarding setting successfully!
- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

- Click on *OK*.



- The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Port Forwarding for HTTP

In this example configuration, a custom application called *HTTP Server* using TCP port 80 is created.

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

Port Forwarding

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

Port Forwarding: Disable Enable

Protocol: Comment: Enable

Local IP Address: Local Port: -

Remote IP Address: Public Port: -

Interface:

Current Port Forwarding Table:

Select	Local IP Address	Protocol	Local Port	Comment	Enable	Remote Host	Public Port	Interface
--------	------------------	----------	------------	---------	--------	-------------	-------------	-----------

- From the *Port Forwarding* check ratio, check on *Enable*
- Click *Apply Changes*
- Type the Local IP Address for your HTTP Server.
- Enter the range of Local Port for your HTTP Server.
- Select *any* from the *Interface* drop-down list.
- Click *Apply*

Port Forwarding

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

Port Forwarding: Disable Enable

Protocol: **Comment:** **Enable**

Local IP Address: **Local Port:** -

Remote IP Address: **Public Port:** -

Interface:

Fields on the first setting block	Description
Enable Port Forwarding	Check this item to enable the port-forwarding feature.
Protocol	There are 3 options available: TCP, UDP and Both.
Enable	Check this item to enable this entry.
Local IP Address	IP address of your local server that will be accessed by Internet.
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 the incoming traffic is allowed. Leave blank for all.
External 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.

Function Button	Description
Apply Changes	Click to change the setting of default actions to the configuration.
Delete Selected	Delete the selected port forwarding rules from the forwarding table. You can click the checkbox at the Select column to select the forwarding rule.
Delete All	Delete all forwarding rules from the forwarding table.

- Configure Port Forwarding setting successfully!

Current Port Forwarding Table:

Select	Local IP Address	Protocol	Local Port	Comment	Enable	Remote Host	Public Port	Interface
<input type="checkbox"/>	10.0.0.33	TCP	80	HTTP	Enable		----	---

Delete Selected

Delete All

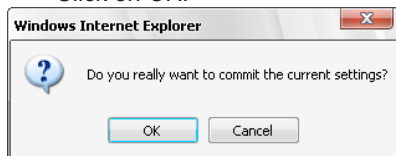
- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

- Click on *OK*.



The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Deleting custom applications

- From the left-hand *Services* menu, click on *Port Forwarding*.
- Check on the *Select* check box.
- Click *Delete Selected*.

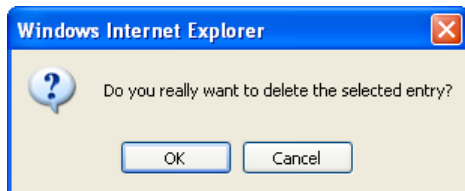
Current Port Forwarding Table:

Select	Local IP Address	Protocol	Local Port	Comment	Enable	Remote Host	Public Port	Interface
<input checked="" type="checkbox"/>	10.0.0.33	TCP	80	HTTP	Enable		----	---

Delete Selected

Delete All

- Click *Delete Selected*.



The Port Forwarding setting has been deleted completely.

Current Port Forwarding Table:

Select	Local IP Address	Protocol	Local Port	Comment	Enable	Remote Host	Public Port	Interface
--------	------------------	----------	------------	---------	--------	-------------	-------------	-----------

Delete Selected

Delete All

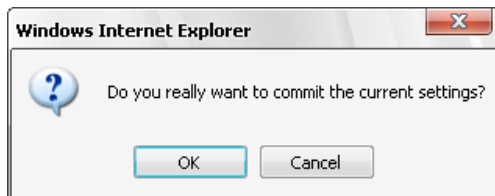
- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

- Click on *OK*.



- The System is Restarting...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

URL Blocking

The URL Blocking is the web filtering solution. The firewall includes the ability to block access to specific web URLs based on string matches. This can allow large numbers of URLs to be blocked by specifying only a FQDN (such as tw.yahoo.com). The URL Blocking enforce a Web usage policy to control content downloaded from, and uploaded to, the Web.

Configuring URL Blocking of FQDN

1. From the left-hand *Services* menu, click on *Firewall* -> *URL Blocking*. The following page is displayed:

URL Blocking Configuration

This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: Disable Enable

FQDN:

URL Blocking Table:

Keyword:

Keyword Filtering Table:

Fields on the first setting block	Description
URL Blocking capability	Check this item to enable the URL Blocking feature.
FQDN	A fully qualified domain name (or FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely, such as tw.yahoo.com. The FQDN will be blocked to access.
Keyword	The filtered keyword such as yahoo. If the URL includes this keyword, the URL will be blocked to access.

Function Button	Description
Apply Changes	Click to disable/enable the URL Blocking capability
Add FQDN	Add FQDN into URL Blocking table.
Delete Selected FQDN	Delete the selected FQDN from the URL Blocking table. You can click the checkbox at the Select column to select the Blocked FQDN.
Add Filtered Keyword	Add filtered keyword into Keyword Filtering table.
Delete Selected Keyword	Delete the selected keyword from the keyword Filtering table. You can click the checkbox at the Select column to select the filtered keyword.

- From the *URL Blocking* check ratio, check on *Enable*
- Click *Apply Changes*
- Type the FQDN in the FQDN field.
- Click *Add*

URL Blocking Configuration

This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: Disable Enable

FQDN:

URL Blocking Table:

Select	FQDN
<input type="checkbox"/>	

- Configure URL Blocking of FQDN setting successfully!

URL Blocking Table:

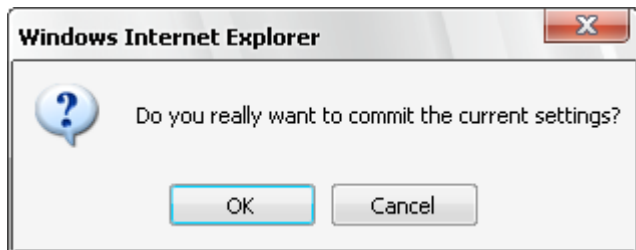
Select	FQDN
<input type="checkbox"/>	tw.yahoo.com

- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

- Click on *OK*.



Configuring URL Blocking of Keyword

- From the left-hand *Services* menu, click on *Firewall -> URL Blocking*. The following page is displayed:

URL Blocking Configuration

This page is used to configure the Blocked FQDN (Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: Disable Enable

FQDN:

URL Blocking Table:

Select	FQDN
--------	------

Keyword:

Keyword Filtering Table:

Select	Filtered Keyword
--------	------------------

Fields on the first setting block	Description
URL Blocking capability	Check this item to enable the URL Blocking feature.
FQDN	A fully qualified domain name (or FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely, such as tw.yahoo.com. The FQDN will be blocked to access.
Keyword	The filtered keyword such as yahoo. If the URL includes this keyword, the URL will be blocked to access.

Function Button	Description
Apply Changes	Click to disable/enable the URL Blocking capability
Add FQDN	Add FQDN into URL Blocking table.
Delete Selected FQDN	Delete the selected FQDN from the URL Blocking table. You can click the checkbox at the Select column to select the Blocked FQDN.
Add Filtered Keyword	Add filtered keyword into Keyword Filtering table.
Delete Selected Keyword	Delete the selected keyword from the keyword Filtering table. You can click the checkbox at the Select column to select the filtered keyword.

- From the *URL Blocking* check ratio, check on *Enable*
- Click *Apply Changes*
- Type the Keyword in the Keyword field.
- Click *Add*

URL Blocking Configuration

This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: Disable Enable

FQDN:

URL Blocking Table:

Select	FQDN
<input type="checkbox"/>	

Keyword:

Keyword Filtering Table:

Select	Filtered Keyword
<input type="checkbox"/>	

- Configure URL Blocking of Keyword setting successfully!

Keyword Filtering Table:

Select	Filtered Keyword
<input type="checkbox"/>	yahoo

Delete Selected

Delete All

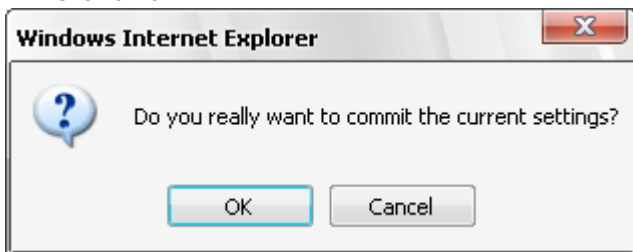
- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

- Click on *OK*.



Domain Blocking

The firewall includes the ability to block access to specific domain based on string matches. For example, if the URL of Taiwan Yahoo web site is "tw.yahoo.com" and you enter "yahoo.com", the firewall will block all the DNS queries with "yahoo.com" string. So the Host will be blocked to access all the URLs belong to "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.

Configuring Domain blocking

From the left-hand *Services* menu, click on *Firewall -> Domain blocking*. The following page is displayed:

Domain Blocking Configuration

This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.

Domain Blocking: Disable Enable

Domain:

Domain Block Table:

Select	Domain
--------	--------

Fields on the first setting block	Description
Domain Blocking capability	Check this item to enable the Domain Blocking feature.
FQDN	Domain

Function Button	Description
Apply Changes	Click to disable/enable the Domain Block capability
Add Domain	Add domain into Domain Block table.
Delete Selected Domain	Delete the selected domain from the Domain Block table. You can click the checkbox at the Select column to select the Blocked domain.

- From the *URL Blocking* check ratio, check on *Enable*
- Click *Apply Changes*
- Type the Keyword in the Keyword field.
- Click *Add*

Domain Blocking Configuration

This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.

Domain Blocking: Disable Enable

Domain:

- Configure Domain Blocking setting successfully!

Domain Block Table:

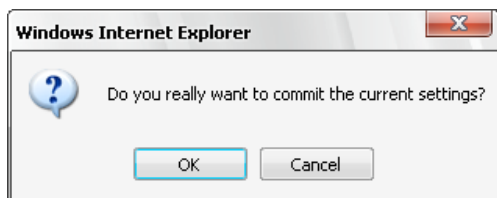
Select	Domain
<input type="checkbox"/>	yahoo.com

- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

- Click on *OK*.



DMZ

A demilitarized zone (DMZ) is a host or small network that acts as neutral ground between the inside and outside network. It contains information that is useful to users of both the inside and outside network. For example, a company may wish to provide software patches to customers via an FTP server. However, it does not want FTP access to any hosts other than the FTP server. This is achieved by creating a DMZ network which is less restrictive than the internal network. Users attached to the outside network can access the DMZ, but they cannot access any other company data.

Configuring DMZ

- From the left-hand *Services* menu, click on *Firewall -> Domain blocking*. The following page is displayed:

DMZ

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

DMZ Host:

Disable Enable

DMZ Host IP Address:

Fields on the first setting block	Description
Enable DMZ	Check this item to enable the DMZ feature.
DMZ Host IP Address	IP address of the local host. This feature sets a local host to be exposed to the Internet.

Function Button	Description
Apply Changes	Click to change the setting to the configuration.

- From the *DMZ Host* check ratio, check on *Enable*
- Type the IP Address in the *DMZ Host IP Address* field.
- Click *Apply Changes*

DMZ

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

DMZ Host: Disable Enable
 DMZ Host IP Address:

- Configure DMZ Host setting successfully! Click *OK*.

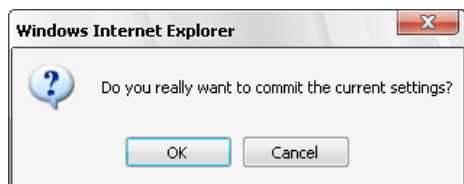
Change setting successfully!

- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

- Click on *OK*.



UPnP

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

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

The DSL device supports a control point for Universal Plug and Play (UPnP) version 1.0, and supports two key features: **NAT Traversal** and **Device Identification**. This feature requires one active WAN interface. In addition, the host should support this feature. In the presence of multiple WAN interfaces, select an interface on which the incoming traffic is present.

With NAT Traversal, when an UPnP command is received to open ports in NAT, the application translates the request into system commands to open the ports in NAT and the firewall. The interface to open the ports on is given to UPnP when it starts up and is part of the configuration of the application.

For Device Identification, the application will send a description of the DSL device as a control point back to the host making the request.

From the web page you can enable or disable UPnP.

Configuring UPnP

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

UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.

UPnP: Disable Enable

WAN Interface:

Apply Changes

Fields on the first setting block	Description
UPnP Daemon	Enable/disable UPnP feature.
Bound WAN Interface	Select WAN interface that will use UPnP from the drop-down lists.

Function Button	Description
Apply Changes	Click to save the setting to the configuration.

- From the *UPnP* check ratio, check on *Enable*
- Select a WAN Interface from the *WAN Interface* drop-down list.
- Click *Apply Changes*

UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.

UPnP: Disable Enable

WAN Interface:

- Configure DMZ Host setting successfully! Click *OK*.

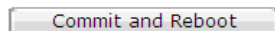
Change setting successfully!



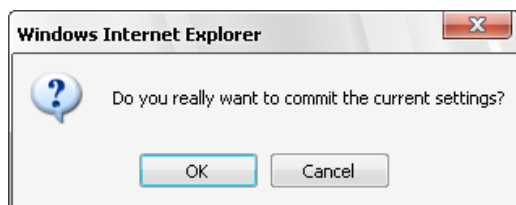
- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.



- Click on *OK*.



UPnP Control Point Software on Windows ME

To install the control point software on Windows ME:

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

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

UPnP Control Point Software on Windows XP with Firewall

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

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

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

1. In the Control Panel, select “Network and Internet Connections”.
2. In the “Network and Internet Connections” dialog box, select “Network Connections”.
3. In the “Network Connections” dialog box, right-click on the local area connection entry for your network; this will display a menu. Select the “Properties” menu entry.
4. In the “Local Area Connection Properties” dialog box, select the “Advanced” tab. Disable the Internet Connection Firewall by de-selecting the entry with the following label:
“Protect my computer and network by limiting or preventing access to the computer from the Internet”.
5. Click “OK”.

SSDP requirements

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

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

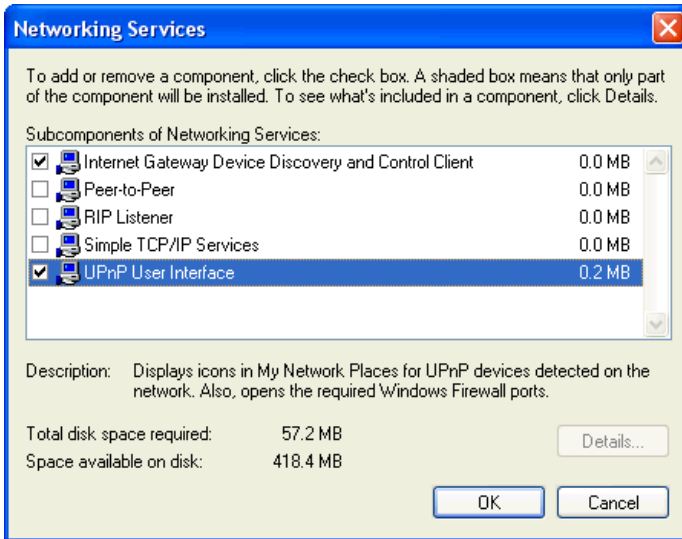
Installation procedure

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

1. In the Control Panel, select “Add/Remove Programs”.
2. In the “Add or Remove Programs” dialog box, click the “Add / Remove Windows Components” button.
3. In the “Windows Component Wizard” dialog box, scroll down the list to display the “Networking Services” entry. Highlight (select) the entry, and click on the “Details” button.
4. The “Networking Services” window is displayed.

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

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



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

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

- “Universal Plug and Play”.

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

- “Internet Gateway device discovery and Control Client”.
- “Universal Plug and Play”.

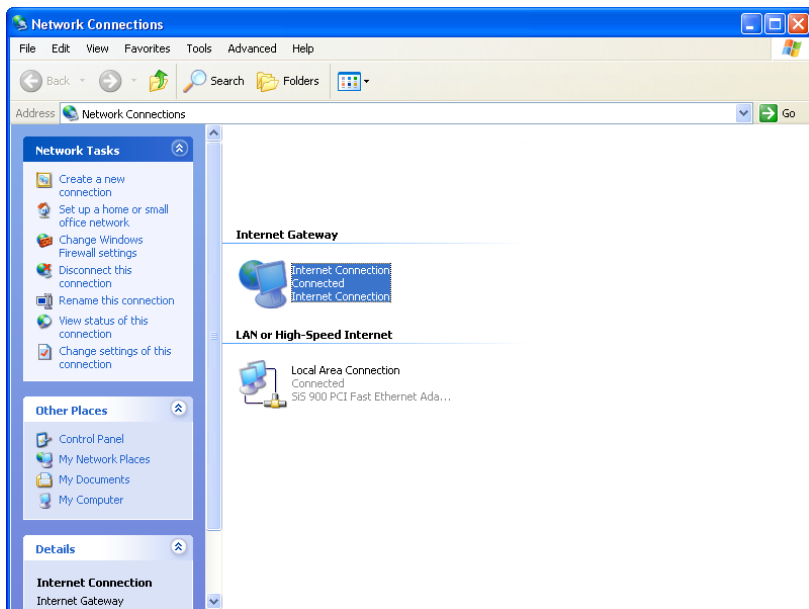
If you are using **Windows XP SP2**, select:

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

6. Reboot your system.

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

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



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 the ADSL Router, and one path to an ISP. In these cases, there is no need 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 the ADSL Router). The ADSL Router and the 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.

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

RIP Configuration

Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol. This page is used to select the interfaces on your device that use RIP, and the version of the protocol used.

RIP: Disable Enable

Apply Changes

Interface:

br0

Receive Mode:

None

Send Mode:

None

Add

RIP Config Table:

Select

Interface

Receive Mode

Send Mode

Delete Selected

Delete All

Fields on the first setting block	Description
RIP	Enable/disable RIP feature.
Fields on the second setting block:	Description
Interface	The name of the interface on which you want to enable RIP.
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.
Function buttons for the second setting block in this page	Description
Add	Add a RIP entry and the new RIP entry will be display in the table

Delete Selected Entry

Delete a selected RIP entry. The RIP entry can be selected on the **Select** column of the **RIP Config Table**.

ARP Table

This ARP Table shows a list of learned MAC addresses.

ARP Table

From the left-hand *Advance* menu, click on *ARP table*. The following page is displayed:

ARP Table

This table shows a list of learned MAC addresses.

IP Address	MAC Address
192.168.1.33	00:1D:09:A2:52:F9

Bridging

You can enable/disable Spanning Tree Protocol and set MAC address aging time in this page.

Bridging

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

Bridge Configuration

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

Ageing Time: (seconds)

802.1d Spanning Tree: Disabled Enabled

Fields on the first setting block	Description
Ageing Time	Set the Ethernet address ageing time, in seconds. After [Ageing Time] seconds of not having seen a frame coming from a certain address, the bridge will time out (delete) that address from Forwarding DataBase (fdb).
802.1d Spanning Tree	Enable/disable the spanning tree protocol

Function buttons	Description
Apply Changes	Save this bridge configuration. New configuration will take effect after saving into flash memory and rebooting the system. See section "Admin" for details.
Show MACs	List MAC address in forwarding table.

Routing

The Routing page enables you to define 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 DSL device provide the most appropriate path for all your Internet traffic.

–On your LAN hosts, a default gateway directs all Internet traffic to the LAN port(s) on the DSL device. Your LAN hosts know their default gateway either because you assigned it to them when you modified your TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet.

–On the DSL device itself, a default gateway is defined to direct all outbound Internet traffic to a route at your ISP. The default gateway is assigned either automatically by your ISP whenever the device negotiates an Internet access, or manually by user to setup through the configuration.

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.

Routing

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

Routing Configuration

This page is used to configure the routing information. Here you can add/delete IP routes.

Enable:

Destination:

Subnet Mask:

Next Hop:

Metric:

Interface:

Static Route Table:

Select	State	Destination	Subnet Mask	NextHop	Metric	IF
Fields on the first setting block		Description				
Enable		Check to enable the selected route or route to be added.				
Destination		The network IP address of the subnet. 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 that this 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 towards 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.				
Function buttons		Description				
Add Route		Add a user-defined destination route.				
Update		Update the selected destination route on the Static Route Table .				
Delete Selected		Delete a selected destination route on the Static Route Table .				
Show Routes		Click this button to view the DSL device's routing table. The IP Route Table displays, as shown in Figure.				

IP Route Table

This table shows a list of destination routes commonly accessed by your network.

Destination	Subnet Mask	NextHop	Metric	Iface
192.168.10.35	255.255.255.255	*	0	ppp0
10.0.0.0	255.255.255.0	*	0	br0
127.0.0.0	255.255.255.0	*	0	lo
0.0.0.0	0.0.0.0	*	0	ppp0

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 DSL device can be managed locally or remotely by SNMP protocol.

SNMP Protocol Configuration

This page is used to configure the SNMP protocol. Here you may change the setting for system description, trap ip address, community name, etc..

SNMP: Disable Enable

System Description:

System Contact:

System Name:

System Location:

System Object ID:

Trap IP Address:

Community name (read-only):

Community name (write-only):

SNMP

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

Fields on the first setting block	Description
System Description	System description of the DSL device.
System Contact	Contact person and/or contact information for the DSL device.
System Name	An administratively assigned name for the DSL device.
System Location	The physical location of the DSL device.
System Object ID	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.
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.
Function buttons	Description
Apply Changes	Save SNMP configuration. New configuration will take effect after saving into flash memory and rebooting the system. See section "Admin" for details.
Reset	Reset the configuration.

Port Mapping

The DSL device 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 DSL device can isolate traffic from group to group for some application. 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 group but only one group.

Port Mapping

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

Port Mapping Configuration

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click "Apply Changes" button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

Disabled Enabled

Grouped Interfaces

Available Interfaces



Select	Interfaces
Default	LAN1, LAN2, LAN3, LAN4, wlan0, vap0, vap1, vap2, vap3, ppp0

Apply Changes

Fields on the first setting block	Description
Enabled/Disabled	Radio buttons to enable/disable the interface group feature. If disabled, all interfaces belong to the default group.
Interface groups	To manipulate a mapping group: <ol style="list-style-type: none"> 1. Select a group from the table. 2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports. 3. Click "Apply Changes" button to save the changes.

Function buttons	Description
Apply Changes	Save SNMP configuration. New configuration will take effect after saving into flash memory and rebooting the system. See section "Admin" for details.

IP QoS

The DSL device provides a control mechanism that can provide different priority to different users or data flows. The QoS is enforced by the QoS rules in the QoS table. A QoS rule contains two configuration blocks: **Traffic Classification** and **Action**. The **Traffic Classification** enables you to classify packets on the basis of various fields in the packet and perhaps the physical ingress port. The **Action** enables you to assign the strictly priority level for and mark some fields in the packet that matches the Traffic Classification rule. You can configure any or all field as needed in these two QoS blocks for a QoS rule.

IP QoS

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

IP QoS

Entries in this table are used to assign the precedence for each incoming packet based on physical LAN port, TCP/UDP port number, and source/destination IP address/subnet masks.

IP QoS: Disabled Enabled Default QoS:

Specify Traffic Classification Rules

Source IP: Netmask: Port:
 Destination IP: Netmask: Port:
 Protocol: Physical Port:

Assign Priority and/or IP Precedence and/or Type of Service and/or DSCP

Outbound Priority: 802.1p:
 Precedence: TOS:

IP QoS Rules:

		Traffic Classification Rules					Mark				
Select	Status	Src IP	Src Port	Dst IP	Dst Port	Protocol	Lan Port	Priority	IP Preced	IP ToS	Wan 802.1p

Fields on the first setting block	Description
IP QoS	Enable/disable the IP QoS function.
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.
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.

Protocol	The selections are TCP, UDP, ICMP and the blank for none. This field is required if the source port or destination port has been entered.
Source Port	The source port of the selected protocol. You cannot configure this field without entering the protocol first.
Destination Port	The destination port of the selected protocol. You cannot configure this field without entering the protocol first.
Physical Port	The incoming ports. The selections include LAN ports, and the blank for not applicable.
Fields on the second setting block	Description
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.
IP Precedence	Select this field to mark the IP precedence bits in the packet that match this classification rule.
IP Type of Service	Select this field to mark the IP TOS bits in the packet that match this classification rule.
802.1p	Select this field to mark the 3-bit user-priority field in the 802.1p header of the packet that match 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.

Remote Access

The Remote Access function can secure remote host access to your DSL device from LAN and WLAN interfaces for some services provided by the DSL device.

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

Remote Access

This page is used to enable/disable management services for the LAN and WAN.

Service Name	LAN	WAN	WAN Port
TELNET	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="23"/>
FTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="21"/>
TFTP	<input type="checkbox"/>	<input type="checkbox"/>	
HTTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="80"/>
SNMP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
PING	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Fields	Description
LAN	Check/un-check the services on the LAN column to allow/un-allow the services access from LAN side; and “WAN”:
WAN	Check/un-check the services on the WAN column to allow/un-allow the services access from WAN side.
WAN Port	This field allows the user to specify the port of the corresponding 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 the dsl_addr is the WAN side IP address of the DSL device.

Function buttons	Description
Apply Changes	Save configuration. New configuration will take effect after saving into flash memory and rebooting the system. See section “Admin” for details.

Others

You can set some other advanced settings here.

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

Other Advanced Configuration

Here you can set some other advanced settings.

IP PassThrough: Lease Time: seconds
 Allow LAN access

Diagnostic

The DSL device supports some useful diagnostic tools.

Ping

Once you have your DSL device configured, it is a good idea to make sure you can ping the network. A ping command sends a message to the host you specify. If the host receives the message, it sends messages in reply. To use it, you must know the IP address of the host you are trying to communicate with and enter the IP address in the Host Address field. Click Go! To start the ping command, the ping result will then be shown in this page.

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

Ping Diagnostic

This page is used to send ICMP ECHO_REQUEST packets to network host. The diagnostic result will then be displayed.

Host Address :

Go !

Fields	Description
Host Address	The IP address you want to ping.

Function buttons	Description
Go	To start the ping command

- Type the IP Address in the *Host Address* field.
- Click Go

Ping Diagnostic

This page is used to send ICMP ECHO_REQUEST packets to network host. The diagnostic result will then be displayed.

Host Address :

192.168.10.100

Go !

- Now you could see the result below:
PING 192.168.10.100 (192.168.10.100): 56 data bytes

64 bytes from 192.168.10.100: icmp_seq=0

64 bytes from 192.168.10.100: icmp_seq=1

64 bytes from 192.168.10.100: icmp_seq=2

--- ping statistics ---

3 packets transmitted, 3 packets received.

Back

ATM Loopback

In order to isolate the 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. ATM uses F4 and F5 cell flows as follows:

- F4: used in VPs
- F5: used in VCs

An ATM connection consists of a group of points. This OAM implementation provides management for the following points:

- Connection endpoint: the end of a VP/VC connection where the ATM cell are terminated
- Segment endpoint: the end of a connection segment

This page allows you to use ATM ping, which generates F5 segment and end-to-end loop-back cells to test the reachability of a segment endpoint or a connection endpoint.

- From the left-hand *Diagnostic* menu, click on *ATM Loopback*. The following page is displayed:

OAM Fault Management - Connectivity Verification

Connectivity verification is supported by the use of the OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

Select PVC:

8/35

Flow Type: F5 Segment F5 End-to-End

Loopback Location ID:

Fields	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.
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.

Function buttons	Description
Go	To start the ATM Loopback test

ADSL

This page shows the ADSL diagnostic result. Click Start button to start the ADSL diagnostic.

- From the left-hand *Diagnostic* menu, click on *ADSL*. The following page is displayed:
- Click Start button to start the ADSL diagnostic.

Diagnostics -- ADSL

Adsl Tone Diagnostics. Only ADSL2/2+ support this function.

Start

	Downstream	Upstream
Hlin Scale	12257	0
Loop Attenuation(dB)	0.0	0.0
Signal Attenuation(dB)	0.0	0.0
SNR Margin(dB)	0.0	0.0
Attainable Rate(Kbps)	0	0
Output Power(dBm)	0.0	0.0

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0	0.000	0.000	-32.0	-23.0	-96.3
1	0.000	0.000	-32.0	-23.0	-96.3
2	0.000	0.000	-32.0	-23.0	-96.3
3	0.000	0.000	-32.0	-23.0	-96.3
4	0.000	0.000	-32.0	-23.0	-96.3
5	0.000	0.000	-32.0	-23.0	-96.3
6	0.000	0.000	-32.0	-23.0	-90.9
7	0.000	0.000	-32.0	-23.0	-96.0
8	0.000	0.000	-32.0	-23.0	-96.3
9	0.000	0.000	-32.0	-23.0	-93.3
10	0.000	0.000	-32.0	-23.0	-84.5
11	0.000	0.000	-32.0	-23.0	-91.4
12	0.000	0.000	-32.0	-23.0	-91.4

Diagnostic Test

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

- From the left-hand *Diagnostic* menu, click on *Diagnostic Test*. The following page is displayed:
- Click *RUN Diagnostic Test* button to start the ADSL diagnostic.

Diagnostic Test

The DSL Router is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic Test" button again to make sure the fail status is consistent.

Select the Internet Connection:

LAN Connection Check

Test Ethernet LAN Connection	PASS
------------------------------	------

ADSL Connection Check

Test ADSL Synchronization	PASS
---------------------------	------

Test ATM OAM F5 Segment Loopback	FAIL
----------------------------------	------

Test ATM OAM F5 End-to-end Loopback	FAIL
-------------------------------------	------

Test ATM OAM F4 Segment Loopback	FAIL
----------------------------------	------

Test ATM OAM F4 End-to-end Loopback	FAIL
-------------------------------------	------

Internet Connection Check

Test PPP Server Connection	PASS
----------------------------	------

Test Authentication with ISP	PASS
------------------------------	------

Test the assigned IP Address	PASS
------------------------------	------

Ping Default Gateway	PASS
----------------------	------

Ping Primary Domain Name Server	PASS
---------------------------------	------

Fields	Description
Select the Internet Connection	The available WAN side interfaces are listed. You have to select one for the WAN side diagnostic.

Function buttons	Description
RUN Diagnostic Test	To start the RUN Diagnostic Test

Commit/Reboot

Whenever you use the web console to change system settings, the changes are initially placed in temporary storage. To save your changes for future use, you can use the Commit/Reboot function. This function saves your changes from RAM to flash memory and reboot the system.

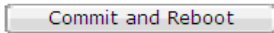
IMPORTANT! Do not turn off your modem or press the Reset button while this procedure is in progress.

Commit/Reboot

- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

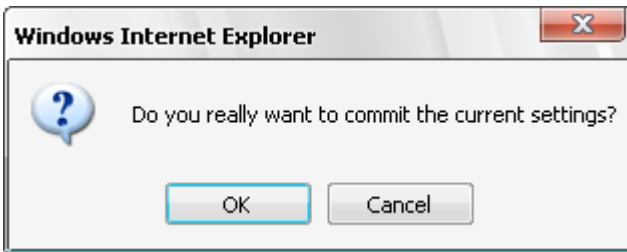
Commit/Reboot

This page is used to commit changes to system memory and reboot your system.



Commit/Reboot page

- Click on *OK*.



- The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Backup/Restore

You can save the current configuration of your Router to a file on your computer. This is highly recommended before you change any configuration settings on the Router or before you upgrade your firmware.

Backup settings

- From the left-hand *Admin* menu, click on *Backup/Restore*. The following page is displayed:

Backup/Restore Settings

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

Save Settings to File:

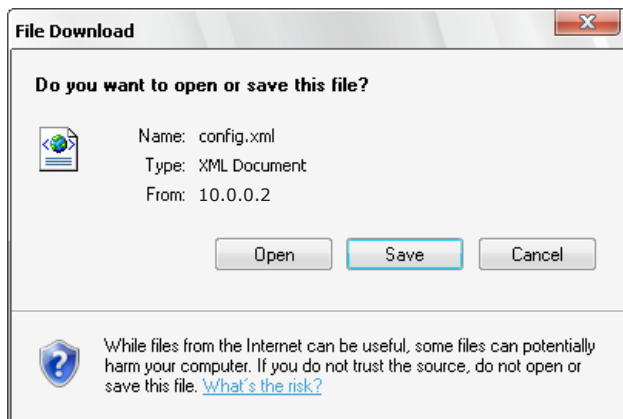
Load Settings from File:

Reset Settings to Default:

Backup & Restore page

Click on *Save*.

- Choose the *Save option* and select a suitable location and filename to save your backup file to.
- Press *Save*



Restore settings

- From the left-hand *Admin* menu, click on *Backup & Restore*. The following page is displayed:
- Click *Browse...* and browse to the location of your backup file
- Click *Upload*

Backup/Restore Settings

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

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

Backup & Restore page

Restore settings from config file successful! The System is Restarting ... The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration

Restore settings from config file successful! The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Resetting to Defaults

This page allows you to reset your device to its default factory settings.

The configuration settings of your device are stored in a configuration file. When you set up your device and access the web pages for the very first time, the configuration file contains a default factory configuration. This configuration has been set by MODECOM for you, and contains the basic settings that you can use without having to make extensive changes to the configuration.

If you do make changes to the default configuration but then wish to revert back

to the original factory configuration, you can do so by resetting the device to factory defaults.



Note

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

Software Reset:

- From the left-hand *Admin* menu, click on *Backup/Restore*. The following page is displayed:
- Click on *Reset*.

Backup/Restore Settings

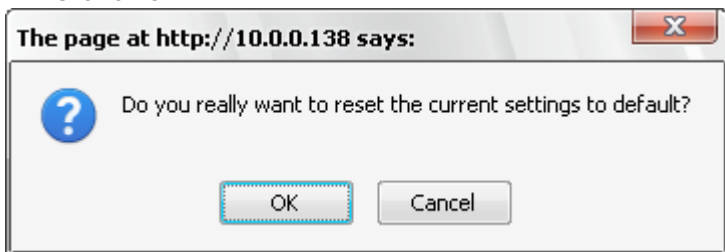
This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

- Click on *OK*.



- Please wait for 1 minute to let the system reboot.

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Password

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

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

Username: **admin**

Password: **administrator**

Username: **user**

Password: **user**

Setting your username and password



Note

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

To change the default password:

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

Password Setup

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

User Name:	<input type="text" value="admin"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirmed Password:	<input type="text"/>

Currently Defined Administration Password: Setup page

This page displays the current username and password settings. Change your own unique password in the relevant boxes. They can be any combination of letters or numbers with a maximum of 30 characters. The default setting uses **admin** for the username and **administrator** for password.

If you are happy with these settings, click **Apply Changes**. You will see following page that the new user has been displayed on the Currently Defined Users. You need to login to the web pages using your new username and new password.

Password Setup

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

User Name:

Old Password:


New Password:

Confirmed Password:

- Administration Password
- Click OK.

Change setting successfully!

- Enter new *User name* and *Password*.
- Click *Apply*.



The server 10.0.0.2 at requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

Password:

Remember my password

Login page

Firmware Update

The *Firmware Update* page allows you to:

- manually download the latest firmware version from website and manually update your firmware. See *Manually updating firmware*.

About firmware versions

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

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



Note

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

Manually updating firmware

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

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

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

Upgrade Firmware

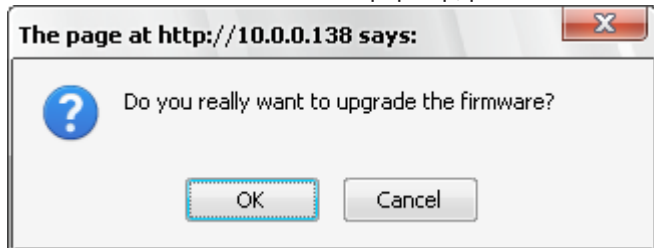
This page allows you upgrade the ADSL Router firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

**Select
File:**

Manual Update Installation section

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

- Use the *Choose file* box to navigate to the relevant directory where the firmware version is saved.
- Once you have selected the file to be installed, click *Open*. The file's directory path is displayed in the *Select File*: text box.
- Click *Upload*. The device checks that the selected file contains an updated version of firmware. A screen pops up, please click *OK*.



- Firmware upgrading, Please wait 120 seconds. Please DO NOT power off the device during the upload because it may crash the system.

**Firmware upgrading, Please wait ...
116**

Please note do NOT power off the device during the upload because it may crash the system.

Firmware update has been update complete and it will bring you to the home page of the device:

- From the left-hand *Admin* menu, click on *Backup/Restore*. The following page is displayed:
- Click on *Reset*.

ADSL Router Status

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

System	
Alias Name	MODECOM MC-4220 ADSL Router
Uptime	1 min
Firmware Version	RR1-A0-4X16M_STD_01_90311__2.0.0-RTK-090212
DSP Version	2.9.0.3d
Name Servers	
Default Gateway	

DSL	
Operational Status	G.dmt,SHOWTIME.
Upstream Speed	992 kbps
Downstream Speed	8064 kbps

LAN Configuration	
IP Address	10.0.0.2
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00e04c861234

WAN Configuration						
Interface	VPI/VCI	Encap	Protocol	IP Address	Gateway	Status
vc0	5/35	LLC	br1483			up

Refresh

Backup/Restore Settings

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

Save Settings to File:

Save...

Load Settings from File:

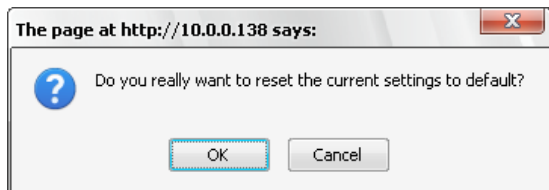
Browse...

Upload

Reset Settings to Default:

Reset

- Click on OK.



- Please wait for 1 minute to let the system reboot.

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

ACL Configuration

This page is used to configure the IP Address for Access Control List. If ACL is enabled, just these IP address that in the ACL Table can access CPE. Here you can add/delete IP Address.

ACL Config

From the left-hand *Admin* menu, click on *ACL Config*. The following page is displayed:

ACL Configuration

This page is used to configure the IP Address for Access Control List. If ACL is enabled, just these IP address that in the ACL Table can access CPE. Here you can add/delete IP Address.

ACL Capability: Disable Enable

Enable:
Interface:
IP Address:
Subnet Mask:

ACL Table:

Select	state	Interface	IP Address
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>		

ACL Configuration page

Check on *Enable*.

- From the Interface drop-down list, select *LAN*.
- Enter the *IP Address* and the *Subnet Mask*.
- Click *Add*.

ACL Configuration

This page is used to configure the IP Address for Access Control List. If ACL is enabled, just these IP address that in the ACL Table can access CPE. Here you can add/delete IP Address.

ACL Capability: Disable Enable

Enable:
Interface:
IP Address:
Subnet Mask:

ACL Table:

Select	state	Interface	IP Address
--------	-------	-----------	------------

- From the *ACL Capability* ratio, select *Enable*.
- Click *Apply Changes*.

ACL Configuration

This page is used to configure the IP Address for Access Control List. If ACL is enabled, just these IP address that in the ACL Table can access CPE. Here you can add/delete IP Address.

ACL Capability: Disable Enable

Enable:
Interface:
IP Address:
Subnet Mask:

ACL Table:

Select	state	Interface	IP Address
<input type="checkbox"/>	Enable	LAN	10.0.0.34/24

From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

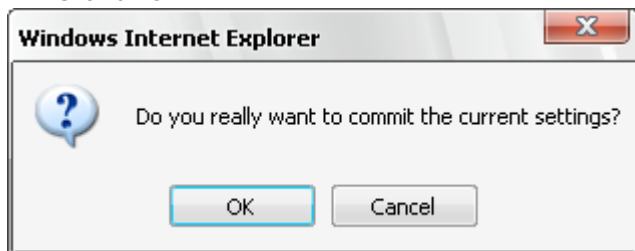
- Click on *Commit and Reboot*.

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

- Click on *OK*.



- The System is Restarting ...

System rebooting, Please wait ... 57

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Time Zone

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

SNTP Server and SNTP Client Configuration settings

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

Time Zone Setting

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

Current Time : Yr Mon Day Hr Mn Sec

Time Zone Select : ▼

Enable SNTP client update

SNTP server : ▼

(Manual IP Setting)

Fields	Description
Current Time	The current time of the specified time zone. You can set the current time by yourself or configured by SNTP.
Time Zone Select	The time zone in which the DSL device resides.
Enable SNTP client update	Enable the SNTP client to update the system clock.
SNTP server	The IP address or the host name of the SNTP server. You can select from the list or set it manually.

Function Button	Description
Apply Changes	Click to save the setting of default actions to the configuration.

Select your own Time Zone from the *Time Zone Select* drop-down list.

- Check on *Enable SNTP client update*.
- You can select the SNTP Server from the drop-down list or add association list using IP Address.
- Click on *Apply Change*.

Time Zone Setting

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

Current Time : Yr Mon Day Hr Mn Sec

Time Zone Select : ▼

Enable SNTP client update

SNTP server : ▼

(Manual IP Setting)

- SNTP Server Configuration page
- Configure SNTP setting successfully! Click **OK**.

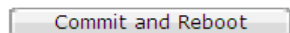
Change setting successfully!



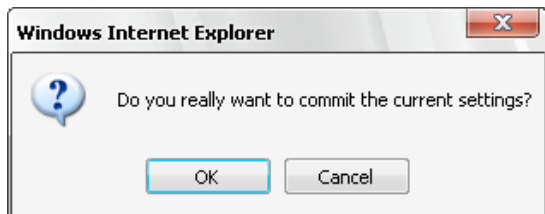
- From the left-hand *Admin* menu, click on *Commit/Reboot*. The following page is displayed:

Commit/Reboot

This page is used to commit changes to system memory and reboot your system.



- Click on *OK*.



Time Zone	GMT +/- offset	Description	Daylight Saving Start	Daylight Saving End
IDLW	-1200	International Date Line West	Not applicable	Not applicable
NT	-1100	Nome	Not applicable	Not applicable
HST	-1000	Hawaii Standard	Not applicable	Not applicable
AKST	-900	Alaska Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
YST	-900	Yukon Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
PST	-800	US Pacific Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
MST	-700	US Mountain Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
CST	-600	US Central Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
EST	-500	US Eastern Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am

AST	-400	Atlantic Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
NFST	-330	Newfoundland Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
NFT	-330	Newfoundland	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
BRA	-300	Brazil Standard	First Sunday of February at 2:00am	Third Sunday of February at 2:00am
AT	-200	Azores	Not applicable	Not applicable
WAT	-100	West Africa	Last Sunday March at 1:00am	Last Sunday October at 1:00am
GMT	+000	Greenwich Mean	Last Sunday March at 1:00am	Last Sunday October at 1:00am
UTC	+000	Universal (Coordinated)	Last Sunday March at 1:00am	Last Sunday October at 1:00am
WET	+000	Western European	Last Sunday March at 1:00am	Last Sunday October at 1:00am

Time Zone	GMT +/- offset	Description	Daylight Saving Start	Daylight Saving End
CET	+100	Central European	Last Sunday March at 2:00am	Last Sunday October at 2:00am
MET	+100	Middle European	Last Sunday March at 2:00am	Last Sunday October at 2:00am
MEWT	+100	Middle European Winter	Last Sunday March at 2:00am	Last Sunday October at 2:00am
SWT	+100	Swedish Winter	Last Sunday March at 2:00am	Last Sunday October at 2:00am
BST	+100	British Summer	Last Sunday March at 2:00am	Last Sunday October at 2:00am
EET	+200	Eastern Europe, Russia Zone 1	Last Sunday March at 2:00am	Last Sunday October at 2:00am
FST	+200	French Summer	Last Sunday March at 2:00am	Last Sunday October at 2:00am
MEST	+200	Middle European Summer	Last Sunday March at 2:00am	Last Sunday October at 2:00am
SST	+200	Swedish Summer	Last Sunday March at 2:00am	Last Sunday October at 2:00am
IST	+200	Israeli Standard	First Friday April at 2:00am	First Friday September at 2:00am
IDT	+300	Israeli Daylight	1st April at 2:00am	First Friday of September at 2:00am

BT	+300	Baghdad	1st April at 2:00am	1st October at 2:00am
IT	+330	Iran	21st March	23rd September
USZ3	+400	Russian Volga	Last Sunday March at 2:00am	Last Sunday in October at 2:00am
USZ4	+500	Russian Ural	Last Sunday of March at 2:00am	Last Sunday October at 2:00am
INST	+530	Indian Standard	Not applicable	Not applicable
USZ5	+600	Russian West-Siberian	Last Sunday March at 2:00am	Last Sunday October at 2:00am
NST	+630	North Sumatra	Not applicable	Not applicable
WAST	+700	West Australian Standard	Not applicable	Not applicable
USZ6	+700	Russia Yenisei	Last Sunday March at 2:00am	Last Sunday October at 2:00am
JT	+730	Java	Not applicable	Not applicable
CCT	+800	China Coast	Not applicable	Not applicable
ROK	+900	Korean Standard	Not applicable	Not applicable

Time Zone	GMT +/- offset	Description	Daylight Saving Start	Daylight Saving End
KST	+900	Korean Standard	Not applicable	Not applicable
JST	+900	Japan Standard	Not applicable	Not applicable
CAST	+930	Central Australian Standard	Last Sunday October at 2:00am	Last Sunday March at 2:00am
KDT	+1000	Korean Daylight	Not applicable	Not applicable
EAST	+1000	Eastern Australian Standard	Last Sunday October at 2:00am	Last Sunday March at 3:00am
GST	+1000	Guam Standard	Last Sunday March at 2:00am	Last Sunday October at 2:00am
CADT	+1030	Central Australian Daylight	Last Sunday October at 2:00am	Last Sunday March at 3:00am
IDLE	+1200	International Date Line East	Not applicable	Not applicable
NZST	+1200	New Zealand Standard	Last Sunday October at 2:00am	Last Sunday March at 2:00am
NZT	+1200	New Zealand	Last Sunday October at 2:00am	Last Sunday March at 2:00am

Time Zone abbreviations

TR-069 Config

TR-069 is a protocol for communication between a CPE and Auto-Configuration Server (ACS). The CPE TR-069 configuration should be well defined to be able to communicate with the remote ACS.

TR-069 Configuration

- From the left-hand *Admin* menu, click on *TR-069 Config*. The following page is displayed:

TR-069 Configuration

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

TR069:	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled
ACS:		
URL:	<input type="text" value="http://"/>	
User Name:	<input type="text" value="username"/>	
Password:	<input type="text" value="password"/>	
Periodic Inform Enable:	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled
Periodic Inform Interval:	<input type="text" value="300"/>	

Connection Request:		
User Name:	<input type="text"/>	
Password:	<input type="text"/>	
Path:	<input type="text" value="/tr069"/>	
Port:	<input type="text" value="7547"/>	

Certificate Management:		
CPE Certificate Password:	<input type="text" value="client"/>	<input type="button" value="Apply"/> <input type="button" value="Undo"/>
CPE Certificate:	<input type="text"/>	<input type="button" value="Browse..."/> <input type="button" value="Upload"/>
CA Certificate:	<input type="text"/>	<input type="button" value="Browse..."/> <input type="button" value="Upload"/>

TR-069 Configuration page

ACS Field	Description
URL	ACS URL. For example, http://10.0.0.1:80 https://10.0.0.1:443
User Name	The username the DSL device should use when connecting to the ACS.
Password	The password the DSL device should use when connecting to the ACS.
Periodic Inform Enable	When this field is enabled, the DSL device will send an Inform RPC to the ACS server at the system startup, and will continue to send it periodically at an interval defined in Periodic Inform Interval field; When this field is disabled, the DSL device will only send Inform RPC to the ACS server once at the system startup.
Periodic Inform Interval	Time interval in second to send Inform RPC.
Connection Request Field	Description
User Name	The username the remote ACS should use when connecting to this device.
Path	The path of the device ConnectionRequestURL. The device ConnectionRequestURL should be configured based on the Device_IP, Path and Port as follows: http://Device_IP:Port/Path
Port	The port of the device ConnectionRequestURL.

Statistics

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.

Interfaces

- From the left-hand *Statistics* menu, click on *Interfaces*. The following page is displayed:
- To display updated statistics showing any new data since you opened this page, 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	527	0	0	957	0	0
8_35	0	0	0	0	0	0

ADSL

This page shows the ADSL line statistic information.

- From the left-hand *Statistics* menu, click on *ADSL*. The following page is displayed:
- To display updated statistics showing any new data since you opened this page, click *Refresh*.

Statistics -- ADSL Line

Mode	T1.413
Latency	Interleave
Trellis Coding	Enable
Status	SHOWTIME.
Power Level	L0
Uptime	00:00:10

	Downstream	Upstream
SNR Margin (dB)	19.1	6.0
Attenuation (dB)	0.5	0.0
Output Power (dBm)	7.5	10.5
Attainable Rate (Kbps)	11636	1056
Rate (Kbps)	8064	896
K (number of bytes in DMT frame)	253	29
R (number of check bytes in RS code word)	2	16
S (RS code word size in DMT frame)	1.00	4.00
D (interleaver depth)	64	8
Delay (msec)	16.00	8.00
FEC	0	1
CRC	0	0
Total ES	0	0
Total SES	0	11
Total UAS	0	0

Configuring your Computers

This appendix provides instructions for configuring the Internet settings on your computers to work with the Wireless ADSL2+ Router.

Configuring Ethernet PCs

Before you begin

By default, the Wireless ADSL2+ Router automatically assigns the required Internet settings to your PCs. You need to configure the PCs to accept this information when it is assigned.



Note

In some cases, you may want to assign Internet information manually to some or all of your computers rather than allow the Wireless ADSL2+ Router to do so. See Assigning static Internet information to your PCs for instructions.

If you have connected your LAN PCs via Ethernet to the Wireless ADSL2+ Router, follow the instructions that correspond to the operating system installed on your PC:

- Windows® XP PCs
- Windows 2000 PCs
- Windows Me PCs
- Windows 95, 98 PCs
- Windows NT 4.0 workstations

Windows® XP PCs

- In the Windows task bar, click the *Start* button, and then click *Control Panel*.
- Double-click the Network Connections icon.
- In the *LAN or High-Speed Internet* window, right-click on the icon corresponding to your network interface card (NIC) and select *Properties*. (Often, this icon is labeled *Local Area Connection*).
- The *Local Area Connection* dialog box is displayed with a list of currently installed network items.
- Ensure that the check box to the left of the item labeled *Internet Protocol TCP/IP* is checked and click *Properties*.
- In the *Internet Protocol (TCP/IP) Properties* dialog box, click the radio button labeled *Obtain an IP address automatically*. Also click the radio button labeled *Obtain DNS server address automatically*.
- Click *OK* twice to confirm your changes, and then close the Control Panel.

Windows 2000 PCs

- First, check for the IP protocol and, if necessary, install it:
- In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
- Double-click the Network and Dial-up Connections icon.

- In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*.
- The *Local Area Connection Properties* dialog box is displayed with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.
- If Internet Protocol (TCP/IP) does not display as an installed component, click *Install...*
- In the *Select Network Component Type* dialog box, select *Protocol*, and then click *Add...*
- Select *Internet Protocol (TCP/IP)* in the Network Protocols list, and then click *OK*.
- You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
- If prompted, click *OK* to restart your computer with the new settings.
- Next, configure the PCs to accept IP information assigned by the Wireless ADSL2+ Router:
- In the *Control Panel*, double-click the Network and Dial-up Connections icon.
- In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*.
- In the Local Area Connection Properties dialog box, select *Internet Protocol (TCP/IP)*, and then click *Properties*.
- In the *Internet Protocol (TCP/IP) Properties* dialog box, click the radio button labeled *Obtain an IP address automatically*. Also click the radio button labeled *Obtain DNS server address automatically*.
- Click *OK* twice to confirm and save your changes, and then close the Control Panel.

Windows Me PCs

- In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
- Double-click the Network and Dial-up Connections icon.
- In the *Network and Dial-up Connections* window, right-click the Network icon, and then select *Properties*.
- The *Network Properties* dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 11.
- If Internet Protocol (TCP/IP) does not display as an installed component, click *Add...*
- In the *Select Network Component Type* dialog box, select *Protocol*, and then click *Add...*
- Select *Microsoft* in the Manufacturers box.
- Select *Internet Protocol (TCP/IP)* in the Network Protocols list, and then click *OK*.
- You may be prompted to install files from your Windows Me installation CD or

other media. Follow the instructions to install the files.

- If prompted, click *OK* to restart your computer with the new settings.
- Next, configure the PCs to accept IP information assigned by the Wireless ADSL2+ Router:
- In the *Control Panel*, double-click the Network and Dial-up Connections icon.
- In *Network and Dial-up Connections window*, right-click the Network icon, and then select *Properties*.
- In the *Network Properties* dialog box, select *TCP/IP*, and then click *Properties*.
- In the TCP/IP Settings dialog box, click the radio button labeled **Server assigned IP address**. Also click the radio button labeled *Server assigned name server address*.
- Click *OK* twice to confirm and save your changes, and then close the *Control Panel*.
-

Windows 95, 98 PCs

- First, check for the IP protocol and, if necessary, install it:
- In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
- Double-click the Network icon.
- The *Network* dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 9.
- If TCP/IP does not display as an installed component, click *Add...*
- The *Select Network Component Type* dialog box displays.
- Select *Protocol*, and then click *Add...*
- The Select Network Protocol dialog box displays.
- Click on *Microsoft* in the Manufacturers list box, and then click *TCP/IP* in the Network Protocols list box.
- Click *OK* to return to the Network dialog box, and then click *OK* again.
- You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
- Click *OK* to restart the PC and complete the TCP/IP installation.
- Next, configure the PCs to accept IP information assigned by the Wireless ADSL2+ Router:
- Open the Control Panel window, and then click the Network icon.
- Select the network component labeled TCP/IP, and then click *Properties*.
- If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
- In the TCP/IP Properties dialog box, click the IP Address tab.
- Click the radio button labeled *Obtain an IP address automatically*.
- Click the DNS Configuration tab, and then click the radio button labeled *Obtain an IP address automatically*.

- Click *OK* twice to confirm and save your changes.
- You will be prompted to restart Windows.
- Click *Yes*.

Windows NT 4.0 workstations

- First, check for the IP protocol and, if necessary, install it:
- In the Windows NT task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
- In the Control Panel window, double click the Network icon.
- In the *Network dialog* box, click the *Protocols* tab.
- The *Protocols* tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to step 9.
- If TCP/IP does not display as an installed component, click *Add...*
- In the *Select Network Protocol* dialog box, select *TCP/IP*, and then click *OK*.
- You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.
- After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.
- Click *Yes* to continue, and then click *OK* if prompted to restart your computer.
- Next, configure the PCs to accept IP information assigned by the Wireless ADSL2+ Router:
- Open the Control Panel window, and then double-click the Network icon.
- In the *Network* dialog box, click the *Protocols* tab.
- In the *Protocols* tab, select *TCP/IP*, and then click *Properties*.
- In the *Microsoft TCP/IP Properties* dialog box, click the radio button labeled *Obtain an IP address from a DHCP server*.
- Click *OK* twice to confirm and save your changes, and then close the Control Panel.

Assigning static Internet information to your PCs

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

In some cases however, you may want to assign Internet information to some or all of your PCs directly (often called “statically”), rather than allowing the Wireless ADSL2+ Router to assign it. This option may be desirable (but not required) if:

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

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

- The IP address and subnet mask of each PC
- The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the Wireless ADSL2+ Router. By default, the LAN port is assigned the IP address *10.0.0.2*. (You can change this number or another number can be assigned by your ISP. See *Addressing* for more information.)
- The IP address of your ISP's Domain Name System (DNS) server.

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



Note

Your PCs must have IP addresses that place them in the same subnet as the Wireless ADSL2+ Router's LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in *Addressing* to change the LAN port IP address accordingly.

IP Addresses, Network Masks, and Subnets

IP Addresses



Note

This section refers only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.
This section assumes basic knowledge of binary numbers, bits, and bytes.

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

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

Structure of an IP address

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

Similarly, IP addresses contain two kinds of information:

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

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

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

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)

Class B: 129.88.16.49 (network = 129.88, host = 16.49)

Class C: 192.60.201.11 (network = 192.60.201, host = 11)

Network classes

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

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

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

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

Some important notes regarding IP addresses:

- The class can be determined easily from field1:
field1 = 1-126: Class A
field1 = 128-191: Class B
field1 = 192-223: Class C
(field1 values not shown are reserved for special uses)
- A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

Subnet masks



Definition mask

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

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

For example, consider a class C network 10.0.0. To split this into two subnets, you would use the subnet mask:

255.255.255.128

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

11111111. 11111111. 11111111.10000000

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

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

255.255.255.192 or 11111111. 11111111. 11111111.11000000

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



Note

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

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

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

Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the Wireless ADSL2+ Router, and provides instructions for using several IP utilities to diagnose problems.

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

Troubleshooting Suggestions

Problem	Troubleshooting Suggestion
LEDs	
<i>Power LED does not illuminate after product is turned on.</i>	Verify that you are using the power cable provided with the device and that it is securely connected to the Wireless ADSL2+ Router and a wall socket/power strip.
<i>Internet LED does not illuminate after phone cable is attached.</i>	Verify that a standard telephone cable (called an RJ-11 cable) like the one provided is securely connected to the DSL port and your wall phone port. Allow about 30 seconds for the device to negotiate a connection with your ISP.
<i>LINK LAN LED does not illuminate after Ethernet cable is attached.</i>	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the Wireless ADSL2+ Router. Make sure the PC and/or hub is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled CAT 5. A 10Mbit/sec network may tolerate lower quality cables.
Internet Access	
<i>My PC cannot access the Internet</i>	Use the ping utility (discussed in the following section) to check whether your PC can communicate with the device's LAN IP address (by default 10.0.0.2). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: Check that the gateway IP address on the computer is your public IP address (see Current Status for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically. Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically.
<i>My LAN PCs cannot display web pages on the Internet.</i>	Verify that the DNS server IP address specified on the PCs is correct for your ISP, as discussed in the item above. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the Wireless ADSL2+ Router is correct, then You can use the ping utility, to test connectivity with your ISP's DNS server.
Web pages	

Problem	Troubleshooting Suggestion
<i>I forgot/lost my user ID or password.</i>	If you have not changed the password from the default, try using “admin” the user ID and “administrator” as password. Otherwise, you can reset the device to the default configuration by pressing the Reset Default button on the Rare panel of the device (see <i>Rare Panel</i>). Then, type the default User ID and password shown above. WARNING: Resetting the device removes any custom settings and returns all settings to their default values.
<i>I cannot access the web pages from my browser.</i>	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the device’s LAN IP address (by default 10.0.0.2). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer or Netscape Navigator v4.0 or later. Verify that the PC’s IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the Wireless ADSL2+ Router.
My changes to the web pages are not being retained.	Be sure to use the <i>Confirm Changes/Apply</i> function after any changes.

Diagnosing Problem using IP Utilities

ping

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

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

ping 10.0.0.2

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

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

```

C:\> Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\G-MAX>ping 192.168.1.1

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128

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

C:\Documents and Settings\G-MAX>

```

Using the ping Utility

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

Using the ping command, you can test whether the path to the Wireless ADSL2+ Router is working (using the preconfigured default LAN IP address 10.0.0.2) or another address you assigned.

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

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

nslookup

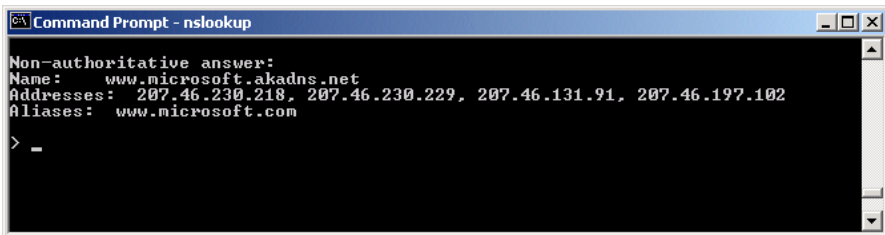
You can use the *nslookup* command to determine the IP address associated with an Internet site name. You specify the common name, and the *nslookup* command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then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

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

Nslookup

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

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



```

C:\> nslookup
Non-authoritative answer:
Name:   www.microsoft.akadns.net
Addresses: 207.46.230.218, 207.46.230.229, 207.46.131.91, 207.46.197.102
Aliases: www.microsoft.com

> -

```

Using the nslookup Utility

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

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

Glossary

- 10BASE-T** A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See *data rate*, *Ethernet*.
- 100BASE-T** A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See *data rate*, *Ethernet*.
- ADSL** Asymmetric Digital Subscriber Line
The most commonly deployed “flavor” of DSL for home users is asymmetrical DSL. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.
- analog** An analog signal is a signal that has had its frequency modified in some way, such as by amplifying its strength or varying its frequency, in order to add information to the signal. The voice component in DSL is an analog signal. See *digital*.
- ATM** Asynchronous Transfer Mode
A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. See *data rate*.

authenticate	To verify a user's identity, such as by prompting for a password.
binary	The "base two" system of numbers, that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See <i>bit</i> , <i>IP address</i> , <i>network mask</i> .
bit	Short for "binary digit," a bit is a number that can have two values, 0 or 1. See <i>binary</i> .
bps	bits per second
bridging	Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing, which can add more intelligence to data transfers by using network addresses instead. The Wireless ADSL2+ Router can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See <i>routing</i> .
broadband	A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.
broadcast	To send data to all computers on a network.
DHCP	Dynamic Host Configuration Protocol DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.
DHCP relay	Dynamic Host Configuration Protocol relay A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the Wireless ADSL2+ Router's interfaces can be configured as a DHCP relay. See <i>DHCP</i> .

DHCP server	Dynamic Host Configuration Protocol server A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See <i>DHCP</i> .
digital	Of data, having a form based on discrete values expressed as binary numbers (0's and 1's). The data component in DSL is a digital signal. See <i>analog</i> .
DNS	Domain Name System The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, <i>www.yahoo.com</i> is the domain name associated with IP address 216.115.108.243. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See <i>domain name</i> .
domain name	A domain name is a user-friendly name used in place of its associated IP address. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site. See <i>DNS</i> .
download	To transfer data in the downstream direction, i.e., from the Internet to the user.
DSL	Digital Subscriber Line A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.
encryption keys	See <i>network keys</i>
Ethernet	The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also <i>10BASE-T</i> , <i>100BASE-T</i> , <i>twisted pair</i> .

FTP	<p>File Transfer Protocol</p> <p>A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.</p>
Gbps	<p>Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.</p>
host	<p>A device (usually a computer) connected to a network.</p>
HTTP	<p>Hyper-Text Transfer Protocol</p> <p>HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See <i>web browser</i>, <i>web site</i>.</p>
Hub	<p>A hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more directions. It connects an Ethernet bridge/Router to a group of PCs on a LAN and allows communication to pass between the networked devices.</p>
ICMP	<p>Internet Control Message Protocol</p> <p>An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.</p>
IEEE	<p>The Institute of Electrical and Electronics Engineers is a technical professional society that fosters the development of standards that often become national and international standards.</p>
Internet	<p>The global collection of interconnected networks used for both private and business communications.</p>
intranet	<p>A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.</p>
IP	<p>See <i>TCP/IP</i>.</p>

IP address	<p>Internet Protocol address</p> <p>The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a <i>network ID</i> that identifies the particular network the host belongs to, and a <i>host ID</i> uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See <i>domain name</i>, <i>network mask</i>.</p>
ISP	<p>Internet Service Provider</p> <p>A company that provides Internet access to its customers, usually for a fee.</p>
LAN	<p>Local Area Network</p> <p>A network limited to a small geographic area, such as a home or small office.</p>
LED	<p>Light Emitting Diode</p> <p>An electronic light-emitting device. The indicator lights on the front of the Wireless ADSL2+ Router are LEDs.</p>
MAC address	<p>Media Access Control address</p> <p>The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of hex characters, with each pair separated by colons. For example; <i>NN:NN:NN:NN:NN:NN</i>.</p>
mask	<p>See <i>network mask</i>.</p>
Mbps	<p>Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.</p>
NAT	<p>Network Address Translation</p> <p>A service performed by many Routers that translates your network's publicly known IP address into a <i>private</i> IP address for each computer on your LAN. Only your Router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.</p>

network	A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a LAN, or very large, such as the <i>Internet</i> .
network mask	A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean “select this bit” while bits set to 0 mean “ignore this bit.” For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See <i>binary, IP address, subnet</i> .
NIC	Network Interface Card An adapter card that plugs into your computer and provides the physical interface to your network cabling. For Ethernet NICs this is typically an RJ-45 connector. See <i>Ethernet, RJ-45</i> .
packet	Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).
ping	Packet Internet (or Inter-Network) Groper A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.
port	A physical access point to a device such as a computer or Router, through which data flows into and out of the device.
PPP	Point-to-Point Protocol A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the Wireless ADSL2+ Router uses two forms of PPP called PPPoA and PPPoE. See <i>PPPoA, PPPoE</i> .
PPPoA	Point-to-Point Protocol over ATM One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.

PPPoE	Point-to-Point Protocol over Ethernet One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.
protocol	A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.
remote	In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.
RIP	Routing Information Protocol The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.
RJ-11	Registered Jack Standard-11 The standard plug used to connect telephones, fax machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.
RJ-45	Registered Jack Standard-45 The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.
routing	Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a Router.
SDNS	Secondary Domain Name System (server) A DNS server that can be used if the primary DSN server is not available. See <i>DNS</i> .
subnet	A subnet is a portion of a network. The subnet is distinguished from the larger network by a <i>subnet mask</i> that selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See <i>network mask</i> .
subnet mask	A mask that defines a subnet. See <i>network mask</i> .

TCP	See <i>TCP/IP</i> .
TCP/IP	<p>Transmission Control Protocol/Internet Protocol</p> <p>The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.</p>
Telnet	<p>An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.</p>
TFTP	<p>Trivial File Transfer Protocol</p> <p>A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.</p>
TKIP	<p>Temporal Key Integrity Protocol (TKIP) provides WPA with a data encryption function. It ensures that a unique master key is generated for each packet, supports message integrity and sequencing rules and supports re-keying mechanisms.</p>
triggers	<p>Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, open secondary connections during normal operations, for example, a connection to a server is established using one port, but data transfers are performed on a separate connection. A trigger tells the device to expect these secondary sessions and how to handle them.</p> <p>Once you set a trigger, the embedded IP address of each incoming packet is replaced by the correct host address so that NAT can translate packets to the correct destination. You can specify whether you want to carry out address replacement, and if so, whether to replace addresses on TCP packets only, UDP packets only, or both.</p>

twisted pair	<p>The ordinary copper telephone wiring used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See <i>10BASE-T</i>, <i>100BASE-T</i>, <i>Ethernet</i>.</p>
unnumbered interfaces	<p>An unnumbered interface is an IP interface that does not have a local subnet associated with it. Instead, it uses a <i>Router-id</i> that serves as the source and destination address of packets sent to and from the Router. Unlike the IP address of a normal interface, the Router-id of an unnumbered interface is allowed to be the same as the IP address of another interface. For example, the WAN unnumbered interface of your device uses the same IP address of the LAN interface (10.0.0.2). The unnumbered interface is temporary – PPP or DHCP will assign a ‘real’ IP address automatically.</p>
upstream	<p>The direction of data transmission from the user to the Internet.</p>
VC	<p>Virtual Circuit A connection from your DSL Router to your ISP.</p>
VCI	<p>Virtual Circuit Identifier Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. See <i>VC</i>.</p>
VPI	<p>Virtual Path Identifier Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. See <i>VC</i>.</p>
WAN	<p>Wide Area Network Any network spread over a large geographical area, such as a country or continent. With respect to the Wireless ADSL2+ Router, WAN refers to the Internet.</p>

- Web browser** A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See *HTTP, web site, WWW*.
- Web page** A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the *home page*. See *hyperlink, web site*.
- Web site** A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See *hyperlink, web page*.
- WWW** World Wide Web
Also called *(the) Web*. Collective term for all web sites anywhere in the world that can be accessed via the Internet.

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

Copyright© 2010. MODECOM S.A. All rights reserved.
MODECOM Logo is a registered trademark of MODECOM S.A.

MODECOM