



# **802.11n Wireless ADSL 2/2+ Router**

**ADN-4000**

---

## **User's Manual**

---

## **Copyright**

Copyright© 2009 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

## **Federal Communication Commission Interference Statement**

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

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

## **FCC Caution**

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

### **Federal Communication Commission (FCC) Radiation Exposure Statement**

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

### **R&TTE Compliance Statement**

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

### **WEEE Regulation**



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

### **Safety**

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

### **Revision**

User's Manual for 802.11n Wireless ADSL 2/2+ Router

Model: ADN-4000v2

Rev: 1.0 (Aug. 2009)

Part No. EM-ADN4000v2\_v1

# Table of Contents

1. INTRODUCTION .....	7
1.1 Feature .....	8
1.2 Package Contents.....	10
1.3 Physical Details.....	10
2. INSTALLATION.....	13
2.1 Choosing the Best Location for Wireless Operation.....	13
2.2 Connecting the ADSL Router.....	13
2.3 Configuring the Network Properties .....	14
3. WEB CONFIGURATION MANAGEMENT .....	18
3.1 Quick Setup .....	19
3.1.1 WAN Interface Setup .....	19
<b>3.1.1.1 Setup VPI/VCI</b> .....	19
<b>3.1.1.2 Select Protocol and Connection</b> .....	20
<b>3.1.1.3 Internet Connection Type - PPP over Ethernet (PPPoE)</b> .....	21
<b>3.1.1.4 Internet Connection Type - PPP over ATM (PPPoA)</b> .....	22
<b>3.1.1.5 Internet Connection Type - Dynamic IP</b> .....	23
<b>3.1.1.6 Internet Connection Type - Static IP</b> .....	24
<b>3.1.1.7 Internet Connection Type - IP over ATM (IPoA)</b> .....	25
<b>3.1.1.8 Internet Connection Type - Bridge</b> .....	26
3.1.2 LAN Interface Setup.....	27
3.1.3 WAN Setup Summary .....	28
3.1.4 Quick Setup Completed.....	29
3.2 DSL Router Device information.....	30
3.2.1 Summary of Device information .....	30
3.2.2 WAN Interface information.....	31
3.2.3 Statistics.....	32
<b>3.2.3.1 Statistics of LAN</b> .....	32
<b>3.2.3.2 Statistics of WAN Service</b> .....	33
<b>3.2.3.3 Statistics of xTM</b> .....	34
<b>3.2.3.4 Statistics of xDSL</b> .....	35
3.2.4 Route table information.....	37
3.2.5 ARP table information.....	38
3.2.6 DHCP IP Leases information .....	38

3.3 Advanced Setup.....	39
3.3.1 Layer2 INTERFACE.....	39
3.3.1.1 ATM Interface.....	39
3.3.1.2 ETH Interface.....	41
3.3.2 WAN CONFIGURATION.....	41
<b>3.3.2.1 Add PPPoE WAN configuration</b> .....	42
<b>3.3.1.2 Add MER (IPoE) Configuration</b> .....	45
<b>3.3.1.3 Add PPPoA Configuration</b> .....	48
<b>3.3.1.4 Add IPoA Configuration</b> .....	51
<b>3.3.1.5 Add Bridge Configuration</b> .....	54
3.3.3 LAN configuration .....	56
3.3.4 NAT-- Network Address Translation .....	57
<b>3.3.4.1 DMZ Host</b> .....	59
<b>3.3.4.2 Port Triggering</b> .....	61
<b>3.3.4.3 NAT -- Virtual Servers Setup</b> .....	62
3.3.5 Security .....	65
<b>3.3.5.1 Outgoing IP Filtering Setup</b> .....	66
<b>3.3.5.2 Incoming IP Filtering Setup</b> .....	69
<b>3.3.5.3 MAC Filtering Setup</b> .....	72
3.3.6 Quality of Service .....	74
<b>3.3.6.1 Enable QoS</b> .....	74
<b>3.3.6.2 QoS--Queue Config</b> .....	76
<b>3.3.6.3 QoS -- QoS Classification</b> .....	78
3.3.7 Routing .....	80
<b>3.3.7.1 Routing – Default Gateway</b> .....	80
<b>3.3.7.2 Static Routes</b> .....	81
<b>3.3.7.3 RIP</b> .....	82
3.3.8 DNS .....	84
<b>3.3.8.1 DNS Server</b> .....	84
<b>3.3.8.2 Dynamic DOMAIN NAME SERVICE (DDNS)</b> .....	86
3.3.9 DSL.....	88
3.3.10 Interface Grouping.....	89
3.3.11 Certificate .....	90
<b>3.3.11.1 Create New Local Certificate</b> .....	90

<b>3.3.11.2 Import Existing Local Certificate</b> .....	92
<b>3.3.11.3 Trusted CA Certificates</b> .....	93
<b>3.4 Wireless</b> .....	<b>94</b>
3.4.1 Wireless – Basic .....	94
3.4.2 Wireless – Security .....	95
3.4.3 Wireless – Advanced .....	96
<b>3.5 Diagnostics</b> .....	<b>98</b>
<b>3.6 Management</b> .....	<b>99</b>
3.6.1 Settings .....	99
<b>3.6.1.1 Settings Backup</b> .....	<b>99</b>
<b>3.6.1.2 Settings Update</b> .....	<b>99</b>
<b>3.6.1.3 Settings Restore Default</b> .....	<b>99</b>
3.6.2 System Log .....	100
3.6.3 SNMP Client.....	103
<b>3.6.3.1 Configure</b> .....	<b>105</b>
3.6.4 TR-69 Client Management .....	106
3.6.5 Internet Time .....	107
3.6.6 Access Control.....	108
<b>3.6.6.1 Access Control – Services</b> .....	<b>108</b>
<b>3.6.6.2 Access Control -- IP Addresses</b> .....	<b>108</b>
<b>3.6.6.3 Access Control – Passwords</b> .....	<b>109</b>
3.6.7 Update Software .....	110
3.6.8 Save/Reboot.....	110
<b>APPENDIX A: GLOSSARY</b> .....	<b>111</b>

# 1. Introduction

The PLANET 802.11n Wireless ADSL 2/2+ Router with 2T2R MIMO antenna technology, ADN-4000, provides office and residential users the ideal solution for sharing a high-speed ADSL 2/2+ broadband Internet connection and four-10/100Mbps Fast Ethernet backbone. It can support downstream transmission rates of up to 24Mbps and upstream transmission rates of up to 3.5Mbps. The product supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 2684 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1483) to establish a connection with ISP.

With built-in IEEE 802.11b/g/n Draft 2.0 wireless network capability, all computers and wireless-enabled network devices can connect to the ADN-4000 without additional cabling. New 802.11n Draft 2.0 wireless capability also gives you the highest speed of wireless experience ever. With a compatible wireless card installed in your PC, you can transfer file up to 300Mbps (transfer data rate). The radio coverage is also doubled, so you don't need to worry if the size of your office or house is big.

To secure the wireless communication, the ADN-4000 supports most up-to-date encryption, WEP, and WPA-PSK/ WPA2-PSK. In order to simplify the security settings, ADN-4000 supports WPS configuration with PBC/PIN type. Your whole wireless network can be secured.

Via the user-friendly management interface, ADN-4000 can be managed by workstations running standard web browsers. Furthermore, ADN-4000 provides DHCP server, NAT, Virtual Server, DMZ, Access Control, IP Filter, PPTP/IPSec/L2TP pass-through, DDNS, and UPnP capability.

The ADN-4000 also serves as an Internet firewall, protecting your network from being accessed by outside users. It provides the natural firewall function (Network Address Translation, NAT). All incoming and outgoing IPs are monitored and filtered. Moreover, it can be configured to block internal users from accessing to the Internet.

## 1.1 Feature

### Internet Access Features

- ♦ **Shared Internet Access** All users on the LAN can access the Internet through the ADN-4000 using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- ♦ **Built-in ADSL 2/2+ Modem** The ADN-4000 provides ADSL 2/2+ modem, and supports all common ADSL connections.
- ♦ **PPPoE, PPPoA, Direct Connection Support** Various WAN connections are supported by ADN-4000.
- ♦ **Fixed or Dynamic IP Address** On the Internet (WAN port) connection, the ADN-4000 supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

### Advanced Internet Functions

- ♦ **Virtual Servers** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ♦ **DMZ Support** The ADN-4000 can translate public IP addresses to private IP address to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the most flexibility to run programs, which could be incompatible in NAT environment.
- ♦ **Firewall** Supports simple firewall with NAT technology and provides option for access control from Internet, like Telnet, FTP, TFTP, HTTP, SNMP, and ICMP services. It also supports IP/MAC /Application/URL filtering.
- ♦ **Universal Plug and Play (UPnP)** UPnP allows automatic discovery and configuration of the Broadband Router. UPnP is supported by Windows ME, XP, or later.
- ♦ **Dynamic DNS Support** When used with the Virtual Servers feature, the ADN-4000 allows users to connect to Servers on your LAN using a Domain Name, even if you have a dynamic IP address which changes every time you connect.
- ♦ **VPN Pass through Support** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP, and IPsec are transparently supported - no configuration is required.
- ♦ **RIP Routing** It supports RIPv1/2 routing protocol for routing capability.
- ♦ **Simple Network Management Protocol (SNMP)** It is an easy way to remotely manage the router via SNMP.



## LAN Features

- ♦ **4-Port Switch** The ADN-4000 incorporates a 4-Port 10/100Base-TX switching hub, making it easy to create or extend your LAN.
- ♦ **DHCP Server Support** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The ADN-4000 can act as a DHCP Server for devices on your local LAN and WLAN.

## Wireless Features

- ♦ **Standards Compliant** The ADN-4000 complies with IEEE 802.11n (Draft 2.0) wireless technology capable of up to 300Mbps data rate.
- ♦ **Two Dipped Antennas with MIMO Technology** The ADN-4000 provides farther coverage, less dead spaces and higher throughput with 2T2R MIMO technology.
- ♦ **Support IEEE 802.11b, g and 802.11n Draft 2.0 Wireless Station** The 802.11n standard provides for backward compatibility with the 802.11b and 802.11g standard, so 802.11b, 802.11g, and 802.11n Draft 2.0 can be used simultaneously.
- ♦ **WEP Support** WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported.
- ♦ **WPS Push Button Control** The ADN-4000 supports WPS (Wi-Fi Protected Setup) to easy connect wireless network without configuring the security.
- ♦ **WPA-PSK Support** WPA-PSK\_TKIP and WAP-PSK\_AES encryption are supported.
- ♦ **Wireless MAC Access Control** The Wireless Access Control feature can check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.

## 1.2 Package Contents

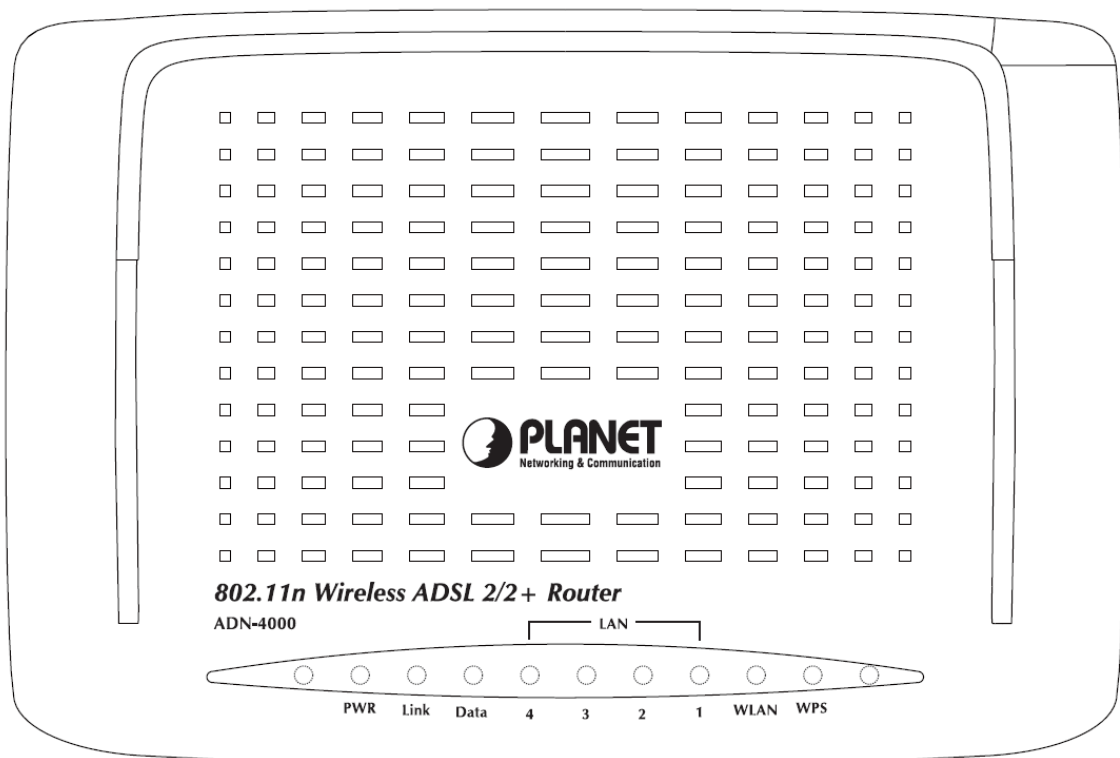
The following items should be included:

- ADN-4000 Unit x 1
- Quick Installation Guide x 1
- User's Manual CD x 1
- Power Adapter x 1
- RJ-45 Cable x 1
- RJ-11 Cable x 2
- ADSL Splitter x 1

If any of the above items are damaged or missing, please contact your dealer immediately.

## 1.3 Physical Details

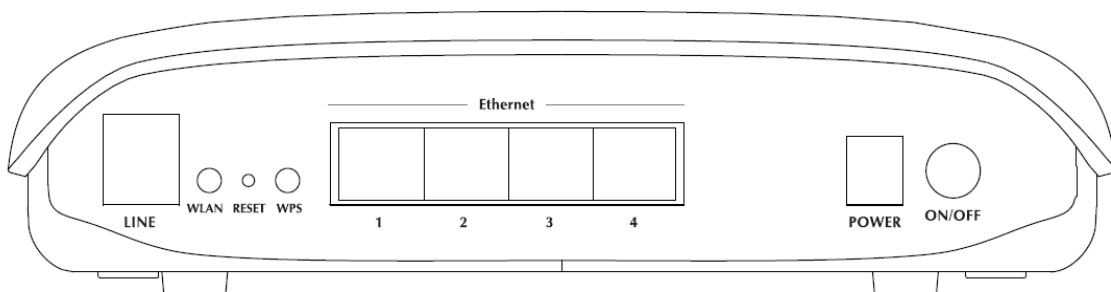
### Front Panel



## LED definition

LED	State	Description
<b>PWR</b>	Off	The power is off.
	Green	The power is on and operating normally.
	Red	The power is self-testing.
		The device enters the console mode of the boot loader.
		The self-testing fails if the LED is always RED.
Blink Red	Upgrading software.	
<b>Link</b>	Off	No signal is detected.
	Blink Green	The DSL line is training.
	Green	The DSL line connection is established.
<b>Data</b>	Off	No Internet connection.
	Green	The users can access the Internet.
	Red	Device attempts to become IP connected but fails.
<b>LAN 1-4</b>	Off	No Ethernet signal is detected.
	Green	Ethernet interface is ready to work.
	Blink Green	Data is passing through Ethernet port.
<b>WLAN</b>	Off	No radio signal is detected.
	Green	WLAN interface is ready to work
	Blink Green	Data is passing through wireless.
<b>WPS</b>	Off	WPS service is not during using, or WPS is setup successfully.
	Blink Green	WPS service tries to establish.

## Rear Panel



## Rear Panel Port and Button Definition

Connector	Description
<b>LINE</b>	The RJ-11 allows data communication between the modem and the ADSL network through a twisted-pair phone wire.
<b>WLAN</b>	The WLAN button can enable and disable the wireless function.
<b>RESET</b>	To restore the factory default settings of device. Keep the device powered on and push a paper clip into the hole. Press down the button over 5 seconds and then release.
<b>WPS</b>	Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and this ADSL router. Press this button on the router and enable WPS function of the wireless clients, the router and clients will automatically configure the security key and connect directly. Please note that the router will wait for WPS requests from wireless clients in 2 minutes after the WPS button is pressed.
<b>LAN 1~4</b>	The RJ-45 allows PC or network devices to connect by network cable.
<b>POWER</b>	The Power connector with 12V DC, 1A
<b>ON/OFF</b>	The Power Button uses for turning on or off the device.

## 2. Installation

This chapter offers information about installing your router. If you are not familiar with the hardware or software parameters presented here, please consult your service provider for the values needed.

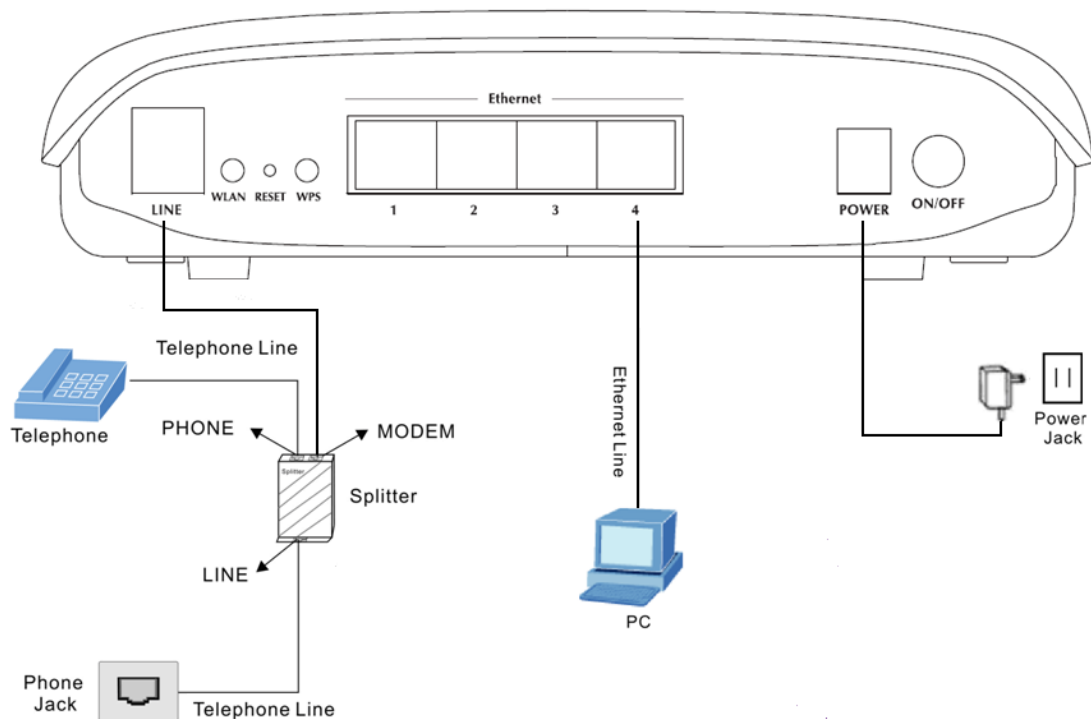
### 2.1 Choosing the Best Location for Wireless Operation

- Keep the numbers of walls and ceilings to the minimum:  
The signal emitted from wireless LAN devices can penetrate through ceilings and walls. However, each wall or ceiling can reduce the range of wireless LAN devices from 1 ~ 30 meters. Position your wireless devices so that the number of walls or ceilings obstructing the signal path is minimized.
- Consider the direct line between access points and workstations:  
A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it appears over 14 meters thick. Be careful to position access points and client adapters so the signal can travel straight through (90° angle) a wall or ceiling for better reception.
- Building materials make difference:  
Buildings constructed using metal framing or doors can reduce effective range of the device. If possible, position wireless devices so that their signals can pass through drywall or open doorways. Avoid positioning them in the way that their signal must pass through metallic materials. Poured concrete walls are reinforced with steel while cinderblock walls generally have little or no structural steel.
- Position the antenna for best reception:  
Play around with the antenna position to see if signal strength improves. Some adapters or access points allow you to judge the strength of the signal.
- Keep your product away (at least 1~2 meters) from electrical devices:
- Keep wireless devices away from electrical devices that generate RF noise such as microwave ovens, monitors, electric motors, etc.

### 2.2 Connecting the ADSL Router

- See the following figure. Connect the DSL port of the DSL Router with a telephone cable.
- Connect the Ethernet port of the DSL Router to the network card of the PC via an Ethernet cable.
- Plug one end of the power adapter to the wall outlet and connect the other end to the PWR port of the DSL Router.

The following figure displays the connection of the DSL Router, PC, and telephones.



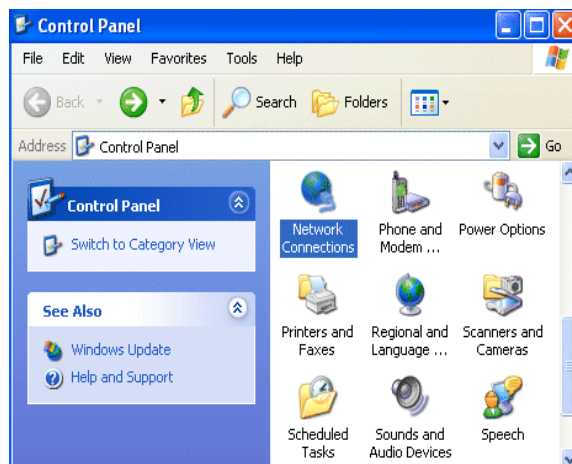
If do not need to connect to the splitter,

- Connect the modem to wall jack with a telephone cable directly.
- Use Ethernet cable to connect “LAN” port of the modem and network adaptor of your computer.

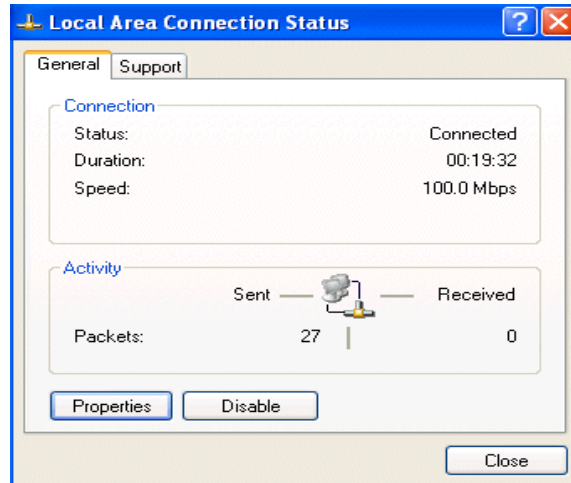
## 2.3 Configuring the Network Properties

### Configuring PC in Windows XP

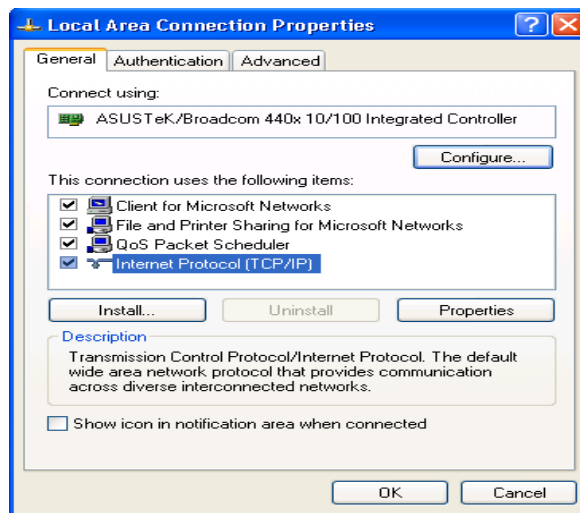
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window, click **Properties**.

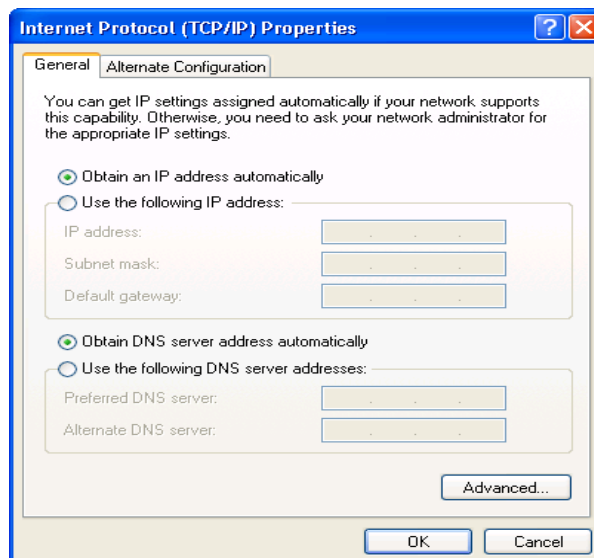


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



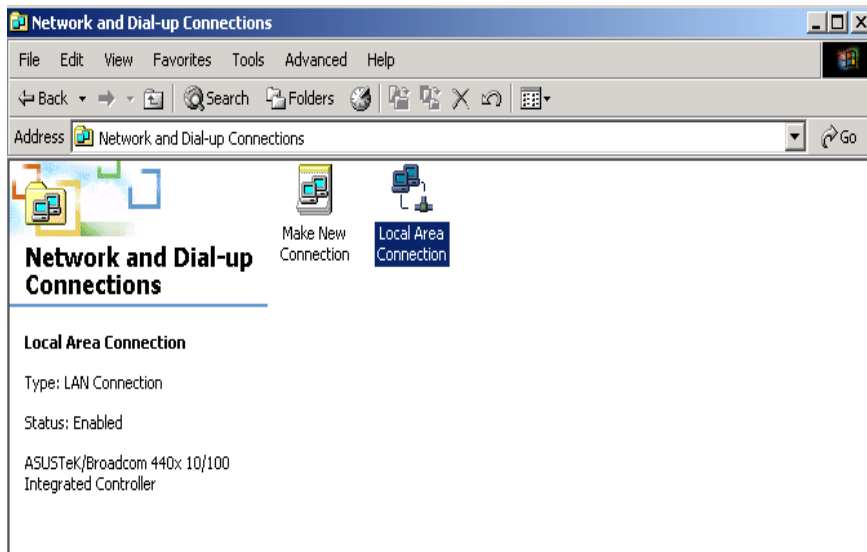
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.

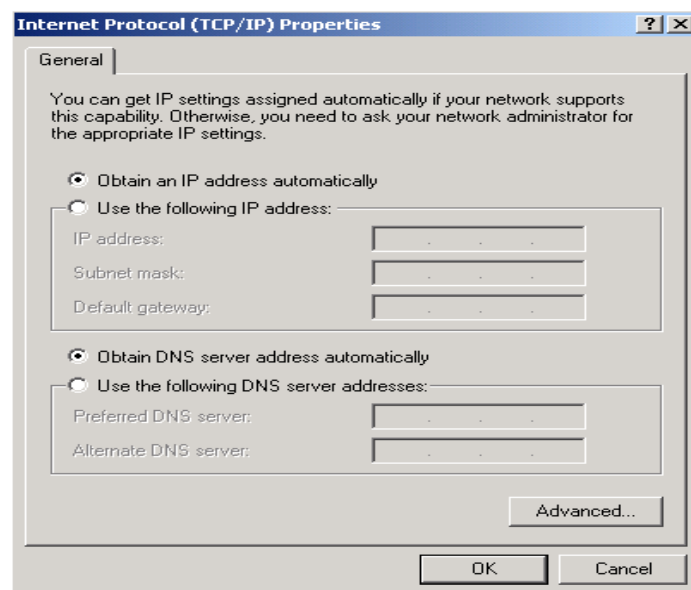


## Configuring PC in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **Local Area Connection**.



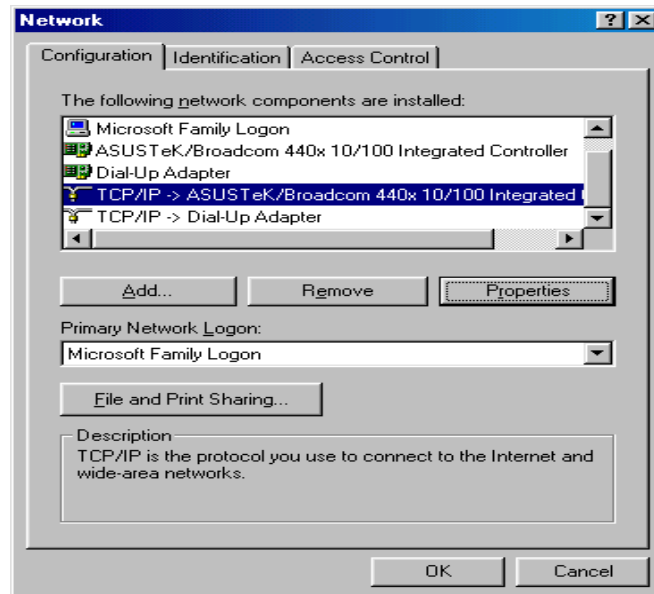
3. In the **Local Area Connection Status** window click **Properties**.
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.



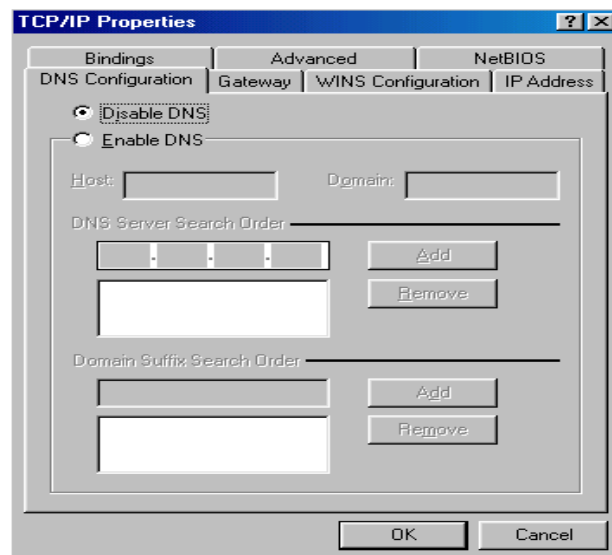


## Configuring PC in Windows 98/Me

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP/IP** → the name of your Network Interface Card (NIC) in your PC.



3. Select the **Obtain an IP address automatically** radio button.
4. Then select the **DNS Configuration** tab.
5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



# 3. Web Configuration Management

## Determine your connection settings

Before you configure the router, you need to know the connection information supplied by your ADSL service provider.

### Connecting the ADSL Router to your network

Unlike a simple hub or switch, the setup of the ADSL Router consists of more than simply plugging everything together. Because the Router acts as a DHCP server, you will have to set some values within the Router, and also configure your networked PCs to accept the IP Addresses the Router chooses to assign them.

Generally there are several different operating modes for your applications. And you can know which mode is necessary for your system from ISP. These modes are router, bridge, PPPoE+NAT, and PPPoA+NAT.

### Configuring with Web Browser

It is advisable to change the administrator password to safeguard the security of your network.

To configure the router, open your browser, type “**http: //192.168.1.1**” into the address bar and click “**Go**” to get to the login page.

Save this address in your Favorites for future reference.



In login dialog, enter “**admin**” as user name and “**admin**” as default password. After log in, you will see the following page. The default screen is **Quick Setup** setting screen. You can configure the device step by step.



## 3.1 Quick Setup

When we enter into Quick Setup page, it mainly includes functions to do.

- **Account setup**
- **Time Server setup**
- **WAN setup**
- **Wireless setup**

'**Quick Setup**' enables speedy and accurate configuration of your Internet connection and other important parameters. The following sections describe these various configuration parameters. Whether you configure these parameters or use the default ones, click '**Next**' to enable your Internet connection.

When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Your physical WAN device can be either Ethernet, DSL, or both. Technical information regarding the properties of your Internet connection should be provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or what protocols, such as PPPOA or PPPoE, you will be using to communicate over the Internet.

**Welcome to use Quick setup wizard !**

Quick setup wizard will guide you to finish route configuration.

Next

### 3.1.1 WAN Interface Setup

In WAN Interface Setup phase, we mainly setup PVC and the property of this PVC:

- **VPI**
- **VCI**
- **Protocol**
- **Connection Mode**

#### 3.1.1.1 Setup VPI/VCI

After logging into the DSL router, When we were not config any PVC at previous time and we have not default settings include PVC, you will see a "**Quick Setup**" web page, which will include some basic configuration that is needed by ATM PVC. the following introductions will guide you through the steps necessary to configure your DSL Router.

According to your Internet service providers (ISP) instructions, specify the following parameters:

■ **VPI (Virtual Path Identifier):**

The virtual path between two points in an ATM network and its valid value is from 0 to 255.

■ **VCI (Virtual Channel Identifier):**

The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

### 3.1.1.2 Select Protocol and Connection

You can select your protocol from the following list; each protocol has its connection mode:

- **PPPoE (PPP over Ethernet)**
- **PPPoA (PPP over ATM)**
- **Dynamic**
- **Static IP**
- **IPoA (IP over ATM)**
- **Bridging**

#### WAN Service Setting

VPI :  (0-255)  
VCI :  (32-65535)  
Protocol :    
Connection mode :

Figure: WAN Service page

For example, Change the connection type of PVC 0/35 to “**bridge**”. Select “**bridging**”, and “**LLC**” (depending on the uplink equipment, generally “LLC”) as “**Connect Mode**”.

### 3.1.1.3 Internet Connection Type - PPP over Ethernet (PPPoE)

- A. Setup the PVC.
- B. Select PPP over Ethernet (PPPoE) from the “Protocol” box and its Connection mode.
- C. Enter PPP information.

**WAN Service Setting**

VPI :  (0-255)  
VCI :  (32-65535)  
Protocol :   
Connection mode :

PPPoE  
Please input the ISP provided user name and password, pay attention to case-sensitive.

User name :   
Password :   
Confirm password :

**Figure: PPP over Ethernet (PPPoE)**

Your Internet Service Provider (ISP) should provide you with the following information:

- PPP Username
- PPP Password
- Authentication Method

### 3.1.1.4 Internet Connection Type - PPP over ATM (PPPoA)

- A. Setup the PVC.
- B. Select PPP over ATM (PPPoA) from the "Protocol" box and Its connection mode.
- C. Enter PPP information.

#### WAN Service Setting

VPI :  (0-255)  
VCI :  (32-65535)  
Protocol :    
Connection mode :

PPPoA  
Please input the ISP provided user name and password, pay attention to case-sensitive.

User name :   
Password :   
Confirm password :

**Figure: PPP over ATM (PPPoA)**

Your Internet Service Provider (ISP) should provide you with the following information:

- PPP Username
- PPP Password
- Authentication Method

### 3.1.1.5 Internet Connection Type - Dynamic IP

- A. Setup the PVC
- B. Select Dynamic IP from the "Protocol" box and its connection type.

#### WAN Service Setting



VPI :  (0-255)  
VCI :  (32-65535)  
Protocol :    
Connection mode :

Figure: Dynamic IP

### 3.1.1.6 Internet Connection Type - Static IP

- A. Setup the PVC.
- B. Select Static IP from the "Protocol" box and its connection mode.
- C. Enter the IP information.

**WAN Service Setting**

VPI :  (0-255)  
VCI :  (32-65535)  
Protocol :    
Connection mode :  

Static IP  
Please enter the following information provided by ISP:

WAN IP Address :   
SubnetMask :   
Default gateway :   
Primary DNS server :   
Secondary DNS server :

**Figure: Static IP**

Your Internet Service Provider (ISP) should provide you with the following

- WAN IP address and Subnet Mask information
- Default gateway information
- DNS server information



### 3.1.1.7 Internet Connection Type - IP over ATM (IPoA)

- A. Setup the PVC.
- B. Select IP over ATM (IPoA) from the "Protocol" box and its connection mode.

**WAN Service Setting**

VPI :  (0-255)  
VCI :  (32-65535)  
Protocol :    
Connection mode :

IPoA  
Please enter the following information provided by ISP:

WAN IP Address :   
SubnetMask :   
Default gateway :   
Primary DNS server :   
Secondary DNS server :

**Figure: IP over ATM (IPoA)**

Your Internet Service Provider (ISP) should provide you with the following.

- WAN IP address and Subnet Mask information
- Default gateway information
- DNS server information

### 3.1.1.8 Internet Connection Type - Bridge

- A. Setup the PVC.
- B. Select Bridge from the "Protocol" box and its connection mode.

#### WAN Service Setting



VPI :  (0-255)  
VCI :  (32-65535)  
Protocol :    
Connection mode :  

Figure: Bridge

### 3.1.2 LAN Interface Setup

In LAN interface setup page, you can modify your default LAN IP and DHCP Server settings. The Default LAN IP is **192.168.1.1** and DHCP is **Enable**.

The screenshot shows the 'LAN Interface Setup' page. On the left is a blue sidebar with menu items: Device Info, Quick Setup, Advanced Setup, Diagnostics, and Management. The main area is titled 'Device Setup' and includes the instruction: 'Configure the DSL Router IP Address and Subnet Mask for LAN interface.' Below this are input fields for 'IP Address' (192.168.1.1) and 'Subnet Mask' (255.255.255.0). There are two radio buttons for DHCP: 'Disable DHCP Server' and 'Enable DHCP Server' (which is selected). Further down are fields for 'Start IP Address' (192.168.1.2), 'End IP Address' (192.168.1.254), 'Subnet Mask' (255.255.255.0), and 'Leased Time (hour):' (24). At the bottom, there is an unchecked checkbox for 'Configure the second IP Address and Subnet Mask for LAN interface'.

Figure: LAN Interface Setup

#### Configuring the DHCP server

The Router has a DHCP server for which the factory setting is active. Consequently, the IP addresses of the PCs are automatically assigned by the DSL Router.

#### Note:

- ◆ If the DHCP server for the DSL Router is activated, you can configure the network setting on the PC so that the option Obtain an IP address automatically is set up. Further information about this can be found in the section entitled
- ◆ If you deactivate the DHCP server, you will have to assign a static IP address for the PCs that use the network settings
- To activate the DHCP server, select 'Enable'.
- If the DHCP server is active, you can define a Lease time. The Lease time determines the period for which the PCs retain the IP addresses assigned to them without changing them.

#### Note:

If you select Never expires, the IP addresses are never changed. Activate this option if you want to make NAT or firewall settings using the IP addresses of the PCs; otherwise you have to assign static IP addresses to these PCs.

### 3.1.3 WAN Setup Summary

When In WAN setup summary phase, the property of the PVC added can view:

- VPI/VCI
- Connection Type:
- Service Name:
- Service Category:
- IP Address:
- Service State:
- NAT
- Firewall
- IGMP
- QoS

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.  
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

Back Save/Reboot

Figure: WAN setup summary

Click “Save/Reboot” to save these settings. And you can click “Back” to make any modifications. After you click “Save/Reboot”, it shows the following message.

#### DSL Router Reboot

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Figure: DSL Router Reboot

**NOTE:** You need to reboot to activate this WAN interface and further configure services over this interface, and it will take about two minutes to done with it.

### 3.1.4 Quick Setup Completed

DSL router does not require further configuration in order to start working. After the setup described in this chapter, you can immediately start using your gateway to:

- Share a broadband connection among multiple users (HTTP, FTP, Telnet, and NetMeeting) and between all of the computers connected to your home network.
- Build a home network by connecting additional PCs and network devices to the gateway.
- Control network parameters, including DHCP, DNS and WAN settings.
- View network status, traffic statistics, system log and more.
- Allow access from the Internet to games and other services provided by computers in the home network.
- Prohibit computers in the home network from accessing selected services on the Internet.
- Block access to specific Internet Web sites from your home network. To learn about how to configure your Firewall security parameters, please refer to section 7.3. If you wish to apply corporate-grade security to your network, please refer to section 7.3.11.

If your gateway is equipped with multiple LAN ports, you can connect additional devices directly to the gateway. Otherwise, connect a hub or switch to the LAN port, to which you can connect additional devices. In both cases, configure newly connected devices to automatically obtain IP address as described above.

## 3.2 DSL Router Device information

Click “Device Info”, It should view the information as below:

- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP

### 3.2.1 Summary of Device information

This interface contains the following information:

- Board ID:
- Software Version:
- Bootloader (CFE) Version:
- Wireless Driver Version:
- Upstream Line Rate
- Downstream Line Rate
- LAN IPv4 Address: The management IP address
- Default Gateway: No gateway in a pure bridging mode; under other modes such as PPPOE/PPPOA, it is the address of the uplink equipment.
- DNS Server address: Obtained from the uplink equipment in PPPOE/PPPOA mode; No DNS Server address in a pure bridging mode; or input them manually.

The screenshot shows a web interface for a DSL router. On the left is a vertical navigation menu with the following items: Device Info (highlighted), Summary, WAN, Statistics, Route, ARP, DHCP, Advanced Setup, Diagnostics, and Management. The main content area is titled "Device Info" and contains a table with the following data:

Board ID:	96358VW2
Software Version:	090513_1532-4.02L_03.A2pB025c1.d21j2
Bootloader (CFE) Version:	1.0.37-102.9
Wireless Driver Version:	5.10.85.0.cpe4.402.0

Below this table is a note: "This information reflects the current status of your DSL connection." Underneath is another table with connection statistics:

Line Rate - Upstream (Kbps):	64
Line Rate - Downstream (Kbps):	1024
LAN IPv4 Address:	192.168.1.1
Default Gateway:	203.73.9.1
Primary DNS Server:	139.175.55.244
Secondary DNS Server:	139.175.252.16

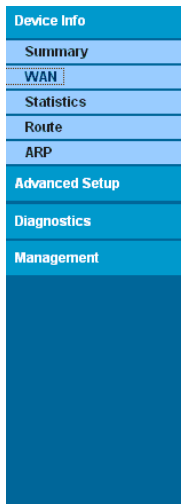
Figure: summary of Device information

### 3.2.2 WAN Interface information

Click “WAN” to show the following interface, depend on the selected connection mode, the Summary screen shows the status and also the connect or disconnect button.

This interface contains the following informations of every WAN connection:

- Interface
- Decsription
- Type
- VlanMuxID
- Igmp
- NAT
- Firewall
- Status
- IPv4 Address



WAN Info								
Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address
ppp0	pppoe_0_0_33	PPPoE	Disabled	Disabled	Enabled	Enabled	Connecting	

Figure: WAN interface information

### 3.2.3 Statistics

In this page, It includes four parts information:

- Statistics of LAN
- Statistics of WAN Service
- Statistics of xTM
- Statistics of xDSL

#### 3.2.3.1 Statistics of LAN

Click “Statistics” --> ”LAN” to show the following interface. You can query information on packets received at the Ethernet. Click “Reset Statistics” to return the values to zero and recount them.

You can view the info as below:

- Interface
- Received
  - Bytes: Bytes of Received
  - Pkts: Packets of Received
  - Errs: Errors packets of Received
  - Drops: Drops packets of Received
- Transmitted
  - Bytes: Bytes of Received
  - Pkts: Packets of Received
  - Errs: Errors packets of Received
  - Drops: Drops packets of Received

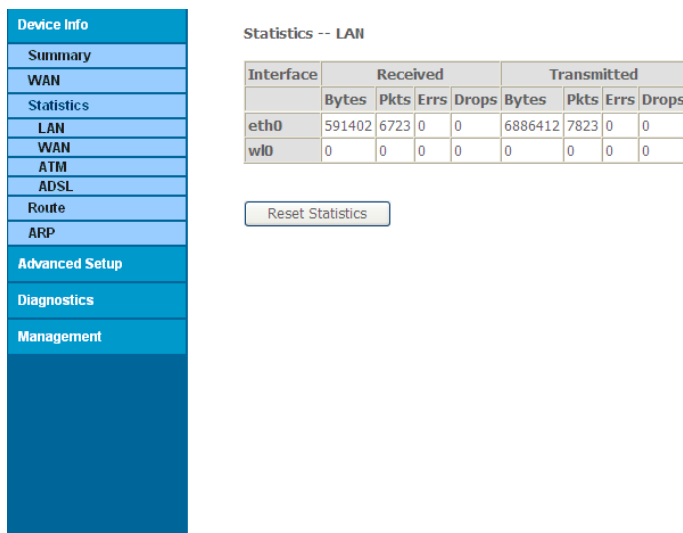


Figure: Statistics of LAN



### 3.2.3.2 Statistics of WAN Service

Click “Statistics” --> “WAN Service” to show the following interface. You can query information on packets received at the WAN interfaces. Click “Reset Statistics” to return the values to zero and recount them.

Informations as below:

- Interface
- Description
- Received
  - Bytes: Bytes of Received
  - Pkts: Packets of Received
  - Errs: Errors packets of Received
  - Drops: Drops packets of Received
- Transmitted
  - Bytes: Bytes of Received
  - Pkts: Packets of Received
  - Errs: Errors packets of Received
  - Drops: Drops packets of Received

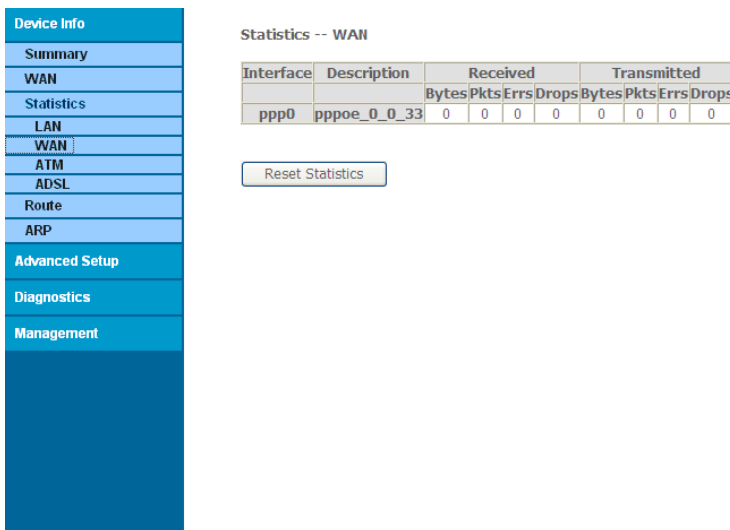


Figure: Statistics of WAN

### 3.2.3.3 Statistics of xTM

Click “Statistics”-->”xTM” to show the following interface. You can query information on packets received at the xTM interfaces. Click “Reset” to return the values to zero and recount them.

There are three part info:

- xTM Interface Statistics:
  - Port Number
  - In Octets
  - Out Octets
  - In Packets
  - Out Packets
  - In OAM Cells
  - Out OAM Cells
  - In ASM Cells
  - Out ASM Cells
  - In Packet Errors
  - In Cell Errors



Figure: Statistics of xTM

### 3.2.3.4 Statistics of xDSL

Click “Statistics”-->”xDSL” to show the following interface.  
 If the DSL line is activated, the following window will show.

Statistics -- xDSL		
Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:	L3	
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames		
Super Frame Errors:		
RS Words:		
RS Correctable Errors::		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

**Figure: Statistics of xDSL**

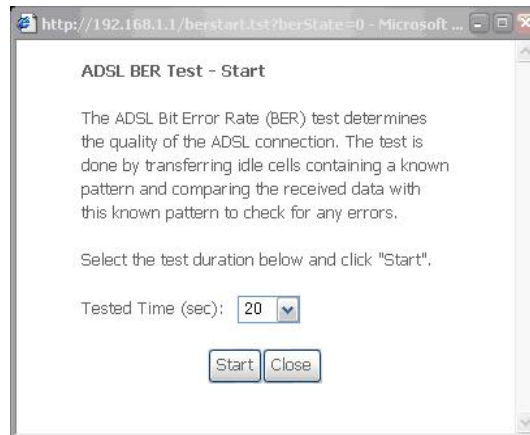
You will see the following information pertinent to the ADSL line in the page:

- Mode:
- Traffic Type:
- Status:
- Link Power State:
- Rate (Kbps): Upstream Line Rate / Downstream Line Rate.

At the lower part of this interface, there is a “Reset Statistics” button. Click it to return values to zero and recount.

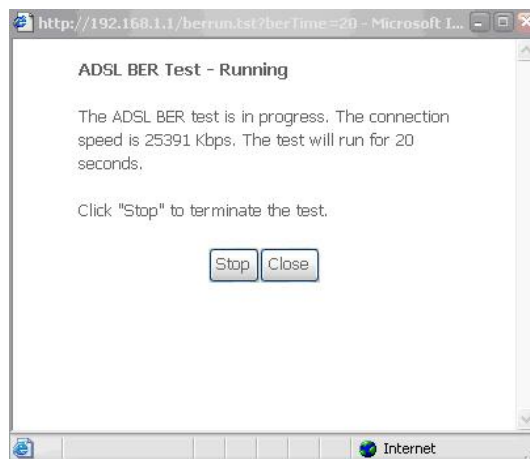
## ADSL BER Test

Click “ADSL BER Test” to do a “Bit Error Rate” Test on the DSL line. The test interface is as follows:

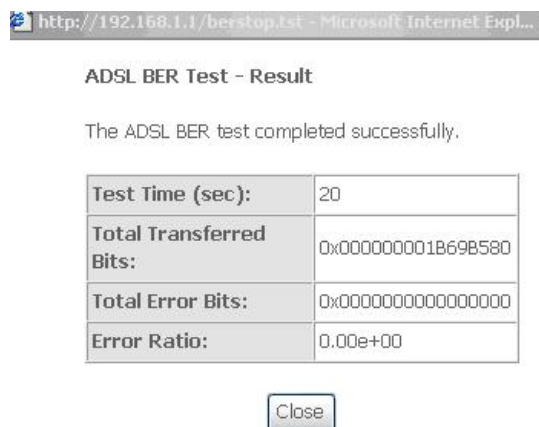


**Figure: ADSL BER Test**

The Tested Time (sec) has the following choices: 1, 5, 10, 20, 60, 120, 180, 240, 300, and 360. Select a time and then click “Start” to pop up the following interfaces in sequence.



**Figure: ADSL BER Test Running Page**



**Figure: ADSL BER Test Result**

**Note:** If the error ratio reaches up to “e-5”, the user will not be able to access the Internet.

### 3.2.4 Route table information

Click "Route". You can view the route table information, Each route item in route table has info as below:

- Destination
- Gateway
- Subnet Mask
- Flag
- Metric
- Service
- Interface

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
203.73.7.1	0.0.0.0	255.255.255.255	UH	0	pppoe_0_0_33_1	ppp_0_0_33_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	203.73.7.1	0.0.0.0	UG	0	pppoe_0_0_33_1	ppp_0_0_33_1

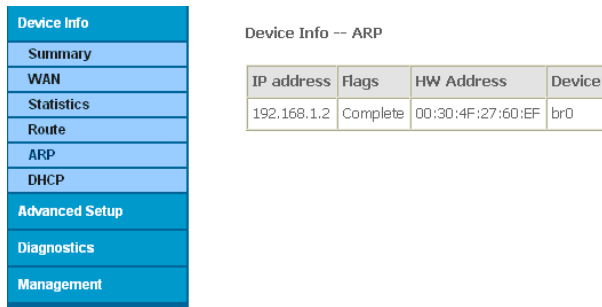
Figure: Route table

### 3.2.5 ARP table information

Click “ARP” to show the following interface. You can query the MAC and IP addresses information of the equipment attached to the Router.

Each ARP item has information as below:

- IP address
- Flags
- HW address
- Device



The screenshot shows a web interface for 'Device Info' with a navigation menu on the left containing: Summary, WAN, Statistics, Route, ARP, DHCP, Advanced Setup, Diagnostics, and Management. The 'ARP' option is selected. The main content area is titled 'Device Info -- ARP' and contains a table with the following data:

IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:30:4F:27:60:EF	br0

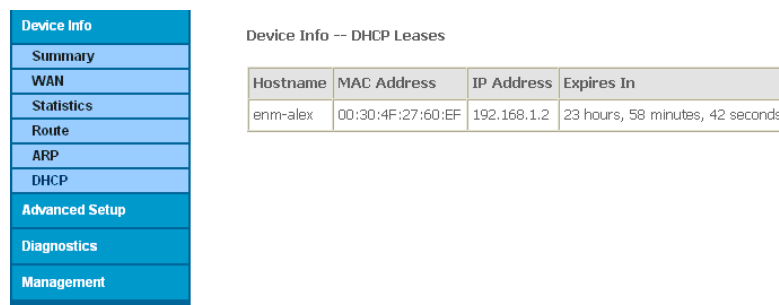
Figure: ARP table

### 3.2.6 DHCP IP Leases information

Click “DHCP” to show the following interface. You can query the IP addresses assignment to which MAC Address in DSL router’s LAN side, Through Ethernet can obtain the IP Address from the DHCP server on DSL router.

Each Leases item include info as below:

- Hostname
- MAC Address
- IP Address
- Expires In: How many times the Device Leases the IP Address for the MAC Address



The screenshot shows a web interface for 'Device Info' with a navigation menu on the left containing: Summary, WAN, Statistics, Route, ARP, DHCP, Advanced Setup, Diagnostics, and Management. The 'DHCP' option is selected. The main content area is titled 'Device Info -- DHCP Leases' and contains a table with the following data:

Hostname	MAC Address	IP Address	Expires In
enm-alex	00:30:4F:27:60:EF	192.168.1.2	23 hours, 58 minutes, 42 seconds

Figure: DHCP Leases List

### 3.3 Advanced Setup

Click “Advanced Setup” to enter the advanced system setup interface. there many items as below:

- Layer2 Interface
- WAN Servic
- LAN
- Security
- Parental control
- Quality of Service
- Routing
- DNS
- DSL
- Upnp
- Dns Proxy
- Interface Grouping
- LAN Ports
- Certificate

Advance Setup is DSL Router’s config center,

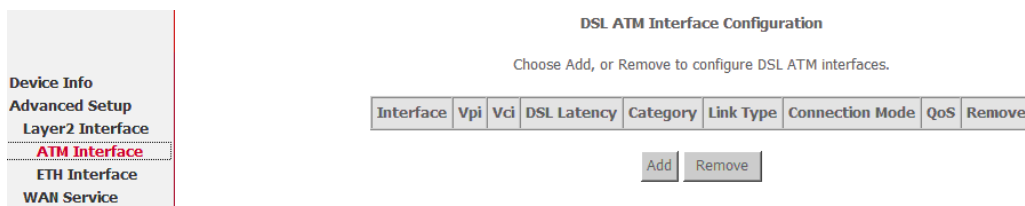
#### 3.3.1 Layer2 INTERFACE

Choose **Advanced Setup > Layer2 Interface** and two items may appear.

- **ATM Interface**
- **ETH Interface**

##### 3.3.1.1 ATM Interface

Choose **Advanced Setup > Layer2 Interface > ATM Interface** . In this page, you can add or remove to configure DSL ATM Interfaces.



Click **Add** to add ATM Interface and the following page appears.

#### ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]   
VCI: [32-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

- EoA
- PPPoA
- IPoA

Encapsulation Mode:

Service Category:

#### Select Connection Mode

- Default Mode - Single service over one connection
- VLAN MUX Mode - Multiple Vlan service over one connection
- MSC Mode - Multiple Service over one Connection

#### Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service.

In this page, you can enter this PVC (VPI and VCI) value, and select DSL link type (EoA is for PPPoE, IPoE, and Bridge.), encapsulation mode, service category, connection Mode.

- **VPI (Virtual Path Identifier):** The virtual path between two points in an ATM network, and its valid value is from 0 to 255.
- **VCI (Virtual Channel Identifier):** The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).
- **DSL Link Type:** EoA (it is for PPPoE, IPoE, and Bridge), PPPoA, or IPoA
- **Encapsulation Mode:** LLC/SNAP-BRIDGING, or VC/MUX
- **Service Category:** UBR Without PCR, UBR With PCR, CBR, Non Realtime VBR, Realtime VBR.
- **Connection Mode:** Default mode, VLAN MUX mode, or MSC mode
- **Enable Quality Of Service:** enable/disable.

In actual applications, you can modify them depending on your requirement.

You can also select the **Enable Quality Of Service** check box in to enable the packet level QoS for a PVC. This improves performance for selected classes of applications.

**Note: QoS cannot be set for CBR and Realtime VBR.**

Click **Apply/Save** to save the configuration, and return the following page:

#### DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

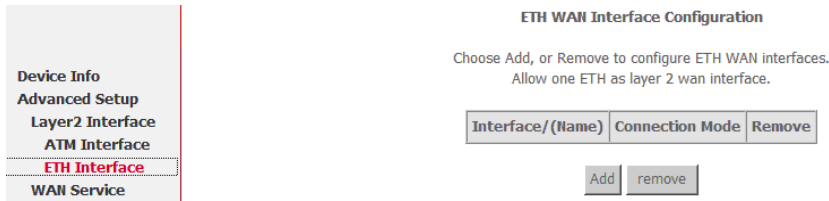
Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Disabled	<input type="checkbox"/>

If you want to remove this Interface, please select the **Remove** check box and click **Remove**.

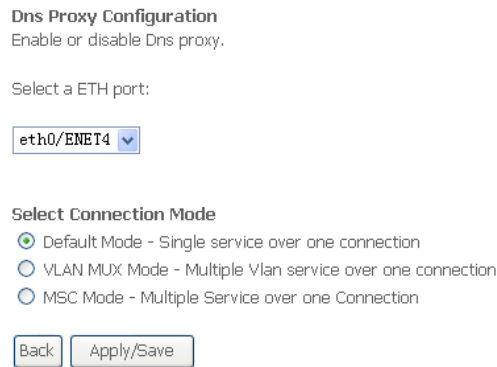


### 3.3.1.2 ETH Interface

Choose **Advanced Setup > Layer2 Interface > ETH Interface**, and the following page appears. In this page, you can add or remove to configure ETH WAN Interfaces.



Click **Add** and the following page appears.



In this page, you can select a ETH port, such as eth0/ENET4, and select connection mode. Click **Apply/Save** to save configuration.

## 3.3.2 WAN CONFIGURATION

Choose **Advance Setup > WAN Service**, and the following page appears.

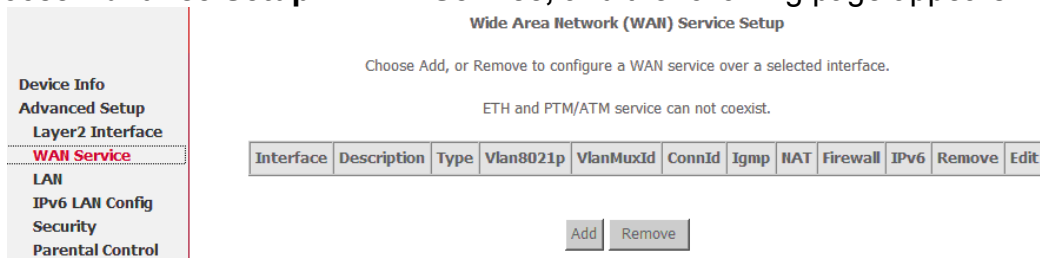
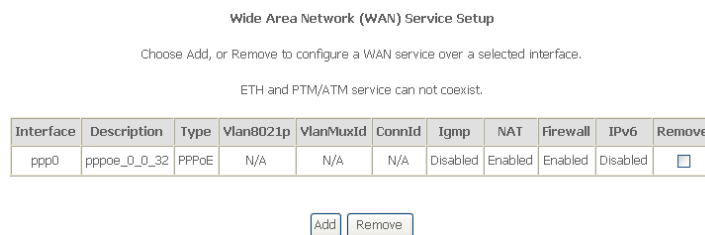


Figure 1 WAN configuration

Click **Add**, it turns into the following page. You can configure PPPoE, PPPoA, Mer (IPoE), Bridge, IPoA WAN configuration.

**Note: ETH and PTM/ATM service can not be coexist.**



Choose **Remove** check box, click **Remove** to delete the WAN configuration.

### 3.3.2.1 Add PPPoE WAN configuration

In the **WAN Service Setup** page, click **Add** to add WAN configuration. This section describes the procedure for adding pppoe\_0\_0\_32 (PPPoE mode).

**Step 1:** Click **Add** to turn into the following page. (At first, you must add suitable ATM configuration for this WAN configuration.) In this page, you can select ATM Interface .

#### WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portid\_vpi\_vci)

For PTM interface, the descriptor string is (portid\_high\_low)

Where portid=0 --> DSL Latency PATH0

portid=1 --> DSL Latency PATH1

portid=4 --> DSL Latency PATH0&1

low =0 --> Low PTM Priority not set

low =1 --> Low PTM Priority set

high =0 --> High PTM Priority not set

high =1 --> High PTM Priority set

atm0/ (0\_0\_32)

Back Next

**Step 2:** After proper selection, click **Next**, and the following page appears.

#### WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description: pppoe\_0\_0\_32

Enable IPv6 for this service

Back Next

**Step 3:** In this page, select WAN service type **PPP over Ethernet(PPPoE)**. Click **Next**, and the following page appears.

#### PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Advanced DMZ

Non DMZ IP Address:

Non DMZ Net Mask:

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

#### IGMP Multicast

Enable IGMP Multicast

Back Next

**Step 4:** In this page, you can modify the PPP username, PPP password, and authentication method.

- **PPP Username:** The correct user name that your ISP provides to you.
- **PPP Password:** The correct password that your ISP provides to you.
- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable Fullcone NAT:** A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.
- **Dial on demand (with idle timeout timer):** If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPOE connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoE dialup. If this function is disabled, the modem performs PPPoE dial-up all the time. The PPPoE connection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.
- **PPP IP extension:** After **PPP IP extension** is enabled, the WAN IP address obtained by the modem through built-in dial-up can be directly assigned to the PC being attached with the modem (at this time, the modem has only one PC). From the view of the PC user, this is even with that the PC dials up to obtain an IP address. But actually, the dial-up is done by the modem. If this function is disabled, the modem itself obtains the WAN IP address automatically.
- **Advanced DMZ:** Only LAN4 port supports this service. This is the virtual server configuration option. The DMZ Host feature allows one local computer to be exposed to the internet, to be this feature, the other computer can easily enter the DMZ Host, a DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.
- **PPP IP extension:** If you want to configure DMZ Host, you should enable it at first.
- **Non DMZ IP Address:** The DMZ host IP address. You can modify it.
- **Non DMZ Net Mask:** The DMZ Host Subnet Mask, it is build upon the DMZ Host IP Address.
- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
- **IGMP Multicast:** IGMP proxy. For example, if you want PPPoE mode to support IPTV, enable it.

After enter the PPP Username and PPP Password, click **Next**, and the following page appears.

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface

**Step 5:** In this page, select a preferred WAN interface as the system default gateway. Click **Next**, and the following page appears.

**DNS Server Configuration**

Get DNS server information from the selected WAN interface  
OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

Obtain DNS info from a WAN interface:  
WAN Interface selected:

Use the following Static DNS IP address:  
Primary DNS server:   
Secondary DNS server:

**Step 6:** In this page, you can get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses. Click **Next**, and the following page appears.

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 32
Connection Type:	PPPoE
Service Name:	pppoe_0_0_32
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

**Step 7:** In this page, it shows all the configurations. Click **Apply/Save** to all the configurations, and the following page appears. Click **Back** to make any modifications.

**Wide Area Network (WAN) Service Setup**

Choose Add, or Remove to configure a WAN service over a selected interface.

ETH and PTM/ATM service can not coexist.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	IPv6	Remove
ppp0	pppoe_0_0_32	PPPoE	N/A	N/A	N/A	Disabled	Enabled	Enabled	Disabled	<input type="checkbox"/>

### 3.3.1.2 Add MER (IPoE) Configuration

In the **WAN Service Setup** page, click **Add** to add WAN configuration. This section describes the procedure for adding ipoe\_0\_0\_32 (Mer mode).

**Step 1:** Click **Add** to turn into the following page. (At first, you must add suitable ATM configuration for this WAN configuration.)

#### WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portid\_vpi\_vci)

For PTM interface, the descriptor string is (portid\_high\_low)

Where portid=0 --> DSL Latency PATH0

portid=1 --> DSL Latency PATH1

portid=4 --> DSL Latency PATH0&1

low =0 --> Low PTM Priority not set

low =1 --> Low PTM Priority set

high =0 --> High PTM Priority not set

high =1 --> High PTM Priority set

atm1/(0\_0\_32) ▼

Back Next

**Step 2:** Select an ATM Interface, such as atm1/ (0\_0\_32). Click **Next** and the following page appears.

#### WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)  
 IP over Ethernet  
 Bridging

Enter Service Description: ipoe\_0\_0\_32

Enable IPv6 for this service

Back Next

**Step 3:** In this page, you can modify the **WAN service type**, **Service Description**, and **Enable IPv6 for this service**. Click **Next** and the following page appears.

#### WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in MER mode.

If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID:  (8 hexadecimal digits)

Option 61 DUID:  (hexadecimal digit)

Option 125:  Disable  Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

**Step 4:** In this page, you can modify the **IP Settings**. Enter information provided by your ISP to configure the WAN IP settings. Click **Next** and the following page appears.

**Note:**

If select Obtain an IP address automatically is chosen, DHCP will be enabled for PVC in MER mode.

If Use the following Static IP address is chosen, enter the WAN IP address, subnet mask and interface gateway.

**Network Address Translation Settings**

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Firewall

**IGMP Multicast**

Enable IGMP Multicast

[Back](#) [Next](#)

**Step 5:** In this page, you can modify the **Network Address Translation Settings**. Click **Next** and the following page appears.

**Routing -- Default Gateway**

Select a preferred wan interface as the system default gateway.

Selected WAN Interface

[Back](#) [Next](#)

**Step 6:** In this page, select a preferred wan interface as the system default gateway. Click **Next** and the following page appears.

**DNS Server Configuration**

Get DNS server information from the selected WAN interface  
OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

Obtain DNS info from a WAN interface:

WAN Interface selected:

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

**Step 7:** In this page, you can get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses. Click **Next** and the following page appears.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 32
Connection Type:	IPoE
Service Name:	ipoe_0_0_32
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

**Step 8:** In this page, click **Apply/Save** to save all the configurations, and the following page appears. If you want to make any modifications, click **Back**.

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

ETH and PTM/ATM service can not coexist.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	IPv6	Remove
atm1	ipoe_0_0_32	IPoE	N/A	N/A	N/A	Disabled	Enabled	Disabled	Disabled	<input type="checkbox"/>

[Add](#) [Remove](#)

### 3.3.1.3 Add PPPoA Configuration

This section describes the procedure for adding pppoa\_0\_0\_35 (PPPoA mode).

**Step 1:** You need to open the **Layer2 Interface > ATM Interface** page to add a PVC for PPPoA mode. Click **Add** and the following page appears.

ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI), select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]

VCI: [32-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA

PPPoA

IPoA

Encapsulation Mode:

Service Category:

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. use Advanced Setup/Quality of Service to assign priorities for the applications.

Enable Quality Of Service.

**Step 2:** Select the DSL link type to **PPPoA**, the Encapsulation Mode to **VC/MUX** (according to the uplink equipment). Click **Apply/Save**, and the following page appears.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
atm0	0	35	Path0	UBR	PPPoA	DefaultMode	Disabled	<input type="checkbox"/>

**Step 3:** Return to the **WAN Service** page, and click **Add**. The following page appears.

#### WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId\_vpi\_vci)

For PTM interface, the descriptor string is (portId\_high\_low)

Where portId=0 --> DSL Latency PATH0

portId=1 --> DSL Latency PATH1

portId=4 --> DSL Latency PATH0&1

low =0 --> Low PTM Priority not set

low =1 --> Low PTM Priority set

high =0 --> High PTM Priority not set

high =1 --> High PTM Priority set



**Step 4:** After proper selection, click **Next**, and the following page appears.

#### WAN Service Configuration

Enter Service Description:

**Step 5:** In this page, you can modify the service description in the text box. Click **Next**, and the following page appears.

#### PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:   
PPP Password:   
Authentication Method:

- Enable Fullcone NAT
- Dial on demand (with idle timeout timer)

- PPP IP extension
- Advanced DMZ

Non DMZ IP Address:   
Non DMZ Net Mask:

- Use Static IPv4 Address
- Enable PPP Debug Mode

#### IGMP Multicast

- Enable IGMP Multicast

**Step 6:** In this page, you can modify the PPP Username, PPP Password, Authentication Method according to your requirement. Click **Next**, and the following page appears.

#### Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface:

**Step 7:** In this page, select a preferred wan interface as the system default gateway. Click **Next**, and the following page appears.

DNS Server Configuration

Get DNS server information from the selected WAN interface  
OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

Obtain DNS info from a WAN interface:  
WAN Interface selected:

Use the following Static DNS IP address:  
Primary DNS server:   
Secondary DNS server:

**Step 8:** In this page, you can get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses. Click **Next** and the following page appears.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoA
Service Name:	pppoa_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

**Step 9:** In this page, click **Apply/Save** to save all the configurations, and the following page appears. If you want to make any modifications, click **Back**.

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

ETH and PTM/ATM service can not coexist.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	IPv6	Remove
pppoa0	pppoa_0_0_35	PPPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled	Disabled	<input type="checkbox"/>

### 3.3.1.4 Add IPoA Configuration

This section describes the procedure for adding ipoa\_0\_0\_35 (IPoA mode).

**Step 1:** You need to open the **Layer2 Interface > ATM Interface** page to add a PVC for IPoA mode. Click **Add** and the following page appears.

ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI), select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]

VCI: [32-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA  
 PPPoA  
 IPoA

Encapsulation Mode:

Service Category:

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. use Advanced Setup/Quality of Service to assign priorities for the applications.

Enable Quality Of Service.

**Step 2:** Select the DSL link type to **IPoA**, the Encapsulation Mode to **LLC/SNAP-ROUTING** (according to the uplink equipment). Click **Apply/Save**, and the following page appears.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
ipoa0	0	35	Path0	UBR	IPoA	DefaultMode	Disabled	<input type="checkbox"/>

**Step 3:** Return to the **WAN Service** page, and click **Add**. The following page appears.

#### WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId\_vpi\_vci)

For PTM interface, the descriptor string is (portId\_high\_low)

Where portId=0 --> DSL Latency PATH0

portId=1 --> DSL Latency PATH1

portId=4 --> DSL Latency PATH0&1

low =0 --> Low PTM Priority not set

low =1 --> Low PTM Priority set

high =0 --> High PTM Priority not set

high =1 --> High PTM Priority set

**Step 4:** After proper modifications, click **Next**, and the following page appears.

WAN Service Configuration

Enter Service Description:

**Step 5:** In this page, you can modify the service description. Click **Next**, and the following page appears.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

WAN IP Address:   
WAN Subnet Mask:

**Step 6:** In this page, enter information provided to you by your ISP to configure the WAN IP settings. Click **Next**, and the following page appears.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast

In this page, Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

**Enable NAT:** Select it to enable the NAT function of the modem. If you do not want to enable NAT, and wish the user of modem to access the Internet normally, you need to add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, enable the NAT function.

**Step 7:** After proper selection, click **Next**, and the following page appears.

### Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.


Selected WAN Interface  

**Step 8:** In this page, select a preferred WAN interface as the system default gateway. Click **Next**, and the following page appears.

### DNS Server Configuration

Get DNS server information from the selected WAN interface  
OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

Obtain DNS info from a WAN interface:

WAN Interface selected:  

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

**Step 9:** In this page, you should use static DNS IP address for IPoA mode. Enter primary DNS server and secondary DNS server. Click **Next**, and the following page appears.

### WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	IPoA
Service Name:	ipoa_0_0_35
Service Category:	UBR
IP Address:	10.10.10.112
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications

**Step 10:** Click **Apply/Save** to save all the configurations. And the following page appears. If you want to make any modifications, click **Back**.

### 3.3.1.5 Add Bridge Configuration

In the **WAN Service Setup** page, click **Add** to add WAN configuration. This section describes the procedure for adding br\_0\_0\_32 (Bridge mode).

**Step 1:** Click **Add** to turn into the following page. (At first, you must add suitable ATM configuration for this WAN configuration.) In this page, you can select ATM Interface.

#### WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId\_vpi\_vci)

For PTM interface, the descriptor string is (portId\_high\_low)

Where portId=0 --> DSL Latency PATH0

portId=1 --> DSL Latency PATH1

portId=4 --> DSL Latency PATH0&1

low =0 --> Low PTM Priority not set

low =1 --> Low PTM Priority set

high =0 --> High PTM Priority not set

high =1 --> High PTM Priority set

atm1/(0\_0\_32) ▼

Back Next

**Step 2:** Select an ATM Interface, such as atm1/(0\_0\_32). Click **Next**, and the following page appears.

#### WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description: br\_0\_0\_32

Enable IPv6 for this service

Back Next

**Step 3:** In this page, you can modify the **WAN service type**, **Service Description** and **Enable IPv6 for this service**. Click **Next**, and the following page appears.

#### WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 32
Connection Type:	Bridge
Service Name:	br_0_0_32
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

**Step 4:** Click **Apply/Save** to save all the configurations, and the following page appears.  
To make any modifications, click **Back**.

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

ETH and PTM/ATM service can not coexist.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	IPv6	Remove
atm1	br_0_0_32	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>

### 3.3.3 LAN configuration

Choose **Advanced Setup > LAN**, and the following page appears. In this page, you can configure an IP address for the DSL Router or enable DHCP server.

#### Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. GroupName

IP Address:

Subnet Mask:

Enable IGMP Snooping

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="text" value="Add Entries"/>	<input type="text" value="Remove Entries"/>	

Configure the second IP Address and Subnet Mask for LAN interface

In this page, you can modify the IP address of the device. The preset IP address is 192.168.1.1. This is the private IP address of the DSL Router, under which the device can be reached in the local network. It can be freely assigned from the block of available addresses. The IP address under which the Router can be reached from outside is assigned by the ISP.

IP Address:

Subnet Mask:



### 3.3.4 NAT-- Network Address Translation

#### Overview

##### Setting up the NAT function

- The DSL Router comes equipped with the NAT (Network Address Translation) function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses. All the local IP addresses are assigned to the router's public IP address by default.
- One of the characteristics of NAT is that data from the Internet is not allowed into the local network unless it has been explicitly requested by one of the PCs in the network. Most Internet applications can run behind the NAT firewall without any problems. For example, if you request Internet pages or send and receive e-mails, the request for data from the Internet comes from a PC in the local network, and so the router allows the data through. The router opens precisely one port for the application. A port in this context is an internal PC address, via which the data is exchanged between the Internet and a client on a PC in the local network. Communicating via a port is subject to the rules of a particular protocol (TCP or UDP).
- If an external application tries to send a call to a PC in the local network, the router will block it. There is no open port via which the data could enter the local network. Some applications, such as games on the Internet, require several links, i.e. several ports so that the players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to users in the local network. These applications cannot be run if Network Address Translation (NAT) has been activated.
- Using port forwarding (the forwarding of requests to particular ports) the router is forced to send requests from the Internet for a certain service, e.g. a game, to the appropriate port(s) on the PC on which the game is running. Port triggering is a special variant of port forwarding. Unlike port forwarding, the DSL Router forwards the data from the port block to the PC which has previously sent data to the Internet via a certain port (trigger port). This means that approval for the data transfer is not tied to one specific PC in the network, but rather to the port numbers of the required Internet service. Where configuration is concerned, this means: You have to define a so-called trigger port for the application and also the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. u The router checks all outgoing data for the port number and protocol. If it identifies a match of port and protocol for a defined trigger

port, then it will open the assigned public ports and notes the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, the router allows it through and directs it to the appropriate PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, the router simply ignores it.

**Note:**

- ◆ An application that is configured for port triggering can only be run by one user in the local network at a time.
- ◆ As long as the public ports are open, they can be used by unauthorized persons to gain access to a PC in the local network.

When the DSL Router is supplied, the NAT function (Network Address Translation) is activated, i.e. all IP addresses of PCs in the local network are converted to the router's public IP address when accessing the Internet. You can use the NAT settings to configure the DSL Router to carry out the following tasks:

**Note:**

For the functions described below, the IP addresses of the PCs must remain unchanged. If the IP addresses of the PCs are assigned via the DHCP server of the DSL Router, you must select Never expires (see page79) as the settings in the Local Network menu entry for the Lease time or assign static IP addresses for the PCs.

You can activate or deactivate the NAT function (by default the NAT function is activated).

### 3.3.4.1 DMZ Host

The DMZ (Demilitarized) Host feature allows one local computer to be exposed to the Internet. You wish to use a special-purpose Internet service, such as an on-line game or video-conferencing Program, that is not present in the Port Forwarding list and for which no port range information is available. You are not concerned with security and wish to expose one computer to all services without restriction.

---

**Note:**

A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computer sin the home net work at risk. When using a DMZ host, you must consider the security implications and protect it if necessary.

You can set up a client in your local network to be a so-called "DMZ host". Your device will then forward all incoming data traffic from the Internet to this client. You can then, for example, operate your own Web server on one of the clients in your local network and make it accessible to Internet users. As the exposed host, the local client is directly visible to the Internet and therefore particularly vulnerable to attacks (e.g. hacker attacks). Only activate this function if it is absolutely necessary (e.g. to operate a Web server) and other functions (e.g. port forwarding) are not adequate. In this case you should take appropriate measures for the clients concerned.

**Note:**

Only one PC per public IP address can be set up as an Exposed Host

#### Add a DMZ host

- To set up a PC as an DMZ host, select DMZ Host from the Advanced Setup→NAT→DMZ host

**NAT -- DMZ Host**

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

Save/Apply

**Figure: DMZ Host Config**

- Enter the Local IP address of the PC that is to be enabled as an Exposed Host.
- Apply the settings by clicking "Save/Apply".

## **Remove DMZ host**

**Clear** the DMZ Host Address

Apply setting by click **Save/Apply**

### 3.3.4.2 Port Triggering

If you configure port triggering for a certain application, you need to determine a so-called trigger port and the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. You can select known Internet services or assign ports or port blocks manually.

#### Add port Triggering

To set up port triggering for a service, select Port Triggering from the Advanced

- Settings → NAT → Port Triggering → add

##### NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

**Figure: Port Triggering**

- Select the required application from the applications list.  
If the application you require is not in the list, you must enter the relevant data on the screen custom application
- Trigger port start and Trigger port end: Enter the port that is to be monitored for outgoing data traffic.
- Trigger protocol: Select the protocol that is to be monitored for outgoing data traffic.
- Open Protocol: Select the protocol that is to be allowed for incoming data traffic
- Open port start and Open port end: Enter the port that is to be opened for incoming traffic.

#### Note:

You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

- Apply the settings by clicking "save/apply"

#### Remove port Triggering

Check remove box

Apply setting by click Save/Apply

### 3.3.4.3 NAT -- Virtual Servers Setup

In its default state, DSL router blocks all external users from connecting to or communicating with your network. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may want to expose your network to the Internet in certain limited and controlled ways in order to enable some applications to work from the LAN (game, voice and chat applications, for example) and to enable Internet-access to servers in the home network. The Port Forwarding feature supports both of these functionalities. If you are familiar with networking terminology and concepts, you may have encountered this topic referred to as “Local Servers” The Port Forwarding screen lets you define the applications that require special handling by DSL router. All you have to do is select the application protocol and the local IP address of the computer that will be using or providing the service. If required, you may add new protocols in addition to the most common ones provided by DSL router. For example, if you wanted to use a File Transfer Protocol (FTP) application on one of your PCs, you would simply select FTP from the list and enter the local IP address or host name of the designated computer. All FTP-related data arriving at DSL router from the Internet will henceforth be forwarded to the specific computer. Similarly, you can grant Internet users access to servers inside your home network, by identifying each service and the PC that will provide it. This is useful, for example, if you want to host a Web server inside your home network. When an Internet user points his/her browser to DSL router external IP address, the gateway will forward the incoming HTTP request to your Web server. With one external IP address (DSL router main IP address), different applications can be assigned to your LAN computers, however each type of application is limited to use one computer. For example, you can define that FTP will use address X to reach computer A and Telnet will also use address X to reach computer A, but attempting to define FTP to use address X to reach both computer A and B will fail. DSL router therefore provides the ability to add additional public IP addresses to port forwarding rules, which you must obtain from your ISP, and enter into the NAT IP Addresses Pool (see section 7.3.7). You will then be able to define FTP to use address X to reach computer A and address Y to reach computer B. Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated. Let's say, that you have a Web server running on your PC on port 8080 and you want to grant access to this server to any one who accesses DSL router via HTTP To accomplish this, do the following:

- Define a port forwarding rule for the HTTP service, with the PC IP or host name.
- Specify 8080 in the Forward to Port' field.

All incoming HTTP traffic will now be forwarded to the PC running the Web server on port 8080 when setting a port forwarding service; you must ensure that the port is not already in use by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP the port used by the gateway VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents.

**Note:**

Some applications, such as FTP, TFTP, PPTP and H323, require the support of special specific Application Level Gateway (ALG) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. DSL router is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network The ALG is automatically assigned based on the destination port

**Add Port Forwarding**

- To set up Virtual Servers for a service, select the Advanced Setup → NAT → Virtual Servers and click “add” to add the Virtual Server.

**NAT -- Virtual Servers Setup**

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	--------

**Figure: Add virtual Servers**

- Select a service ,or custom your server
- Set Server IP address
- Enter the Set Server IP address of the computer that will provide the service (the server in the Local Host field. Note that unless an additional external IP address has been added, only one LAN computer can be assigned to provide a specific service or application.
- Set External port start external port end
- Select protocol
- Set Internal port start and internal port end
- Entry Remote IP
- Click OK to apply the settings

If the application you require is not in the list, you must manually enter the relevant data on the screen:

Select the protocol for the service you are providing from the Protocol list. Under Public port, enter the port number of the service you are providing. In the Local port field, enter the internal port number to which service requests are to be forwarded. In the Local IP address field, enter the IP address of the PC that provides the service.

**Example:** the Web server has been configured to react to requests on port 8080. However, the requests from websites enter the Web server via port 80 (standard value). If you add the PC to the forwarding table and define port 80 as the public port and port 8080 as an internal port, all requests from the Internet are diverted to the service with the port number 80 on the Web server of the PC you have defined with port 8080.

**Note:**

You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

**Del Port Forwarding**

- Click remove box
- Click remove to apply the settings



### 3.3.5 Security

Security is an important function of DSL; it protects the resources of a private network from users from other networks. Also the item prevents unauthorized internet users from accessing private networks connected to the internet. All messages entering or leaving the intranet (i.e., the local network to which you are connected) must pass through the security examines, which examines each message and blocks those that do not meet the specified security criteria.

There are three basic types of security techniques:

- IP packet filtering: The system examines each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure.
- Circuit-level gateway implementation: This process applies security mechanisms when a TCP or UDP connection is established. Once the connect has been made, packets can flow between the hosts without further checking.
- MAC frame filtering: The system examines each frame entering or leaving the network form layer 2. And accord to user-defined rules accepts and rejects frame.

A security management program can be configured one of two basic ways:

- A default-deny policy.
- A default-allow policy.

A default-deny approach to security is by far the more secure, but due to the difficulty in configuring and managing a network in that fashion, many networks instead use the default-allow approach. Let's assume for the moment that your security management program utilizes a default-deny policy, and you only have certain services enabled that you want people to be able to use from the Internet.

NOTE: The security is like a firewall.

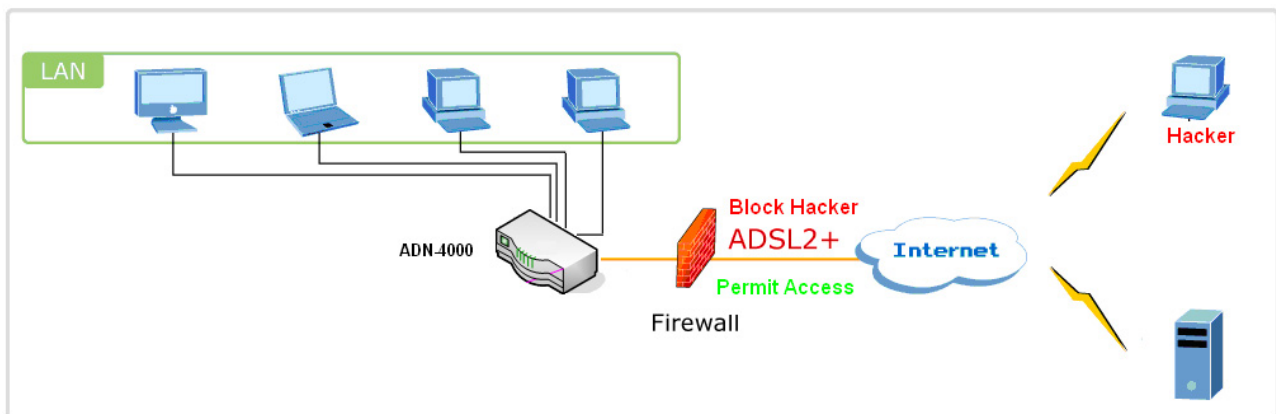


Figure: the Security application

Click “Security” -->” IP Filtering” to show the following interface. By default, the firewall is enabled. The firewall is used to block document transmissions between the Internet and your PC. It serves as a safety guard and only permits authorized documents to be sent into the LAN.

**Note:** If the Router configured as **bridge mode**, the **IP Filtering** will **disabled** and the **IP filtering** interface will disappear.

And if the Router configured as **Non-Bridge mode PVC**, the **MAC Filtering** will **disabled** and the **MAC Filtering** interface will disappear.

### 3.3.5.1 Outgoing IP Filtering Setup

When Outgoing IP Filtering rules setup being enable on the ROUTER, the various security functions for the local network will enable at the same time .You can protect the network against hacker attacks and block individual PC’s access to selected services or internet sites.

Click “Security”-->” IP Filtering”-->” Outgoing” to show the following interface.

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

#### Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
-------------	----------	-----------------------	-------------	----------------------	------------	--------

**Figure: Outgoing IP Filtering Config**

Click “Add” to enter the related interface defining the IP filtering rule as follows.

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

#### Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

**Figure: Outgoing IP Filtering Add Setup**

- Filter Name: Enter the name of outgoing filter rule
- Protocol: Select one among TCP/UDP TCP UDP or ICMP protocols
- Source IP address: Enter an IP address. When you have set IP address, the outgoing packet (protocol selected packet) will block.
- Source subnet mask
- Source port : UPD/TCP source port or a range of ports
- Destination IP address: Destination IP (default no set)
- Destination subnet mask:
- Destination port : UPD/TCP destination port or a range of ports

There is an example to introduce how to configure the outgoing IP Filtering.

The topology is as follows:

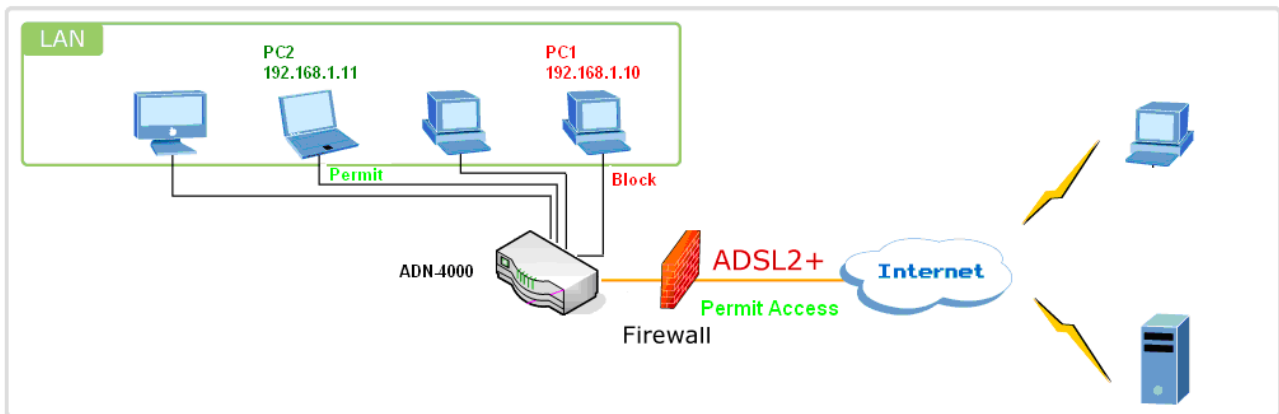


Figure: Outgoing IP filter application

**Request:**

- I need to block a whose IP address is 192.168.1.10. All outgoing UDP/TCP packet from that PC1(192.168.1.10) is disallowed.
- Allow all outgoing traffic packet from PC2 (192.168.1.11).

## Configuration:

1. By default, all outgoing IP traffic from LAN is allowed, so allow all the IP packet come for the PC2.
2. The detailed configuration steps are as follows:

### Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:	<input type="text" value="Filter1"/>
Protocol:	<input type="text" value="TCP/UDP"/>
Source IP address:	<input type="text" value="192.168.1.10"/>
Source Subnet Mask:	<input type="text" value="255.255.255.0"/>
Source Port (port or port:port):	<input type="text"/>
Destination IP address:	<input type="text"/>
Destination Subnet Mask:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>
DSCP Mark:	<input type="text"/>

**Figure: Outgoing IP Filtering Add Setup example**

3. Click "Save/apply" to show below.

### Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove
Filter1	TCP/UDP	192.168.1.10 / 255.255.255.0					<input type="checkbox"/>

**Figure: Outgoing IP Filtering Config Complete**

### 3.3.5.2 Incoming IP Filtering Setup

The incoming IP filter is used to block and permit IP packet transmission from internet. By default incoming IP filter block all incoming packet from internet. When incoming IP Filtering rules setup being enable on the ROUTER, you can permit remote individual PC to access various local network service .

Click “Security”-->” IP Filtering”-->” Incoming” to show the following interface.

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be ACCEPTED by setting up filters.

#### Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

**Figure: Incoming IP Filtering Config**

Click “Add” to enter the related interface defining the IP filtering rule as follows.

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

And you must select at least one or multiple WAN interfaces to apply this rule.

#### Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

#### WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces

Select one or more WAN/LAN interfaces displayed below to apply this rule.

- Select All
- pppoe\_0\_0\_33/ppp0
- br0/br0

**Figure: Incoming IP Filtering Add Setup**

- Filter Name: Enter the name of incoming filter rule
- Protocol: Select one among TCP/UDP TCP UDP or ICMP protocols
- Source IP address: Enter an IP address. When you have set IP address, the incoming packet (protocol selected packet) will allow.
- Source subnet mask:
- Source port : UPD/TCP source port or a range of ports
- Destination IP address: Destination IP (default no set)
- Destination subnet mask:
- Destination port : UPD/TCP destination port or a range of ports
- Wan interfaces: You can select WAN interfaces and PVC

There is an example to introduce how to configure the incoming IP Filtering:

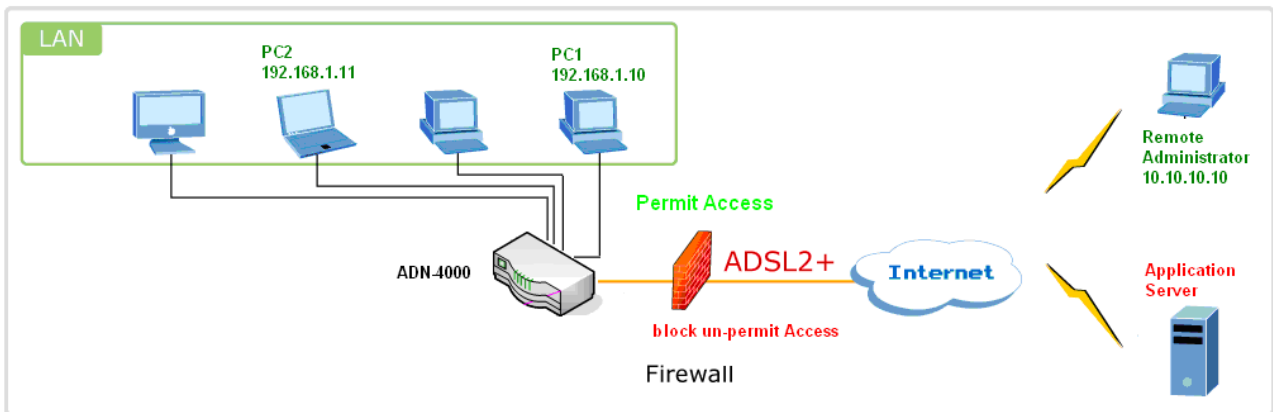


Figure: incoming IP filter application

**Request:**

- I need to permit a PC whose IP address is 10.10.10.10. All Incoming TCP/UDP packet traffic from that PC(10.10.10.10) is allowed.
- Block all IP traffic from other PC .

**Configuration:**

1. By default, all incoming IP traffic from internet is blocked, so all the IP packets come for the internet are blocked.
2. The detailed configuration steps are as follows:

**Add IP Filter -- Incoming**

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

DSCP Mark:

**WAN Interfaces (Configured in Routing mode and with firewall enabled only)**

Select at least one or multiple WAN interfaces displayed below to apply this rule.

Select All

**Figure: Incoming IP Filtering Add Setup example**

3. Click "Save/apply" to show below.

**Incoming IP Filtering Setup**

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove
Incoming	ALL	TCP/UDP	10.10.10.10 / 255.255.0.0					<input type="checkbox"/>

**Figure: Incoming IP Filtering Config Complete**

### 3.3.5.3 MAC Filtering Setup

Maybe you want to manage Layer 2 MAC addresses to block or permit a computer within the home network. When you enable MAC filter rules, the ROUTER serves as a firewall which works at layer 2.

Click "Security" --> "MAC Filtering" to show the following interface.

**Note:** MAC Filtering is only effective on ATM PVCs configured in Bridge mode. If the ATM PVC is configured in other routing mode (such as PPPoE mode), the "MAC Filtering Setup" will not appear in the "Security" option.

**FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

#### MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:

**WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

Interface	Policy	Change
atm0	FORWARD	<input type="checkbox"/>

Change Policy

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------

Add Remove

Figure: MAC Filtering Setup overview



Click “add” to add MAC filter rules. The interface shows below.

#### Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Save/Apply

**Figure: MAC Filtering Add Config**

- Protocol Type: Select one among PPPoE IPV4 IPV6 AppleTalk IPX NETBEUI or ICMP protocols
- Destination MAC Address:
- Source MAC Address :
- Frame Direction: The direction of transmit frame, you can select LAN->WAN (from LAN to WAN) WAN -> LAN (from WAN to LAN) LAN ⇔ WAN.
- WAN Interface: Select a WAN interface.

### 3.3.6 Quality of Service

Many communication and multimedia applications require large, high speed bandwidths to transfer data between the local network and the internet. However, for many applications there is often only one internet connection available with limited capacity. QoS (Quality of Service) divides this capacity between the different applications and provides underplayed, continuous data transfer where data packets with higher priority are given preference.

Click “Quality of Service” to show the following interface. Under “Quality of Service”, there are two network share mode:” Queue Config”, ”QoS Classification”.

Quality of Service (QoS) for networks is an industry-wide set of standards and mechanisms for ensuring high-quality performance for critical applications. By using QoS mechanisms, network administrators can use existing resources efficiently and ensure the required level of service without reactively expanding or over-provisioning their networks.

Traditionally, the concept of quality in networks meant that all network traffic was treated equally. The result was that all network traffic received the network’s best effort, with no guarantees for reliability, delay, variation in delay, or other performance characteristics. With best-effort delivery service, however, a single bandwidth-intensive application can result in poor or unacceptable performance for all applications. The QoS concept of quality is one in which the requirements of some applications and users are more critical than others, which means that some traffic needs preferential treatment.

#### 3.3.6.1 Enable QoS

In this interface, you can do QoS queue management configuration. By default, the system is enable QoS and set a default DSCP mark to automatically mark incoming traffic without reference to particular classifier.

Click ”Advance Setup”→”Quality of Classification” to show following interface:

**QoS -- Queue Management Configuration**

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

**Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.**

**Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.**

Enable QoS

Select Default DSCP Mark

**Figure: QoS queue management configuration**

Choose “Enable QoS” can enable QoS and the system can set default DSCP mark

Click “save/Apply” to active QoS.

### 3.3.6.2 QoS--Queue Config

The queuing in packet QoS will become effective only when packet is forwarded to QoS-enabled PVC. Packet forwarding is determined by IP routing or bridging, not under control of the packet QoS.

Click “Queue Config” to pop up an interface as below. In this interface, you can configure QoS Queue. A maximum 24 entries can be configured.

QoS Queue Configuration can allocated three queues .Each of the queues can be configured for a precedence value (Lower integer values for precedence imply higher priority for this queue relative to others). The queue entry configured here will be used by the classifier to place ingress packets appropriately.

QoS Queue Setup -- A maximum 16 entries can be configured.

If you disable WMM function in Wireless Page, queues related to wireless will not take effects

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	1			<input checked="" type="checkbox"/>	
WMM Voice Priority	2	wl0	2			<input checked="" type="checkbox"/>	
WMM Video Priority	3	wl0	3			<input checked="" type="checkbox"/>	
WMM Video Priority	4	wl0	4			<input checked="" type="checkbox"/>	
WMM Best Effort	5	wl0	5			<input checked="" type="checkbox"/>	
WMM Background	6	wl0	6			<input checked="" type="checkbox"/>	
WMM Background	7	wl0	7			<input checked="" type="checkbox"/>	
WMM Best Effort	8	wl0	8			<input checked="" type="checkbox"/>	

Figure:QoS Queue Config overview

#### NOTE:

Lower integer values for precedence imply higher priority for this queue relative to others. For example: add a QoS queue entry and allocate it to a specific network interface (PVC 0/8/81) . Set integer values for queue precedence are 2.

**Step 1.** Click “add ” bottom to show following interface:

#### QoS Queue Configuration

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others**

Click 'Apply/Save' to save and activate the queue.

Name:

Enable:

Interface:

Precedence:

Figure: QoS Queue Config

- Name: Fill a name for the entry.
- Enable: Enable or Disable to configure a QoS queue entry.
- Interface: select a specific network interface. When you have already selected a network interface, the specific network interface selected will automatically allocate to the queue
- Precedence: select an integer value for queue precedence. When you have already selected a integer value, the queue entry will place to ingress packets appropriately. Lower integer values for precedence imply higher priority for this queue relative to others.

**Step 2.** Add a QoS queue entry and assign it to a specific network interface, set integer values for queue precedence is 2. Show following interface:

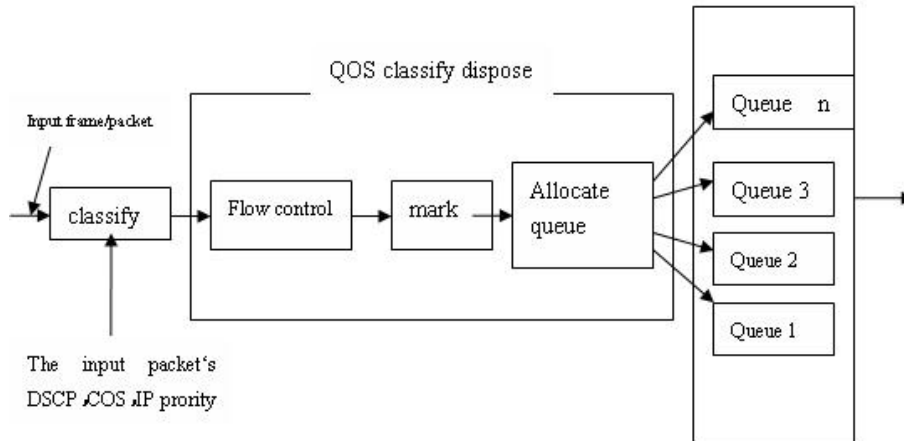
**Step 3.** After proper modifications, click “Save/Apply”. (This configuration will take effective at once.)

If you want to delete a certain queue, you can disable this queue and choose this queue, last click “Remove” button to delete it.

After the queue config is already configured, you can create several traffic class rules to classify the upstream traffic.

### 3.3.6.3 QoS -- QoS Classification

Some application require that specific bandwidths ensure its data be forward in the time. QoS classification can creates traffic class rule to classify the upstream traffic. Assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. After QoS classification, QoS divides capacity between the different applications and provides un-delayed, continuous data transfer where data packet with higher priority are given preference. The follow diagram show how QoS classify the



Click “QoS Classification” to pop up an interface as below. In this interface, you can configure network traffic classes.

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.  
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

The QoS function has been disabled. Classification rules would not take effects.

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>																		

Figure: QoS Classification Conifg overview

Click “Add” to show the following interface.

### Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte.

A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Traffic Class Name:	<input type="text"/>
Rule Order:	Last <input type="button" value="v"/>
Rule Status:	Disable <input type="button" value="v"/>

### Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface:	<input type="text"/> <input type="button" value="v"/>
Ether Type:	<input type="text"/> <input type="button" value="v"/>
Source MAC Address:	<input type="text"/>
Source MAC Mask:	<input type="text"/>
Destination MAC Address:	<input type="text"/>
Destination MAC Mask:	<input type="text"/>

### Specify Classification Results

Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:	<input type="text"/> <input type="button" value="v"/>
Mark Differentiated Service Code Point (DSCP):	<input type="text"/> <input type="button" value="v"/>
Mark 802.1p priority:	<input type="text"/> <input type="button" value="v"/>
Tag VLAN ID:	<input type="text"/>

Apply/Save

Figure: QoS Classification Conifg

## 3.3.7 Routing

### 3.3.7.1 Routing – Default Gateway

In this interface, you can modify the Default Gateway settings.

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

**NOTE:**

If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

#### Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface

Save/Apply

Figure: Default Gateway



### 3.3.7.2 Static Routes

Networking devices forward packets using route information that is either manually configured or dynamically learned using a routing protocol. Static routes are manually configured and define an explicit path between two networking devices. Unlike a dynamic routing protocol, static routes are not automatically updated and must be manually reconfigured if the network topology changes. The benefits of using static routes include security and resource efficiency. Static routes use less bandwidth than dynamic routing protocols and no CPU cycles are used to calculate and communicate routes. The main disadvantage to using static routes is the lack of automatic reconfiguration if the network topology changes.

Static routes can be redistributed into dynamic routing protocols but routes generated by dynamic routing protocols cannot be redistributed into the static routing table. No algorithm exists to prevent the configuration of routing loops that use static routes.

Static routes are useful for smaller networks with only one path to an outside network and to provide security for a larger network for certain types of traffic or links to other networks that need more control. In general, most networks use dynamic routing protocols to communicate between networking devices but may have one or two static routes configured for special cases

#### Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.  
Note: If selected "MER" as WAN interface, default gateway must be configured.

Destination Network Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
<input type="checkbox"/> Use Gateway IP Address	<input type="text"/>
<input checked="" type="checkbox"/> Use Interface	<input type="text" value="pppoe_0_0_33/ppp0"/>
<input type="button" value="Save/Apply"/>	

Figure: Static routes Add Config

#### Add static route

- Enter destination network address
- Enter subnet Mask
- Enable "Use Gateway IP Address" and enter IP address
- Select use interface
- Apply setting by click Save/Apply

### 3.3.7.3 RIP

#### **Background**

The Routing Information Protocol, or RIP, as it is more commonly called, is one of the most enduring of all routing protocols. RIP is also one of the more easily confused protocols because a variety of RIP-like routing protocols proliferated, some of which even used the same name! RIP and the myriad RIP-like protocols were based on the same set of algorithms that use distance vectors to mathematically compare routes to identify the best path to any given destination address. These algorithms emerged from academic research that dates back to 1957. Today's open standard version of RIP, sometimes referred to as IP RIP, is formally defined in two documents: Request For Comments (RFC) 1058 and Internet Standard (STD) 56. As IP-based networks became both more numerous and greater in size, it became apparent to the Internet Engineering Task Force (IETF) that RIP needed to be updated. Consequently, the IETF released RFC 1388 in January 1993, which was then superseded in November 1994 by RFC 1723, which describes RIP 2 (the second version of RIP). These RFCs described an extension of RIP's capabilities but did not attempt to obsolete the previous version of RIP. RIP 2 enabled RIP messages to carry more information, which permitted the use of a simple authentication mechanism to secure table updates. More importantly, RIP 2 supported subnet masks, a critical feature that was not available in RIP.

This chapter summarizes the basic capabilities and features associated with RIP. Topics include the routing update process, RIP routing metrics, routing stability, and routing timers.

#### **Routing Updates**

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send

## RIP Routing Metric

RIP uses a single routing metric (hop count) to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop count value, which is typically 1. When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop

### Routing -- RIP Configuration

To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

Global RIP Mode  Disabled  Enabled

Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	<input type="checkbox"/>
ppp_0_0_33_1	0/0/33	2	Passive	<input type="checkbox"/>

Save/Apply

Figure: RIP Configuration

### RIP configuration

- To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode.
- To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface.

Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

## 3.3.8 DNS

Short for **Domain Name System** (or **Service** or **Server**), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name `www.example.com` might translate to `198.105.232.4`.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

### 3.3.8.1 DNS Server

In this interface, you can modify the DNS server settings.

**DNS Server Configuration**

Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with IPoA, static MER protocol.

Obtain DNS info from a WAN interface:

WAN Interface selected:

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

**Figure: DNS Server Configuration overview**

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment.

If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. The interface is below.

### DNS Server Configuration

Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with IPoA, static MER protocol.

Obtain DNS info from a WAN interface:

WAN Interface selected:

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

**Figure: DNS Server Add Configuration**

Click 'Save' button to save the new configuration.

**NOTE:** You must reboot the router to make the new configuration effective.

### 3.3.8.2 Dynamic DOMAIN NAME SERVICE (DDNS)

#### OVERVIEW

Dynamic DNS allows binding of domain names to hosts with dynamically assigned IP addresses by a Dynamic Host Control Protocol (DHCP) server and updates the name server with the new information about the host or the network. This is particularly useful to broadband users hosting internet services such as File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) on their local hosts connected to the broadband network at home. Dynamic DNS allows access to such hosts connected to the broadband networks using a domain name to exchange files, send receive email with highly personalized email addresses and host a website. The primary requirement in such case is for the domain name to be associated with the ever changing IP address of the host or the network. For more details about dynamic DNS please refer to RFC 2136.

To provide such support for the feature described above, a client is installed in the host serving the internet traffic directed to the domain. The client updates the IP address of the host whenever the host renegotiates the IP address for any reason. The system provides support for dynamic DNS allows the users to configure the following dynamic DNS servers for DDNS service:

- **DynDNS.org**: A free DNS service for hosts with dynamic IP addresses.
- **TZO**: A service provider providing dynamic and static DNS services for a fee.

To use one of the providers mentioned above requires the users to register with the dynamic DNS service provider the information about the host and the install the client software on the host which can update the service provider with the IP address and the domain name information.

#### CONFIGURATION

The DDNS feature in Linux reference software requires to be configured in the menu config to include the support for this feature. Once the software support is configured to be built for a profile, this feature can be configured using the WEB UI as:

- Choose the Advanced Setup from the WEB UI, choose the DNS menu item under Advanced
- Setup and select the Dynamic DNS menu item under DNS.

##### Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Figure: Dynamic DNS Configuration overview

- Click the Add button to configure new host information.

### Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider	<input type="text" value="DynDNS.org"/>
Hostname	<input type="text" value="ddns.dyndns.org"/>
Interface	<input type="text" value="pppoe_0_0_33/ppp0"/>
<b>DynDNS Settings</b>	
Username	<input type="text" value="ddns"/>
Password	<input type="password" value="••••"/>

Figure: Dynamic DNS Add Configuration

- **D-DNS provider:** Dynamic DNS provider's website.
  - **Hostname:** This is the domain name which can be modified.
  - **Interface:** The interface that the packets pass through on the ROUTER.
  - **Username:** This is the Username needed access the DDNS's management interface.
  - **Password:** This is the Password you will be prompted to enter when you access the DDNS's management interface.
- Select the service provider for the DDNS service; provide the hostname and the interface to use when sending the DDNS updates. Also enter the service provider specific registration information and click Save/Apply to use the feature.

### 3.3.9 DSL

In this interface, you can check the DSL settings. Mostly, the user just need to remain this factory default setting. Our Router support these modulations: G.Dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+ and AnnexM. The ROUTER will negotiate the modulation mode with the DSLAM.

#### DSL Settings

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable

Figure: DSL modulation settings



### 3.3.10 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Selecting the “Enable virtual ports” button in WEB UI “Interface Grouping” page will create three virtual interfaces within the system. Each virtual interface represents a physical Ethernet port within the external Ethernet Switch.

**Interface Grouping -- A maximum 16 entries can be configured**

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0	ENET(1-4)	
			wl0_Guest1	
			wl0_Guest2	
			wl0_Guest3	

### 3.3.11 Certificate

To use Certificate user interface, choose “Certificate” under “Advanced Setup” menu. There are two menu items under “Certificate” menu: “Local” and “CA”. For either type of certificate, the base screen shows a list of certificates stored in Router.

#### Local Certificates

Add, View or Remove certificates from this page.  
Local certificates are used by peers to verify your identity.

Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action
<a href="#">Create Certificate Request</a>		<a href="#">Import Certificate</a>		

Figure: Local Certificate overview

In the menu, “Local” means local certificates. “Trusted CA” means trusted Certificate Authority certificates. Local certificates preserve the identity of the Router. CA certificates are used by the Router to verify certificates from other hosts.

Local certificates can be created by two ways:

- Create a new certificate request, have it signed by a certificate authority and load the signed certificate
- Import an existing signed certificate directly

#### 3.3.11.1 Create New Local Certificate

##### Certificate name:

Creates an SSL certificate in the specified certificate repository (administrator's or domain's repository) by using a private key file and a corresponding certificate file.

##### Common Name:

The common name is the "fully qualified domain name," (or FQDN) used for DNS lookups of your server (for example, www.mydomain.com). Browsers use this information to identify your Web site. Some browsers will refuse to establish a secure connection with your site if the server name does not match the common name in the certificate. Please do not include the protocol specify "http://" or any port numbers or pathnames in the common name. Do not use wildcard characters such as \* or ? and do not use an IP address.

##### Organization Name:

The name of the organization to which the entity belongs (such as the name of a company).

##### State/Province Name:

This is the name of the state or province where your organization's head office is located. Please enter the full name of the state or province.

## Country/Region Name:

This is the two-letter ISO abbreviation for your country (for example, GB for the United Kingdom).

Follow the following steps to create a new certificate:

Click “Create Certificate Request”, enter necessary information:

Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:	<input type="text"/>
Common Name:	<input type="text"/>
Organization Name:	<input type="text"/>
State/Province Name:	<input type="text"/>
Country/Region Name:	<input type="text" value="US (United States)"/>

Apply

Figure: create new certificate request

Click “Apply” and wait several seconds, the generated certificate request will be shown:

### Certificate signing request

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

Name	123
Type	request
Subject	CN=321/O=654/ST=456/C=US
Signing Request	<pre>-----BEGIN CERTIFICATE REQUEST----- MIIBdjCB4AIBADA3MqwCgYDVQQDEwMzMjExDDAKBgNVBAoTAzY1NDEMMAoGA1UE CBMNDNDU2MQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA /QYOr3OO2Yg4cxYo56juN4cG61GGh6Y2SdmLZ8q6X8TBjzlw+1aB2IwNJPQnrYoc nuvIErKGU+qVBt87ZBcTaOlYovqEYtMoU/SLmDZbDaB9PgS69WpxlMChupVXL7i8 hMbDue7Rs3W7QAv1CzXnC4XQo18iEvYgxcVSEVKDm7MCAwEAAaAAMA0GCSqGSIb3 DQEBBAUAA4GBAKb6PFfocVLfAi1oLNWJctq7w2EtLm/t07NKF/cy/1SAW0KoTnfJ4 MGDlwyxP7yu9czg/kbf2jRi7Z5uIQ8qoSG8DtZJEMyQ1+LUMDF/oIEZTSnx1z6WW q33nU0o4+EBtZ9GwQarbmNg9S3zwgtppKIiH5/sumQ8k0NAyq9QFLZwj -----END CERTIFICATE REQUEST-----</pre>

Back

Load Signed Certificate

Figure: generated certificate request

The certificate request needs to be submitted to a certificate authority, which would sign the request. Then the signed certificate needs to be loaded into Router. Click “Load Certificate” button from the previous screen or from the base screen will bring up the load certificate page. Paste the signed certificate and click apply and a new certificate is created.

#### Load certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

xCertificate: 

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

Figure: Load Certificate

### 3.3.11.2 Import Existing Local Certificate

To import existing certificate, click “Import Certificate” button and paste both certificate and corresponding private key:

#### Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate: 

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

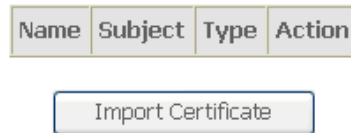
Figure: Import Certificate

### 3.3.11.3 Trusted CA Certificates

Click “Certificate” --> “Trusted CA” to show the interface. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

#### Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.



**Figure: Trusted CA certificates**

Click “Import Certificate”. CA certificate can only be imported. The screen for importing is shown below:

Certificate Name:

Certificate: 

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

**Figure: Import CA Certificate**

## 3.4 Wireless

### 3.4.1 Wireless – Basic

Choose **Wireless > Basic**, the following page appears.

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

Enable Wireless

Hide Access Point

Clients Isolation

Disable WMM Advertise

Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: 02:10:18:01:00:04

Channel:

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="wld_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wld_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wld_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

- **Enable Wireless:** If you want to make wireless be available, you have to check this box first. Otherwise, the Hide Access Point SSID, Country, Enable Wireless Guest Network, and Guest SSID boxes are not displayed.
- **Hide Access Point:** Check this box if you want to hide any access point for your router, so a station cannot obtain the SSID through passive scanning.
- **Clients Isolation:** When many clients connect to the same access point, they can access each other. If you want to disable the access between clients which connect the same access point, you can check this box.
- **Disable WMM Advertise:** WMM is short for wi-fi multimedia, which can provide high-performance multimedia voice and video data transfers.
- **SSID:** For added security, you should change the default SSID to a unique name.
- **Channel:** The option of the channel with which your gateway is configured. This parameter further specifies your wireless connection. For example, the channel will adjust according to nations to adapt to each nation's frequency provision (FCC 1~11, ETSI 1~13, JP 1~14).
- **Max Clients:** Specifies maximum wireless client stations to be able to link with AP. Once the clients exceed the max value, all other clients are refused. The value of maximum clients is 16.
- **Wireless - Guest/Virtual Access Points:** If you want to make Guest/Virtual network function be available, you have to check those boxes in the table below. In the current software version, three virtual access points can be configured.

After setting, click **Save/Apply** to save the basic wireless options and make the change take effect.

### 3.4.2 Wireless – Security

Choose **Wireless > Security**, the following page appears. In this page, the data is not encrypted when it is transferred from the device to the client station. This is the default option.

#### Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.  
You may setup configuration manually  
OR  
through WiFi Protected Setup(WPS)

#### WPS Setup

Enable WPS

#### Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.  
Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WEP Encryption:

- **Enable WSC:** If enable **Manual Setup AP**, you can not enable WSC.
- **Select SSID:** Select the wireless LAN of SSID to configure security features.
- **Network Authentication:** Select the authentication mode for the selected wireless LAN of SSID to be open. That is no WEP encryption, so the **WEP Encryption** is disabled.

### 64-bit WEP

If you select the "Shared" as the Network Authentication, you can select **64-bit** or **128-bit** as the Encryption Strength. In the following figure, select **64-bit** as an example.

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.  
Click "Save/Apply" when done.

Select SSID:

Network Authentication:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys  
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

- **Network Authentication:** Select the authentication mode for the selected wireless LAN of SSID to be open or shared.
- **WEP Encryption:** Enable WEP Encryption.
- **Encryption Strength:** Select the desired Data Security level to be 64-bit.
- **Current Network Key:** Select one of network key that you set on the Key boxes as default one.
- **Network Key 1 to 4:** Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.

The authentication modes are as follows: 802.1X, WPA, WPA-PSK, WPA2, WPA2 –PSK, Mixed WPA2/WPA, Mixed WPA2/WPA –PSK.

After proper configuration, click **Save/Apply** to save the wireless security options and make the modification effect.

### 3.4.3 Wireless – Advanced

Choose **Wireless > Advanced**, the following page appears. This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

#### Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click "Apply/Save" to configure the advanced wireless options.

Band:	<input type="text" value="2.4GHz"/>	
Channel:	<input type="text" value="1"/>	Current: 1
Auto Channel Timer(min)	<input type="text" value="0"/>	
802.11n/EWC:	<input type="text" value="Auto"/>	
Bandwidth:	<input type="text" value="20MHz in 2.4G Band and 40MHz in 5G Band"/>	Current: 20MHz
Control Sideband:	<input type="text" value="Lower"/>	Current: None
802.11n Rate:	<input type="text" value="Auto"/>	
802.11n Protection:	<input type="text" value="Auto"/>	
Support 802.11n Client Only:	<input type="text" value="Off"/>	
54g™ Rate:	<input type="text" value="1 Mbps"/>	
Multicast Rate:	<input type="text" value="Auto"/>	
Basic Rate:	<input type="text" value="Default"/>	
Fragmentation Threshold:	<input type="text" value="2346"/>	
RTS Threshold:	<input type="text" value="2347"/>	
DTIM Interval:	<input type="text" value="1"/>	
Beacon Interval:	<input type="text" value="100"/>	
Global Max Clients:	<input type="text" value="16"/>	
XPress™ Technology:	<input type="text" value="Disabled"/>	
Transmit Power:	<input type="text" value="100%"/>	
WMM(Wi-Fi Multimedia):	<input type="text" value="Enabled"/>	
WMM No Acknowledgement:	<input type="text" value="Disabled"/>	
WMM APSD:	<input type="text" value="Enabled"/>	

Apply/Save



- **Band:** Select using wireless frequency band range. The radio frequency remains at 2.4GHz.
- **Channel:** Fill in the appropriate channel to correspond with your network settings. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channeling functionality.
- **Auto Channel Timer (min):** Specifies the timer of auto channelling.
- **802.11n/EWC:** Select **disable** 802.11n or **Auto**.
- **Bandwidth:** Select the bandwidth for the network.
- **802.11n Rate/54g™ Rate:** Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **802.11n Protection:** The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without “speaking” at the same time.
- **Support 802.11n Client Only:** Only stations that are onfigured in 802.11n mode can associate.
- **Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Basic Rate:** Select the basic transmission rate ability for the AP.
- **Fragmentation Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
- **RTS Threshold:** This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
- **DTIM Interval:** (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Beacon Interval:** A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
- **XPress™ Technology:** Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The defaule is Disabled.

- **Transmit Power:** Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.
- **WMM (Wi-Fi Multimedia):** Select whether WMM is enable or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
- **WMM No Acknowledgement:** Select whether ACK in WMM packet. By default, the 'Ack Policy' for each access category is set to Disable, meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. To disable the acknowledgement can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.
- **WMM APSD:** APSD is short for automatic power save delivery, Selecting enable will make it has very low power consumption. WMM Power Save is an improvement to the 802.11e amendment adding advanced power management functionality to WMM.

Click **Save/Apply** to configure the advanced wireless options and make the changes take effect.

### 3.5 Diagnostics

Click “Diagnostics” to show the interface.

Your Router is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network		
Test your ENET(1-4) Connection:	PASS	<a href="#">Help</a>
Test your Wireless Connection:	PASS	<a href="#">Help</a>
Test the connection to your DSL service provider		
Test ADSL Synchronization:	PASS	<a href="#">Help</a>
Test ATM OAM F5 segment ping:	PASS	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping:	PASS	<a href="#">Help</a>
Test the connection to your Internet service provider		
Test PPP server connection:	PASS	<a href="#">Help</a>
Test authentication with ISP:	PASS	<a href="#">Help</a>
Test the assigned IP address:	PASS	<a href="#">Help</a>
Ping default gateway:	PASS	<a href="#">Help</a>
Ping primary Domain Name Server:	PASS	<a href="#">Help</a>

**Figure: Diagnostics page**

## 3.6 Management

### 3.6.1 Settings

#### 3.6.1.1 Settings Backup

Click the “Backup Settings”, backup the DSL router configurations.

##### Settings - Backup

Backup DSL router configurations. You may save your router configurations to a file on your PC.

Backup Settings

Figure: Backup Config

#### 3.6.1.2 Settings Update

Click the “Browsing...” button, select the correct update configure settings file. Then click the “Update Settings” to update the Router settings.

##### Tools -- Update Settings

Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:  Browse...

Update Settings

Figure : Update Settings

#### 3.6.1.3 Settings Restore Default

Click “Restore Default Settings” to restore DSL router settings to the factory defaults.

##### Tools -- Restore Default Settings

Restore DSL router settings to the factory defaults.

Restore Default Settings

Figure: Restore Default Settings

### 3.6.2 System Log

Click “System Log” to show the following interface. The system log dialog allows you to view the system log and configure the system log options.

#### System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.



**Figure: System Log overview**

Click “Configure System Log” to show the following interface. You can enable or disable the system log and then select the log level, display level and mode, and click “Apply” to end your configurations.

#### System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log:  Disable  Enable

Log Level:    
Display Level:    
Mode:

Both the log level and display level have eight choices. The default log level is “Debugging” and the default display level is “Error”.

The mode options are “Local”, “Remote”, and “Both”. The default one is “Local”.

### System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

Log:  Disable  Enable

Log Level:

Display Level:

Mode:

- Error
- Warning
- Notice
- Informational
- Debugging

**Figure: System Log Config-1**

If you select “Remote” or “Both”, all events will be transmitted to the specified UDP port of the specified log server.

### System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

Log:  Disable  Enable

Log Level:

Display Level:

Mode:

Server IP Address:

Server UDP Port:

**Figure: System Log Config-2**

After operations under “Configure System Log”, click “View System Log” to query the system logs. In this example, the “View System Log” is a system default one.

**Note:** The log and display of the system events are above the set level. If you intend to record all information, you need to set the levels as “Debugging”.

### System Log

Date/Time	Facility	Severity	Message
Jan 1 01:38:08	user	crit	kernel: ADSL G.994 training
Jan 1 01:38:16	user	crit	kernel: ADSL G.992 started
Jan 1 01:38:20	user	crit	kernel: ADSL G.992 channel analysis
Jan 1 01:38:24	user	crit	kernel: ADSL G.992 message exchange
Jan 1 01:38:25	user	crit	kernel: ADSL link up, interleaved, us=1146, ds=25505
Jan 1 01:38:26	daemon	crit	pppd[628]: PPP server detected.
Jan 1 01:38:26	daemon	crit	pppd[628]: PPP session established.
Jan 1 01:38:27	daemon	err	pppd[628]: Couldn't increase MRU to 1500
Jan 1 01:38:27	daemon	err	pppd[628]: Couldn't increase MRU to 1500
Jan 1 01:38:27	daemon	crit	pppd[628]: PPP LCP UP.
Jan 1 01:38:27	daemon	crit	pppd[628]: Received valid IP address from server. Connection UP.
Jan 1 01:38:33	daemon	err	user: tr69c: Unable to retrieve attributes in scratch PAD
Jan 1 01:38:33	daemon	err	user: Stored Parameter Attribute data is corrupt or missing

**Figure: view system event logs**

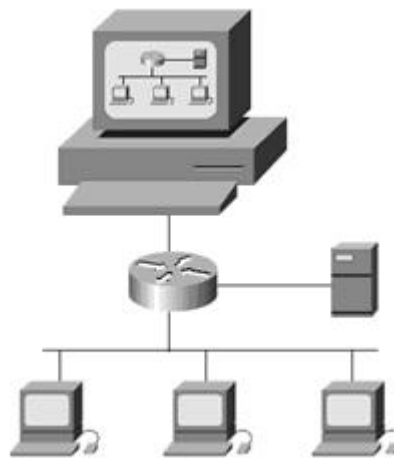
Click “Refresh” to refresh the system event logs or “Close” to exit from this interface.

### 3.6.3 SNMP Client

#### SNMP Protocol

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Two versions of SNMP exist: SNMP version 1 (SNMPv1) and SNMP version 2 (SNMPv2). Both versions have a number of features in common, but SNMPv2 offers enhancements, such as additional protocol operations. Figure 1 illustrates a basic network managed by SNMP.



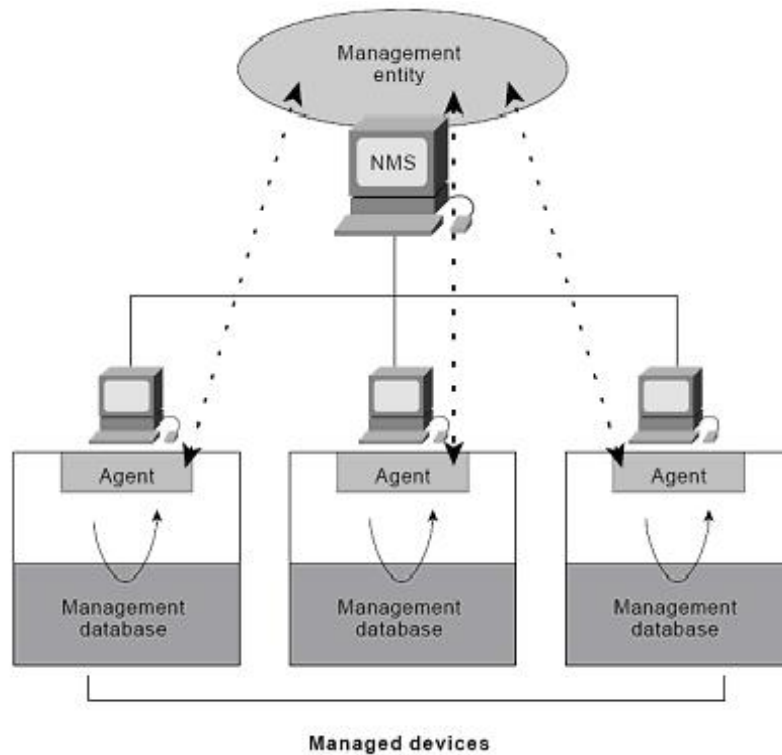
**Figure1: SNMP Facilitates the Exchange of Network Information between Devices**

An SNMP-managed network consists of three key components: managed devices, agents, and network-management systems (NMSs).

A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be routers and access servers, switches and bridges, hubs, computer hosts, or printers.

An agent is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network.



**Figure2: An SNMP-Managed Network Consists of Managed Devices, Agents, and NMSs**

Managed devices are monitored and controlled using four basic SNMP commands: read, write, trap, and traversal operations.

The **read** command is used by an NMS to monitor managed devices. The NMS examines different variables that are maintained by managed devices.

The **write** command is used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices.

The **trap** command is used by managed devices to asynchronously report events to the NMS. When certain types of events occur, a managed device sends a trap to the NMS.

Traversal operations are used by the NMS to determine which variables a managed device supports and to sequentially gather information in variable tables, such as a routing table.



### 3.6.3.1 Configure

Click “SNMP Agent” sub menu item under “Management” menu item, show figure 3 as following:

#### SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent:  Disable  Enable

Read Community:	<input type="text" value="public"/>
Set Community:	<input type="text" value="private"/>
System Name:	<input type="text" value="ADN-4000"/>
System Location:	<input type="text" value="Taiwan"/>
System Contact:	<input type="text" value="www.planet.com.tw"/>
Trap Manager IP:	<input type="text" value="0.0.0.0"/>

**Figure: SNMP Config**

Click “Enable” button to open SNMP function, and then click “Save/Apply”.

## 3.6.4 TR-69 Client Management

### TR-069 Client-configuration

Click “Management” --> “TR-069Client” to show the **TR-069 Client** configuration page.

#### TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform  Disable  Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console  Disable  Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

**Figure: TR-069 Client Configuration**

- **Inform:** IF the Enable option is selected, the CPE will accept the commands from ACS, the CPE will not accept the commands from ACS when the Disable option is selected.
- **Inform Interval:** How many seconds does the CPE inform the ACS to connect.
- **ACS URL:** input the ACS URL
- **ACS User Name:** The ACS user name is that the TR-069 Service provide to you.
- **ACS Password:** The ACS password is that the TR-069 Service provide to you.
- **Display SOAP messages on serial console:** When select Enable option, the SOAP information will display on the serial console, when select disable, it will not.
- **Connection Request Authentication:** If this checkbox is selected, you need to input the Connection Request User Name and the Connection Request Password. or you needn't to input.
- **Connection Request User Name:** the connection user name that the TR-069 Service provide to you
- **Connection Request Password:** the Connection Request Password that the TR-069 Service provide to you.
- When Click “Save/Apply”, the configuration will save and apply.

### 3.6.5 Internet Time

Click the “Internet Time”, the interface show you. In this page, the ROUTER can synchronize with Internet time servers.

#### Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

Save/Apply

Figure: Internet Time overview

After enable “Automatically synchronize with Internet time servers.” the interface shows below. Enter proper configurations, and then click “Save/Apply”.

#### Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:

Second NTP time server:

Time zone offset:

Save/Apply

Figure: Internet Time Setup

## 3.6.6 Access Control

### 3.6.6.1 Access Control – Services

Click “Access Control”-->”Services” to show the following interface. In the interface, you can enable/disable the FTP, HTTP, ICMP, SSH, TELNET and TFTP services. And the LAN side and WAN side can have different configurations.

Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

Services	LAN	WAN	WAN Port
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	2121
HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	8080
ICMP	Enable	<input type="checkbox"/> Enable	
SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	161
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	22
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	23
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	69

Save/Apply

Figure: Access Control-Services Setup

### 3.6.6.2 Access Control -- IP Addresses

Click “Access Control”-->”IP Addresses” to show the following interface.

Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

Access Control Mode:  Disable  Enable

IP Address Remove

Add Remove

Figure: Access Control-IP Addresses overview

If enabled, permits access to local management services from IP addresses contained in the Access Control List.

If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Click “add” to show the following interface. In the interface input the IP address of the management station permitted to access the local management services, and click “Save/Apply”.

#### Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address:

Save/Apply

**Figure: Access Control-IP Addresses**

### 3.6.6.3 Access Control – Passwords

Click “Access Control”-->”Passwords” to show the following interface. In the interface, you can modify the accounts passwords.

Access to your DSL router is controlled through three user accounts: **admin, support, and user**

#### Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:

Old Password:

New Password:

Confirm Password:

Save/Apply

**Figure: Password modify page**

### 3.6.7 Update Software

Click “Update Firmware” to show the following interface. In this interface, you can update the ROUTER Firmware. Click the “Browse...” button to find the right version file and press “Update Firmware” to do the update.

#### Tools -- Update Software

**Step 1:** Obtain an updated software image file from your ISP.

**Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

**Step 3:** Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

**Figure: Update Software page**

**NOTE:** Do not turn off your Router during firmware updates. When the update is finished, the Router will reboot automatically. Do not turn off your Router either before the reboot is over. You must guarantee the update software is right and accurate. It is strictly forbidden to use other software for updates.

After update software, it is suggested to restore the Router to the factory defaults and configure it again.

### 3.6.8 Save/Reboot

Click “Save/Reboot” to show the following interface. Click the “Save/Reboot” button to save and reboot the router.

Click the button below to save and reboot the router.

**Figure: Router Save/reboot page**

# Appendix A: Glossary

## **Address mask**

A bit mask select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes it called subnet mask.

## **AAL5**

ATM Adaptation Layer - This layer maps higher layer user data into ATM cells, making the data suitable for transport through the ATM network.

## **ADSL**

Asymmetric digital subscriber line

## **ATM**

Asynchronous Transfer Mode - A cell-based data transfer technique in which channel demand determines packet allocation. ATM offers fast packet technology, real time, and demand led switching for efficient use of network resources.

## **AWG**

American Wire Gauge - The measurement of thickness of a wire

## **Bridge**

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

## **Broadband**

Characteristic of any network multiplexes independent network carriers onto a single cable. Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another. Broadcast a packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

## **CO**

Central Office. Refers to equipment located at a Telco or service provider's office.

## **CPE**

Customer Premises Equipment located in a user's premises

**DHCP (Dynamic Host Configuration Protocol)**

DHCP is software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. DHCP eliminates having to manually assign permanent IP addresses to every device on your network. DHCP software typically runs in servers and is also found in network devices such as Routers.

**DMT**

Discrete Multi-Tone frequency signal modulation

**Downstream rate**

The line rate for return messages or data transfers from the network machine to the user's premises machine.

**DSLAM**

Digital Subscriber Line Access Multiplex

**Dynamic IP Addresses**

A dynamic IP address is an IP address that is automatically assigned to a client station (computer, printer, etc.) in a TCP/IP network. Dynamic IP addresses are typically assigned by a DHCP server, which can be a computer on the network or another piece of hardware, such as the Router. A dynamic IP address may change every time your computer connects to the network.

**Encapsulation**

The technique layer protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), and followed by the application protocol data.

**Ethernet**

One of the most common local area network (LAN) wiring schemes, Ethernet has a transmission rate of 10 Mbps.

**FTP**

File Transfer Protocol. The Internet protocol (and program) transfer files between hosts.

**Hop count**

A measure of distance between two points on the Internet. It is equivalent to the number of gateways that separate the source and destination.



**HTML**

Hypertext Markup Language - The page-coding language for the World Wide Web.

**HTML browser**

A browser used to traverse the Internet, such as Netscape or Microsoft Internet Explorer.

**http**

Hypertext Transfer Protocol - The protocol carry world-wide-web (www) traffic between a www browser computer and the www server being accessed.

**ICMP**

Internet Control Message Protocol - The protocol handle errors and control messages at the IP layer. ICMP is actually part of the IP protocol.

**Internet address**

An IP address is assigned in blocks of numbers to user organizations accessing the Internet. These addresses are established by the United States Department of Defense's Network Information Center. Duplicate addresses can cause major problems on the network, but the NIC trusts organizations to use individual addresses responsibly. Each address is a 32-bit address in the form of x.x.x.x where x is an eight-bit number from 0 to 255. There are three classes: A, B and C, depending on how many computers on the site are likely to be connected.

**Internet Protocol (IP)**

The network layer protocol for the Internet protocol suite

**IP address**

The 32-bit address assigned to hosts that want to participate in a TCP/IP Internet.

**ISP**

Internet service provider - A company allows home and corporate users to connect to the Internet.

**MAC**

Media Access Control Layer - A sub-layer of the Data Link Layer (Layer 2) of the ISO OSI Model responsible for media control.

**MIB**

Management Information Base - A collection of objects can be accessed via a network management protocol, such as SNMP and CMIP (Common Management Information Protocol).

**NAT**

Network Address Translation - A proposal for IP address reuse, where the local IP address is mapped to a globally unique address.

**NVT**

Network Virtual Terminal

**PAP**

Password Authentication Protocol

**PORT**

The abstraction used in Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.

**POTS**

Plain Old Telephone Service - This is the term describe basic telephone service.

**PPP**

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

**PPPoE**

PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

**Remote server**

A network computer allows a user to log on to the network from a distant location.

**RFC**

Request for Comments - Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFC can be found at [www.ietf.org](http://www.ietf.org).

**Route**

The path that network traffic takes from its source to its destination. The route a datagram may follow can include many gateways and many physical networks.

In the Internet, each datagram is routed separately.

**Router**

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

**Routing Table**

Information stored within a router that contains network path and status information. It is used to select the most appropriate route to forward information along.

**Routing Information Protocol**

Routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

**SNMP**

Simple Network Management Protocol - The network management protocol of choice for TCP/IP-based Internet.

**SOCKET**

- (1) The Berkeley UNIX mechanism for creating a virtual connection between processes.
- (2) IBM term for software interfaces that allow two UNIX application programs to talk via TCP/IP protocols.

**Spanning-Tree Bridge Protocol (STP)**

Spanning-Tree Bridge Protocol (STP) - Part of an IEEE standard. A mechanism for detecting and preventing loops from occurring in a multi-bridged environment.

When three or more LAN's segments are connected via bridges, a loop can occur. Because of a bridge forwards all packets that are not recognized as being local, some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

## **Spoofing**

A method of fooling network end stations into believing that keep alive signals have come from and returned to the host. Polls are received and returned locally at either end

## **Static IP Address**

A static IP address is an IP address permanently assigned to computer in a TCP/IP network. Static IP addresses are usually assigned to networked devices that are consistently accessed by multiple users, such as Server PCs, or printers. If you are using your Router to share your cable or DSL Internet connection, contact your ISP to see if they have assigned your home a static IP address. You will need that address during your Router's configuration.

## **Subnet**

For routing purposes, IP networks can be divided into logical subnets by using a subnet mask. Values below those of the mask are valid addresses on the subnet.

## **TCP**

Transmission Control Protocol - The major transport protocol in the Internet suite of protocols provides reliable, connection-oriented full-duplex streams.

## **TFTP**

Trivial File Transfer Protocol. A simple file transfer protocol (a simplified version of FTP) that is often boot diskless workstations and other network devices such as routers over a network (typically a LAN).

## **Telnet**

The virtual terminal protocol in the Internet suite of protocols - Allows users of one host to log into a remote host and act as normal terminal users of that host.

## **Transparent bridging**

The intelligence necessary to make relaying decisions exists in the bridge itself and is thus transparent to the communicating workstations. It involves frame forwarding, learning workstation addresses, and ensuring no topology loops exist (in conjunction with the Spanning-Tree algorithm).

## **UDP**

User Datagram Protocol - A connectionless transport protocol that runs on top of TCP/IP's IP. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagram without acknowledgments or guaranteed delivery. Best suited for small, independent requests, such as requesting a MIB value from an SNMP agent, in which first

setting up a connection would take more time than sending the data.

### **UNI signaling**

User Network Interface signaling for ATM communications.

### **Virtual Connection (VC)**

A link that seems and behaves like a dedicated point-to-point line or a system that delivers packets in sequence, as happens on an actual point-to-point network. In reality, the data is delivered across a network via the most appropriate route. The sending and receiving devices do not have to be aware of the options and the route is chosen only when a message is sent. There is no pre-arrangement, so each virtual connection exists only for the duration of that one transmission.

### **WAN**

Wide area network - A data communications network that spans any distance and is usually provided by a public carrier (such as a telephone company or service provider)



## EC Declaration of Conformity

For the following equipment:

\*Type of Product : 802.11n Wireless ADSL 2/2+ 4-Port Router  
\*Model Number : ADN-4000  
\* Produced by:  
Manufacturer's Name : **Planet Technology Corp.**  
Manufacturer's Address : 9F, No. 96, Min Chuan Road, Hsin Tien,  
Taipei, Taiwan, R.O.C.

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to 1999/5/EC R&TTE. For the evaluation regarding the R&TTE the following standards were applied:

EN 300 328 V1.7.1	(2006-05)
EN 301 489-1 V1.6.1	(2005-09)
EN 301 489-17 V1.2.1	(2002-08)
EN60950-1	(2001 + A11: 2004)
EN50385	(2002)

Responsible for marking this declaration if the:

Manufacturer     Authorized representative established within the EU

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **9F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname : **Allen Huang**

Position / Title : **Product Manager**

Taiwan  
Place

15<sup>th</sup>, Sep., 2009  
Date

Allen  
Legal Signature

**PLANET TECHNOLOGY CORPORATION**

e-mail: sales@planet.com.tw    http://www.planet.com.tw

11F, No. 96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C. Tel:886-2-2219-9518 Fax:886-2-2219-9528