

# User's Manual

## PENTAGRAM Cerberus ADSL2 Wi-Fi Plus (P6331-6)



*The latest versions of manual, drivers and applications are available on  
[www.pentagram.eu](http://www.pentagram.eu)*

2008-10-09

**NOTE!** Any information and technical data are subject to change without prior notification and/or indication in this manual.

© **2007 PENTAGRAM**

All rights reserved; copying and reproduction is strictly forbidden.

# INDEX

INTRODUCTION .....	5
FEATURES .....	5
PACKAGE CONTENTS .....	7
PRODUCT OVERVIEW .....	7
IMPORTANT NOTES .....	7
FRONT PANEL .....	7
BACK PANEL .....	8
DEFAULT SETTINGS .....	8
RESETTING ROUTER .....	9
CONNECTING CERBERUS TO COMPUTER .....	9
CONFIGURE TCP/IP .....	9
CONFIGURE ROUTER VIA WEB BROWSER .....	14
LOGIN .....	14
NAVIGATION .....	15
STATUS TAB .....	16
QUICK START TAB .....	20
CONFIGURATON TAB .....	22
SAVE CONFIGURATION TO FLASH TAB .....	60
RESTART TAB .....	60
TROUBLESHOOTING .....	61
USING LEDS TO DIAGNOSE PROBLEMS .....	61
PROBLEMS WITH THE WEB INTERFACE .....	61
PROBLEMS WITH THE LOGIN USERNAME AND PASSWORD .....	62
PROBLEMS WITH LAN INTERFACE .....	62
PROBLEMS WITH WAN INTERFACE .....	62
PROBLEMS WITH THE INTERNET ACCESS .....	63



## **Introduction**

Thank you for purchasing the Cerberus ADSL2 Wi-Fi Plus (P 6331-6) ADSL2+ Modem/Router by PENTAGRAM. Your new router is an all-in-one unit that combines an ADSL modem, ADSL router, Ethernet network switch and wireless Access Point to provide everything you need to get the machines on your network connected to the Internet over an ADSL broadband connection.

The Cerberus ADSL2 Wi-Fi Plus (P 6331-6) router complies with ADSL2+ standards for deployment worldwide and supports downstream rates of up to 24 Mbps and upstream rates of up to 1 Mbps. Designed for small office, home office and residential users, the router enables even faster Internet connections. You can enjoy ADSL services and broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever before.

## **Features**

- A 4-port 10/100Mbps fast Ethernet switch is built-in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports, with auto detection allowing you to use either straight or cross-over Ethernet cables.
- With built-in 802.11g access point for extending the communication media to WLAN while providing the WEP, WPA/WPA2 and WDS for securing your wireless networks.
- Network Address Translation (NAT) allows multiple users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateways (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.
- This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors, and it makes setting up a network simple and affordable. UPnP architecture leverages TCP/IP and the Web to enable proximity networking in addition to control and data transfer among networked devices. With this feature enabled, you can seamlessly connect to Net Meeting or MSN Messenger.
- The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. To use the service, you must first apply for an account from a DDNS service such as <http://www.dyndns.org/>.
- The Cerberus ADSL2 Wi-Fi Plus (P6311-6) provides an embedded PPPoE client function to establish a connection. You get greater access speed without changing the operation concept, while sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are also provided.
- Virtual Server: You can specify which services are visible to outside users. The router detects an incoming service request and forwards it to the specific local computer for handling. For example, you can assign a PC in a LAN to act as a Web server inside and expose it to the outside network. Outside users can browse inside the web server directly while it is protected by NAT. A DMZ host setting is also provided for local computers exposed to the outside Internet network.

- Dynamic Host Configuration Protocol (DHCP) Client and Server: On a WAN site, the DHCP client obtains an IP address from the Internet Service Provider (ISP) automatically. On a LAN site, the DHCP server allocates a range of client IP addresses, including subnet masks and DNS IP addresses and distributes them to local computers. This provides an easy way to manage the local IP network.
- Static and RIP1/2 Routing: An easy static routing table or RIP1/2 routing protocol supports routing capability.
- SNMP (Simple Network Management Protocol): SNMP allows convenient remote management of the router.
- Web-based GUI: A web-based GUI offers easy configuration and management. User-friendly and with on-line help, it also supports remote management capability for remote users to configure and manage this product.
- Firmware Upgradeable: You can upgrade the router with the latest firmware through its web-based GUI.
- Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management information move through the router at lightning speed, even under heavy load. The QoS features are configurable by source IP address, destination IP address, protocol, and port. You can throttle the speed at which different types of outgoing data pass through the router, to ensure P2P users don't saturate upload bandwidth, or office browsing doesn't bring client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.
- High Speed Internet Access: downstream rates of up to 24Mbps and upstream rates of up to 1Mbps. Cerberus ADSL2 Wi-Fi Plus (P6311-6) is compliant with the following standards:
  - ANSI T1.413 issue 2,
  - ITU-T G.992.1 (G.dmt),
  - ITU-T G.992.2 (G.lite),
  - ITU-T G.992.3 (ADSL2 G.dmt.bis),
  - ITU-T G.992.5 (ADSL2+),
  - ITU-T G.994.1 (G.hs),
  - Reach Extended ADSL (RE ADSL).
- Multi-Protocol to Establish a Connection: The router supports following protocols to establish a connection with an ISP:
  - PPPoA (PPP over ATM Adaptation Layer 5 – RFC 2364),
  - PPPoE (PPP over Ethernet – RFC 2516)
  - RFC 1483/2684 encapsulation over ATM (bridged or routed),The router also supports VC-based and LLC-based multiplexing.

## Package Contents

1. PENTAGRAM Cerberus ADSL2 Wi-Fi Plus (P6331-6)
2. Power adapter 12 V, 1 A
3. Ethernet cable (RJ-45)
4. Telephone cable (RJ-11)
5. CD
6. Quick Installation Guide

## Product Overview

### Important Notes

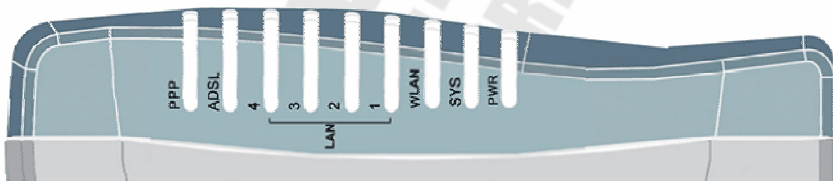


- Do not use the router in high humidity or high temperatures.
- Do not use the same power source for the router as other equipment.
- Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.



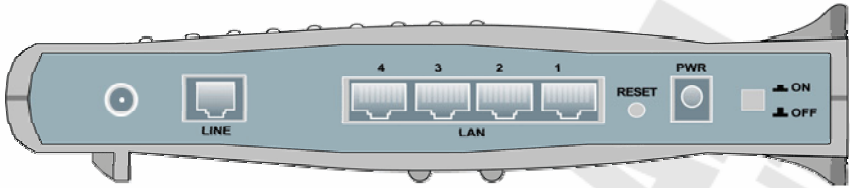
- Avoid using this product and all accessories outdoors.
- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

### Front Panel



LED	Action	Description
<b>PWR</b>	Off	No power is supplied to the device
	Steady light	Connected to an AC power supply
<b>SYS</b>	Steady light	System is ready
	Off	Access point is disabled
<b>WLAN</b>	Steady light	Access point is enabled
	Blinking light	Transmitting/Receiving data
<b>LAN (1-4)</b>	Off	No Ethernet connection
	Steady light	Connected to an Ethernet port
	Blinking light	Transmitting/Receiving data
<b>ADSL</b>	Off	No ADSL signal
	Steady light	ADSL signal is established
	Blinking Light	Establishing ADSL signal
<b>PPP</b>	Steady light	PPPoA / PPPoE connection established

## Back Panel



Label	Used for...
RP-SMA Connector	Connecting the external antenna
LINE (RJ-11)	Connecting the telephone cable
LAN 1-4 (RJ-45)	Connecting with computers/devices through Ethernet cable
RESET	Resetting the device.
PWR	Connecting with supplied power adapter
ON/OFF	Switching the device on/off

## Default Settings

Before changing configuration familiarize yourself with these default settings.

IP Address	192.168.1.100
Subnet Mask	255. 255. 255.0
SSID	Pentagram P 6331-6
DHCP Server	Enabled
DHCP Server IP Address Pool	100 IP addresses from 192.168.1.101
IP Address Lease Time	43200 seconds (12 hours)
User Name	<b>admin</b>
Password	<b>pentagram</b>

It is recommended to set username and password as soon as possible.

If you ever forget the password to log in, you may need to reset router to restore the factory default settings. This procedure is described on the next page.

## **Resetting router**

- Turn router on and wait about 2 minutes for router initialization.
- Hold the **RESET** button until the LEDs all turn Off, turn On and then turn Off. The router performs configuration factory reset and the router reboots. You can then access the router from the web GUI.

## **Connecting Cerberus to Computer.**

Cerberus can be connected to computer via Ethernet or WLAN:

### **Connecting via Ethernet Port (Ethernet Card)**

All Ethernet ports of router are made in the technology, which automatically activates Crossover if necessary. Thanks to autonegotiation of connection speed the router will automatically select the maximum available speed rate. Transfer at 10/100 Mbit/s rate requires the category 5 cable wired with RJ-45 connectors. In case of "straight" cable both connectors must be crimped in standard EIA/TIA 568B. In case of Crossover cable one connector must be in standard EIA/TIA 56A, and the second in EIA/TIA 568B. After connecting the device to one of the ports, corresponding LED will begin to blink. That signals the process of the auto-checking of port and the negotiation of connection speed rate.

### **Connecting via WLAN Interface (Wireless Card)**

To connect PC to Cerberus via WLAN, Wireless Adapter must be properly installed and configured and both router and PC must be in the same subnet.

## **Configure TCP/IP**

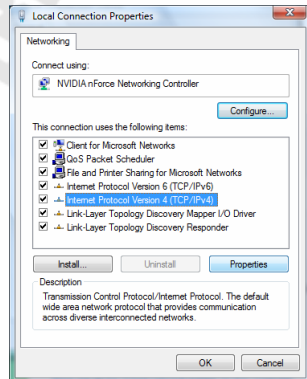
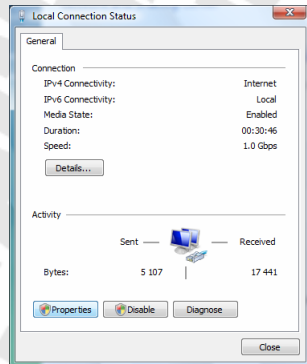
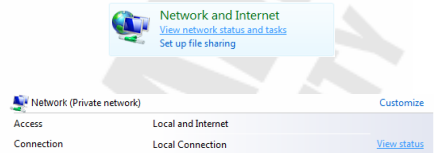
After connecting the computer to the router (by LAN adapter or WLAN interface) the TCP/IP protocol should be configured. The protocol should be automatically installed together with Network card drivers. It is advised that TCP/IP should be configured to receive IP address and all the necessary network parameters from DHCP server automatically. You can find step-by-step configuration for different Windows systems below.

**Note:** In some cases computer with Windows Vista or Windows XP SP3 cannot obtain an IP address from router's DHCP server. If you encounter this, follow this steps to resolve this problem (Microsoft Support page) <http://support.microsoft.com/kb/928233/en-us> (this article may be not available in user language).

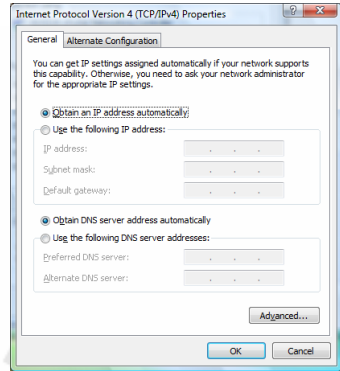
## Windows Vista

**Note:** Network configuration require administrator privileges. When *User Account Control* window pops up, either click Continue (Administrator user) or select Administrator user and enter valid password (Standard user).

1. Click **Start** → **Control Panel**.
2. Click **View network status and tasks**.
3. Click **View status** for appropriate connection.
4. On **General** tab, Click the **Properties** button.
5. On **General** tab, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

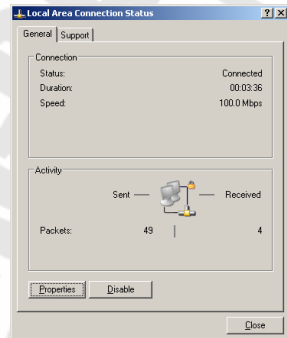
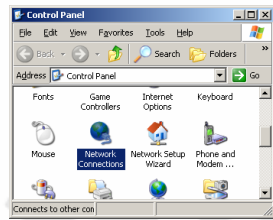


6. On **General** tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
7. Click **OK** to save settings and close **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

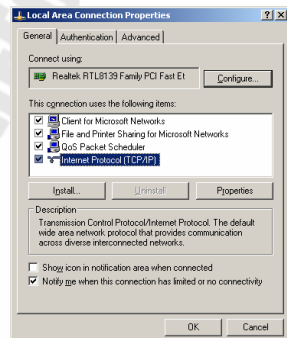


## Windows 2000/XP

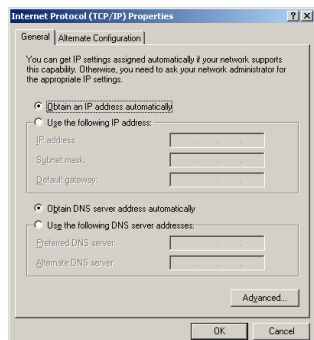
1. Click **Start** → **Settings** → **Control Panel**.  
Double-click the **Network Connections** icon (2000/XP Classic view) or click **Network and Internet Connections** icon and then **Network Connections** icon (XP Default view).
2. Double-click the **Local Area Connection** icon.
3. On **General** tab, Click the **Properties** button.



4. On **General** tab, select **Internet Protocol (TCP/IP)** and click **Properties**.

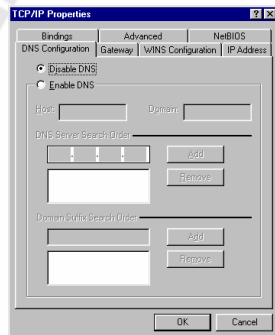
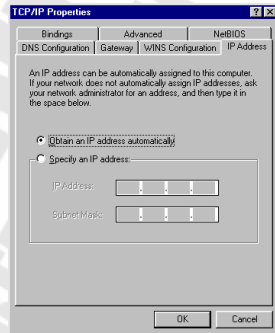
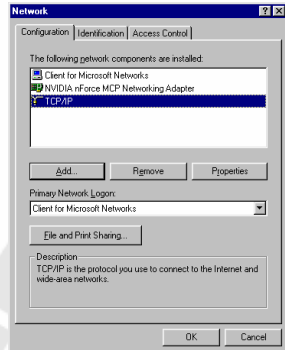


5. On **General** tab, select **Obtain an IP address automatically** and **DNS server address automatically**.
6. Click **OK** to save settings and close **Internet Protocol (TCP/IP) Properties** window.



## Windows 95/98/Me

1. Click **Start** → **Settings** → **Control Panel**. Double-click the **Network** icon.
2. On **Configuration** tab, select **TCP/IP** for appropriate network adapter and click **Properties**.
3. On **IP Address** tab, select **Obtain an IP address automatically**.
4. On **DNS Configuration** tab, select **Disable DNS**.
5. Click **OK** to save settings and close **TCP/IP Properties** window.



To make sure that network adapter properly obtained an IP address from router's DHCP server:

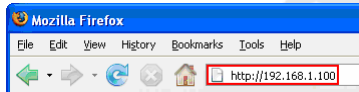
1. click **Start > Run**
2. type **cmd** (Win 2000/XP) or **command** (Win 95/98/ME) and press Enter
3. in command line type **ipconfig /all** and press Enter
4. check if the **IP Address** is **192.168.1.x**

## ***Configure router via web browser***

Cerberus ADSL2 Wi-Fi Plus (P6331-6) router can be configured via web browser, which is usually integrated with operating system. Router offers clear and simple interface.

### ***Login***

1. Launch the Web browser
2. In address bar enter the default IP address: **http://192.168.1.100**



3. Enter username and password – default **admin / pentagram**

## Navigation

**PENTAGRAM**  
THE PERFECT SIMPLICITY

**ADSL Firewall Router**

Pentagram Cerberus  
P 6331-6

**Status**

**Device Information**

Model Name	Pentagram Cerberus P 6331-6
Host Name	home.gateway
System Up-Time	2 hour(s) 29 min(s)
Current Time	Tue Sep 18 15:19:20 2007
Hardware Version	TRENDCHIP TC3162
Software Version	1.35-RC33-180-80.3
Bootrom Version	1.06
MAC Address	00:04:ed:60:1c:08
Home URL	PENTAGRAM

**LAN**

IP Address	192.168.1.100
SubNetmask	255.255.255.0
DHCP Server	DHCP Server Running

**WAN**

ipwan	PPPoA VC-Mux
VPI / VCI	0 / 35
Connection	Connecting
IP Address	
Netmask	
Gateway	
Primary DNS	

**Port Status**

Port	Ethernet	ADSL	Wireless
Connected	✓	✗	✓

SAVE CONFIG RESTART

### Buttons

- **Save Settings** – Opens Save Config to FLASH page.
- **Restart Router** – Opens Restart page.

### Tabs

The web interface includes the following tabs:

- **Status (ARP Table, Wireless Association, Routing Table, DHCP Table, System Log, Security Log)**
- **Quick Start**
- **Configuration (LAN, WAN, System, Firewall, QoS, Virtual Server, Advanced)**
- **Save Config to FLASH**

## Status Tab

Status			
<b>Device Information</b>			
Model Name	Pentagram Cerberus P 6331-6		
Host Name <a href="#">▶</a>	home.gateway		
System Up-Time	2 hour(s) 29 min(s)		
Current Time <a href="#">▶</a>	Tue Sep 18 15:19:20 2007		
Hardware Version	TRENDCHIP TC3162		
Software Version	1.35-RC33-180-80.3		
Bootrom Version	1.06		
MAC Address	00:04:ed:60:1c:08		
Home URL	<a href="#">PENTAGRAM</a>		
<b>LAN</b>			
IP Address <a href="#">▶</a>	192.168.1.100		
SubNetmask	255.255.255.0		
DHCP Server <a href="#">▶</a>	DHCP Server Running		
<b>WAN</b>			
ipwan <a href="#">▶</a>	PPPoA VC-Mux		
VPI / VCI	0 / 35		
Connection	Connecting		
IP Address			
Netmask			
Gateway			
Primary DNS <a href="#">▶</a>			
<b>Port Status</b>			
Port	Ethernet	ADSL <a href="#">▶</a>	Wireless <a href="#">▶</a>
Connected	✓	✗	✓

### Device Information

- **Host Name** – Provide a name for the router for identification purposes. Host Name lets you change the router name.

Host Name	
Device Host Name	
Host Name	<input type="text" value="home.gateway"/>
<input type="button" value="Apply"/>	

- **System Up-Time** – Records system up-time.
- **Current Time** – Set the current time. See the Time Zone section for more information.
- **Hardware Version** – Chipset version
- **Software Version** – Firmware version
- **LAN MAC Address** – The LAN MAC address
- **WAN MAC Address** – The WAN MAC address
- **Home URL** – Connects to the Home Website.

### LAN

- **IP Address** – LAN port IP address.
- **Sub Net Mask** – LAN port IP subnet mask.
- **DHCP Server** – LAN port DHCP role - Server, Relay or None.

**WAN**

- **IP WAN** – Name of the WAN connection.
- **VPI/VCI** – Virtual Path Identifier and Virtual Channel Identifier
- **Connection** – Selects “Disconnected” or “Connected”
- **IP Address** – WAN port IP address.
- **Net mask** – WAN port IP subnet mask.
- **Gateway** – The IP address of the default gateway.

**Port Status**

User can look up for your connected condition

**Status / ARP Table**

The router's ARP (Address Resolution Protocol) Table shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is a quick way to determine the MAC address of the network interface of your PCs to use with the router's **Firewall – MAC Address Filter** function. See the Firewall section of this manual for more information.

ARP Table			
IP <-> MAC List			
IP Address	MAC Address	Interface	Static
192.168.1.101	00:0E:2E:00:11:5F	iplan	No
192.168.1.102	00:0C:76:73:00:51	iplan	No

- **IP Address** – A list of IP addresses of devices on your LAN (Local Area Network).
- **MAC Address** – MAC (Media Access Control) address for each device on your LAN.
- **Interface** – The interface name (on the router) that this IP Address connects to.
- **Static** – Static status of the ARP table entry:  
**no** for dynamically-generated ARP table entries  
**yes** for static ARP table entries added by the user

**Status / Wireless Association**

Wireless Association Table	
Wireless client's MAC address and the corresponding IP address	
IP Address	MAC
192.168.1.101	00:0E:2E:00:11:5F

**IP Address** – It is IP Address of wireless client that join this network.

**MAC** – The MAC address of wireless client.

## Status / Routing Table

Routing Table						
Routing Table						
#	Destination	Netmask	Gateway/Interface	Cost		
1	239.255.255.250	255.255.255.255	0.0.0.0/iplan	0	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶
2	192.168.1.0	255.255.255.0	0.0.0.0/iplan	0	<a href="#">Edit</a> ▶	<a href="#">Delete</a> ▶

[Create](#) ▶

---

Static Route						
Add Rule3						
Destination	<input type="text"/>					
Netmask	<input type="text"/>					
Gateway	<input type="text"/>		Interface	<input type="text" value="Please Select"/>		
Cost	<input type="text" value="0"/>					

# – Item number

**Destination** – IP address of the destination network.

**Netmask** – The destination netmask address.

**Gateway/Interface** – IP address of the gateway or existing interface that this route uses.

**Cost** – The cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.

**Interface** – Select the interface through which packets are forwarded.

## Status / DHCP Table

DHCP Table			
Leased Table			
IP Address	MAC Address	Client Host Name	Register Time
192.168.1.101	00:0e:2e:00:11:5f	PENTLAB_05	2000/01/01 02:29:32 - 2000/01/01 14:29:32
192.168.1.102	00:0c:76:73:00:51	PENTLAB_02	2000/01/01 00:49:25 - 2000/01/01 12:49:25

**Leased** – DHCP assigned IP addresses information.

**IP Address** – IP addresses of devices on your LAN (Local Area Network).

**MAC Address** – The MAC Address that you want to assign the fixed IP address

**Client Host Name** – Expired IP addresses information

**Register Time** – Register time information

## Status / System Log

Display system logs accumulated up to the present time. You can trace historical information with this function.

**System Log**

Current Time: Sat Jan 1 03:06:57 2000

If you would like to save the log to a text file, right click [here](#) and select "Save Target As ..."

Refresh Clear

## Status / Security Log

This screen displays security log information. If a hacker attacks your server, he is isolated by the firewall function and the router records related information. This helps you know where the hacker comes from.

**Security Log**

Current Time: Sat Jan 1 03:07:15 2000

If you would like to save the log to a text file, right click [here](#) and select "Save Target As ..."

Refresh Clear

## Quick Start Tab

For detailed instructions on configuring WAN settings, see the **WAN** section of this manual.

The information you need for the Quick Start wizard to get you online are your login (often in the form of username@ispname), your password, and the encapsulation type.

Your ISP can supply all the details you need. Alternatively, if you have deleted the current WAN Connection in the **WAN – ISP** section of the interface, you can use the router's PVC Scan feature to determine the Encapsulation types offered by your ISP.

Quick Start		Built-In Known Profile for IP TV / VOD applications	
<b>Connection</b>			
Encapsulation	PPPoA VC-Mux	Auto Scan	
VPI	0		
VCI	35		
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
<b>Optional Settings</b>			
IP Address	0.0.0.0	(0.0.0.0 means 'Obtain an IP address automatically')	
SubnetNetmask	0.0.0.0		
Default Gateway	0.0.0.0		
<b>DNS</b>			
Obtain DNS automatically	<input checked="" type="checkbox"/> Enable		
Primary DNS			
Secondary DNS			
<b>PPP</b>			
Username			
Password			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

## Connection

**Encapsulation** – Select the encapsulation type your ISP uses or choose **Auto Scan**.

Auto Scan	
Before you scan the PVCs, please DELETE all the WAN interfaces.	
IP Address	if provided by ISP
Gateway	if provided by ISP
<input type="button" value="Start"/> <input type="button" value="Cancel"/>	

Click **Start** to begin scanning for encapsulation types offered by your ISP. If the scan is successful, you are presented with a list of supported options.

**VCI** – Enter the VCI assigned to you. This field may already be configured.

**VPI** – Enter the VPI assigned to you. This field may already be configured.

**NAT** – Select “Enabled” or “Disabled”.

## Optional Setting

**IP Address** – Type your ISP assigned IP address in the IP Address text box.

**Subnet Mask** – Enter a subnet mask in dotted decimal notation.

**Default Gateway** – You must specify a gateway IP address (supplied by your ISP)

## DNS

**Obtain DNS automatically** – Select this check box to use DNS.

**Primary DNS** – Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

**Secondary DNS** – Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

## PPP

**Username** – Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is usually in the format of “username@ispname” instead of simply “username”.

**Password** – Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).



## Configuraton Tab

Click this item to access the following sub-items that configure the ADSL router: **LAN, WAN, System, Firewall, QoS, Virtual Server** and **Advanced**. These functions are described in the following sections.

### Configuration / LAN (Local Area Network)

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building. There are four items within the LAN section: **Ethernet, Wireless, Wireless Security** and **DHCP Server**.

- **Ethernet**

The router supports two Ethernet IP addresses in the LAN, and two different LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN, so there is no need to configure a Secondary IP address. The default IP address for the router is 192.168.1.254.

Ethernet	
<b>Primary IP Address</b>	
IP Address	192.168.1.100
SubnetNetmask	255.255.255.0
RIP	Disable
<b>Secondary IP Address</b>	
The Secondary IP Address should be on the same subnet as the Primary IP Address and uses the same Subnet Mask.	
IP Address	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**RIP** – RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

**Note:** The Subnet mask of the Secondary IP Address depends on the setting of the Primary IP Address.

- **Wireless**

Wireless	
<b>Parameters</b>	
WLAN service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	802.11b+g
ESSID	Pentagram P 6331-6
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Regulation Domain	Europe
Channel ID	Channel 1 (2.412 GHz)
WMM (QoS)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM-APSD	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MAC Address	00:13:D3:71:CD:86
AP Version	RT2561T 1.0.8.0-3
<b>Wireless Distribution System (WDS)</b>	
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
1.Peer WDS MAC Address	
2.Peer WDS MAC Address	
3.Peer WDS MAC Address	
4.Peer WDS MAC Address	
** WDS depends on the settings of main security encryption type. **	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Mode** – 802.11b+g (Mixed mode), 802.11b and 802.11g. The factory default is 802.11b+g.

**ESSID** – Enter the unique ID given to the Access Point (AP), which is already built-in to the router's wireless interface. To connect to this device, your wireless clients must have the same ESSID as the device.

**Regulation Domain** – There are five Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

**Channel ID** – Select the ID channel that you would like to use.

**MAC Address** – The AP's MAC Address

**AP Version** – The Access Point firmware version.

### Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed simply define peer's MAC address of the connected AP. WDS takes advantages of cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

In addition, WDS enhances its link connection security in WEP mode, WEP key encryption must be the same for both access points.

**WDS Service** – The default setting is Disable. Check Enable radio button to activate this function.

**Peer WDS MAC Address** – It is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.

**Note:** For MAC Address, Semicolon (;) must be included

- **Wireless Security**

You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **disabled**.

Wireless Security	
Parameters	
Security Mode	Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

### WPA Pre-Shared Key

Wireless Security	
Parameters	
Security Mode	WPA Pre-Shared Key
WPA Algorithm	TKIP
WPA Shared Key	0000000000
Group Key Renewal	3600 Seconds
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**WPA Algorithms** – TKIP (Temporal Key Integrity Protocol) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

**WPA Shared Key** – The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

**Group Key Renewal** – The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

### WPA2 Pre-Shared Key

Wireless Security	
Parameters	
Security Mode	WPA2 Pre-Shared Key
WPA2 Algorithm	TKIP
WPA2 Shared Key	0000000000
Group Key Renewal	3600 Seconds
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**WPA2 Algorithms** – TKIP (Temporal Key Integrity Protocol) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

**WPA2 Shared Key** – The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

**Group Key Renewal** – The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

**WEP**

Wireless Security	
Parameters	
Security Mode	WEP
WEP Authentication	Open System
WEP Encryption	HEX <input checked="" type="radio"/> WEP64 <input type="radio"/> WEP128
Default Used WEP Key	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4
Key 1	0000000000
Key 2	0000000000
Key 3	0000000000
Key 4	0000000000
Passphrase	<input type="text"/> <input type="button" value="Generate Key"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**WEP Encryption** – To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP. If you require high security for transmissions, there are two alternatives to select from: **WEP 64** and **WEP 128**. WEP 128 will offer increased security over WEP 64.

**Passphrase** – This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. You can input the same string in both the AP and Client card settings to generate the same WEP keys. Please note that you do not have to enter **Key (1-4)** as below when the **Passphrase** is enabled..

**Key (1-4)** – Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for WEP64 and WEP128 respectively, the separator is “-“. For example, using WEP64, 11-22-33-44-55 is a valid key, whilst 1122334455 is invalid.

**Hide ESSID** – User can select Enable or Disable to hide ESSID.

- DHCP Server**

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

DHCP Server	
Configuration	
DHCP Server Mode	<input type="radio"/> Disable <input checked="" type="radio"/> DHCP Server <input type="radio"/> DHCP Relay Agent
<input type="button" value="Next"/>	

DHCP Server Status	
Status	DHCP Server Running
Subnet Definitions	
Subnet Value	192.168.1.0
SubnetNetmask	255.255.255.0
Domain Name	home.gateway
DNS Server	192.168.1.100
Maximum/Default Lease Time	86400 / 43200 seconds
IP Range	192.168.1.100 - 192.168.1.199

## Cerberus ADSL2 Wi-Fi Plus (P6331-6)

To disable the router's DHCP Server, check **Disabled** and click **Next** then click **Apply**. When the DHCP Server is disabled you need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (the default is 192.168.1.254).

**DHCP**  
**Disable server and relay agent**  
The DHCP server and relay agent will be disabled.

To configure the router's DHCP Server, check **DHCP Server** and click **Next**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check **Use Router as a DNS Server**, the ADSL Router performs the domain name lookup, finds the IP address from the outside network automatically and forwards it back to the requesting PC in the LAN (your Local Area Network).

**DHCP SERVER**  
**Parameters**

Domain Name	home.gateway
Use Router as DNS Server	<input checked="" type="checkbox"/>
Primary DNS Server Address	192.168.1.100
Secondary DNS Server Address	
Default Lease Time	43200 seconds
Maximum Lease Time	86400 seconds
Range Start	192.168.1.101
Range End	192.168.1.200
TFTP Server Name(Option 66)	

  
**Specify fixed Mac Address Mapping to fixed IP Address (optional)**  
**\*Please note that the IP Address can only be set within the IP Range Start and IP Range End specified above in the DHCP SERVER Parameters**

	Host Name	MAC Address	IP Address
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

The MAC address is represented as a string of 2 digit hexadecimal numbers separated by colons (:) - ( eg. 00:11:22:33:44:55 )

If you check **DHCP Relay Agent** and click **Next** then you must enter the IP address of the DHCP server which assigns an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click **Apply** to enable this function.

**DHCP Relay**

Parameters

DHCP Relay Server	<input type="text"/>
-------------------	----------------------



## Configuration / WAN (Wide Area Network)

A WAN (Wide Area Network) is an outside connection to another network or the Internet. There are three items within the WAN section: **ISP**, **DNS** and **ADSL**.

- **ISP**

The factory default is PPPoA. If your ISP uses this access protocol, click **Edit** to input other parameters as below. If your ISP does not use PPPoA, you can change the default WAN connection entry by clicking **Change**.

A simpler alternative is to select **Quick Start** from the main menu on the left. See the **Quick Start** section of the manual for more information.

Main WAN Connection						
Main WAN Connection Configuration						
Name	Description	Creator	VPI	VCI		
PPPoA.Routed	PPPoA	admin	0	35	<a href="#">Edit</a>	<a href="#">Change</a>

Changing wan service will save your configuration to flash and immediately restart the router.

Other WAN Bridge Connection						
Bridged WAN connection List						
Name	Description	Creator	VPI	VCI		
<a href="#">Create</a>						

Built-In Known Profile for IP TV / VOD applications
0: Standard Default;Auto PVC, WAN-DHCP, LAN NAT -DHCP
<a href="#">Apply</a> <a href="#">Cancel</a>

Changing IP TV / VOD type will save your configuration to flash and immediately restart the router.

## RFC 1483 Routed Connections

WAN Connection		
RFC 1483 Routed		
Description	1483_Routed_mode	
VPI	0	
VCI	35	
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Encapsulation Method	LLC Bridged	
IP Assignment	<input checked="" type="radio"/> Obtain an IP address automatically via DHCP client	
	<input type="radio"/> Use the following IP address	
	IP Address	
	Netmask	
RIP	Gateway	
	Disable	
<a href="#">Apply</a> <a href="#">Cancel</a>		

**Description** – Your description of this connection.

**VPI / VCI** – Enter the information provided by your ISP.

**NAT** – The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

**Encapsulation method** – Select the encapsulation format, the default is LLC Bridged. Select the one provided by your ISP.

**DHCP client** – Enable or disable the DHCP client, specify if the router can get an IP address from the Internet Service Provider (ISP) automatically or not.

**Obtain an IP address automatically via DHCP client** to enable the DHCP client function or click Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.

**RIP** – RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

## PPPoA Routed Connections

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP.

WAN Connection	
PPPoA Routed	
Description	PPPoA
VPI	0
VCI	35
Encapsulation Method	VcMux
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	
Password	
IP Address	0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')
Authentication Protocol	Auto
Connection	Always On
RIP	Disable
MTU	1472
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Description** – User-definable name for the connection.

**VPI / VCI** – Enter the information provided by your ISP.

**NAT** – The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

**Username** – Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

**Password** – Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

**IP Address** – Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

**Authentication Protocol Type** – Default is **Chap (Auto)**. Your ISP advises you whether to use **Chap** or **Pap**.

**Connection** – If you want the router to establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.

**RIP** – RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

**MTU** – Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that the IP attempts to send through the interface.

## PPPoE Routed Connections

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.

WAN Connection	
PPPoE Routed	
Description	PPPoE
VPI	0
VCI	35
Encapsulation Method	LLC
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	
Password	
Service Name	
IP Address	0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')
Authentication Protocol	Auto
Connection	Always On
Idle Timeout	10 minutes
RIP	Disable
MTU	1472
PPPoE Relay	<input type="checkbox"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Description** – A user-definable name for this connection.

**VPI / VCI** – Enter the information provided by your ISP.

**NAT** – The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

**Username** – Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

**Password** – Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

**Service Name** – This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is 20 alphanumeric characters.

**IP Address** – Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

**Authentication Protocol** – Default is Chap. Your ISP advises on using Chap or Pap.

### Connection:

- **Always on** – If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.
- **Connect on Demand** – If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

**Idle Timeout** – Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

**RIP** – RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

**MTU** – Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

## RFC 1483 Bridged Connections

WAN Connection	
RFC 1483 Bridged	
Description	1483_Bridged_mode
VPI	0
VCI	35
ATM Class	UBR
PCR	0
SCR	0
MBS	0
Encapsulation Method	LLC Bridged
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Description** – A user-definable name for this connection.

**VPI / VCI** – Enter the information provided by your ISP.

**Encapsulation method** – Select the encapsulation format, this is provided by your ISP.

- **DNS**

DNS	
Parameters	
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable
Primary DNS	
Secondary DNS	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as *www.pentagram.eu* and an IP address. An IP address is a 32-bit number in the form of xxx.xxx.xxx.xxx, for example 192.168.1.254. You can think of an IP address as a telephone number for devices on the Internet, and the DNS allows you to find the telephone number for any particular domain name. Since an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP has provided it when you logon. Usually when you choose PPPoE or PPPoA as your WAN – ISP protocol, the ISP provides the DNS IP address automatically. You may leave the configuration field blank. Alternatively, your ISP may provide you with an IP address of their DNS. If this is the case, you must enter the DNS IP address.

If you choose one of the other protocols, RFC1483 Routed or Bridged, check with your ISP, as it may provide you with an IP address for their DNS server. You must enter the DNS IP address if you set the DNS Server address on your PC to the LAN IP address of this router.

- **ADSL**

ADSL	
Parameters	
ADSL Mode	Annex A
Modulator	ADSL Multimode
DSP FirmwareVersion	DMT FwVer: 3.5.18.0_A_TC, HwVer:T14F7_1.0
DMT Status	Down
Operational Mode	-----
Upstream	0 kbps
Downstream	0 kbps
Noise Margin (Upstream)	N/A (ADSL is not UP)
Noise Margin (Downstream)	N/A (ADSL is not UP)
Attenuation (Upstream)	N/A (ADSL is not UP)
Attenuation (Downstream)	N/A (ADSL is not UP)
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>	

**ADSL Mode** – There are four modes **Open Annex Type** and **Follow DSLAM's Setting, Annex A, Annex L, Annex M and Annex J** that user can select for this connection.

**Modulator** – There are four modes **AUTO, ADSL multimode, ADSL2 and ADSL2+** that user can select for this connection.

**DSP Firmware Version** – DSP code version

**DMT Status** – DMT Status

**Operational Mode** – To show the state when user select "AUTO" on connect mode.

**Annex Type** – To show the router's type, e.g. Annex A, Annex B

**Upstream** – Upstream rate

**Downstream** – Downstream rate

**Noise Margin / Attenuation** – Characteristics of ADSL line.

## Configuration / System

There are six items within the System section: **Time Zone**, **Remote Access**, **Firmware Upgrade**, **Backup/Restore**, **Restart** and **User Management**.

- **Time Zone**

Time Zone	
Parameters	
Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Local Time Zone (+GMT Time)	(GMT+01:00)Sarajevo, Skopje, Sofija, Warsaw, Zagreb
SNTP Server IP Address	192.43.244.18
	128.138.140.44
Daylight Saving	<input checked="" type="checkbox"/> Automatic
Resync Period	1440 minutes
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, the router retrieves the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

**Resync Period** (in minutes) is the periodic interval the router waits before it resynchronizes the router's time with that of the specified SNTP server. To avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

- **Remote Access**

Remote Access	
Remote Access Control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Allowed Access IP Address Range	from <input type="text"/> to <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

To temporarily permit remote administration of the router (i.e. from outside your LAN), select a time period the router permits remote access for and click **Enable**. You may change other configuration options for the web administration interface using **Device Management** options in the **Advanced** section of the GUI.

- **Firmware Upgrade**

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified. Your router allows you to upgrade the software it runs to take advantage of these changes. Clicking on **Browse** allows you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.

Firmware Upgrade	
You may upgrade the system software on your network device	
After upgrading, let your router restart with current settings or factory default settings	
Restart Router with	<input checked="" type="radio"/> Factory Default Settings <input type="radio"/> Current Settings
New Firmware Image	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Upgrade"/> <input type="button" value="Cancel"/>	

**Restart Router with** – To choose **Factory Default Setting** or **Current Settings** that user want.

**New Firmware Image** – Type in the location of the file you wish to upload in this field or click **Browse...** to find it.

**Browse...** – Click **Browse...** to find the .afw file you wish to upload. Remember that you must decompress compressed (.zip) files before you can upload them.

**Upgrade** – Click upgrade to begin the upload process. This process may take up to two minutes.

**Warning: DO NOT power down the router or interrupt the firmware upgrade while it is still in process. Improper operation may damage the router.**

- **Backup / Restore**

Backup/Restore	
Allows you to backup the configuration settings to your computer, or restore configuration from your computer.	
Backup Configuration	
Backup configuration to your computer.	
<input type="button" value="Backup"/>	
Restore Configuration	
Configuration File	<input type="text"/> <input type="button" value="Browse..."/>
<small>"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.</small>	
<input type="button" value="Restore"/>	

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.

Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using

the **current version** of the router's firmware. **Settings files saved to your PC should not be manually edited in any way.**

Select the settings files you wish to use, and press **Restore** to load those settings into the router.

- **Restart Router**

Click Restart with option Current Settings to reboot your router and restore your last saved configuration.

Restart	
After restarting, Please wait for several seconds to let the system	
Restart Router with	<input type="radio"/> Save Config to FLASH <input checked="" type="radio"/> Current Settings <input type="radio"/> Factory Default Settings
<input type="button" value="Restart"/> <input type="button" value="Cancel"/>	

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings.

You may also reset your router to factory settings by pressing in the small Reset pinhole button on the back of your router for 10-12 seconds while the router is turned on.

- **User Management**

User Management			
Current Defined Users			
Valid	User		
True	admin	<a href="#">Edit</a>	
<a href="#">Create</a>			

To prevent unauthorized access to your router's configuration interface, all users are required to login with a password. You can set up multiple user accounts, each with their own password.

You are able to **Edit** existing users and **Create** new users who are able to access the device's configuration interface. Once you have clicked on **Edit**, you are shown the following options:

User Management	
Edit	
Username	admin
Password	*****
Valid	True
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

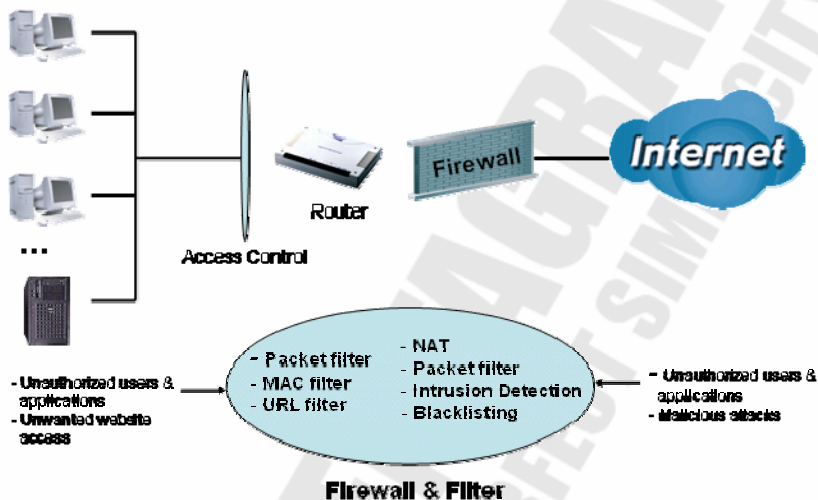
You can change the user's **password**, whether their account is active and **Valid**, as well as add a comment to each user account. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however you can delete any other created accounts by clicking **Cancel** when editing the user.

You are strongly advised to change the password on the default "admin" account when you receive your router, and any time you reset your configuration to Factory Defaults.

## Configuration / Firewall

### Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet. See the **WAN** configuration section for more details on NAT.



**Firewall** – Prevents access from outside your network. The router provides three levels of security support:

**NAT natural firewall** – This masks LAN users’ IP addresses, which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when the NAT function is enabled.

**Note:** *When using Virtual Servers (port forwarding) your PCs are exposed to the degree specified in your Virtual Server settings provided the ports specified are opened in your firewall packet filter settings.*

**Firewall Security and Policy (General Settings)** – Inbound direction of Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet.

**Intrusion Detection** – Enable Intrusion Detection to detect, prevent, and log malicious attacks.

**MAC Filter rules** – Prevents unauthorized computers accessing the Internet.

**URL Filter** – Blocks PCs on your local network from unwanted websites.

A detailed explanation of each of the following five items appears in the **Firewall** section below: **Packet Filter**, **Ethernet MAC Filter**, **Wireless MAC Filter**, **Intrusion Detection**, **Block WAN Request** and **URL Filter**.

## ● Packet Filter

Packet filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. This configuration program allows you to set up to 6 different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is “**or**” operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action is taken.

Packet Filter							
Default Rules		Forward ▾					
Parameters							
Name	Application Type	Active	Flow	Packet Type	Action	Log	Schedule Time
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>							
Default Rules Drop mode cannot be enabled without any rules. Doing so could block all access to the Internet.							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>							

**Add** – Click this button to add a new packet filter rule and the next figure appears.

**Edit** – Check the Rule No. you wish to edit, and then click “Edit”.

**Delete** – Check the Rule No. you wish to delete, and then click “Delete”.

Packet Filter (Application Based)			
Parameters			
Application Type	User Defined ▾ (You may select a predefined packet filtering profile for a well-known application here.)		
Parameters			
Name	APPL1	Packet Flow	<input type="radio"/> Outgoing(Local to Remote) <input checked="" type="radio"/> Incoming(Remote to Local)
Active	Yes ▾	Packet Type	Any ▾
Log	No ▾	Action When Matched	Drop ▾
Local Machine IPs	from	to	
Remote Machine IPs	from	to	
Local Application Ports	from	to	
Remote Application Ports	from	to	
Schedule Time	<input checked="" type="radio"/> Always <input type="radio"/> Schedule from 08 ▾ : 00 ▾ to 18 ▾ : 00 ▾ <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat		
<input type="button" value="Return"/> <input type="button" value="Cancel"/>			

**Application** – User can choose they want.

**Packet Flow** – Determine whether the rule is for outgoing packets or for incoming packets.

**Active** – Choose **Yes** to enable the rule, or choose **No** to disable the rule.

**Packet Type** – Specify the packet type (TCP, UDP, ICMP or any) that the rule applies to. Select **TCP** if you wish to search for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to search for the connectionless application service on the remote server using the port number.

**Log** – Choose **Yes** if you wish to generate logs when the filter rule is applied to a packet.

**Action When Matched** – If a packet matches this filter rule, **Forward** or **Drop** this packet.

**Source IP Address** – Enter the incoming or outgoing packet’s source IP address(es).

**Source Port** – Check the TCP or UDP packet’s source port number(s).

**Destination IP Address** – Enter the incoming or outgoing packet's destination IP address(es).

**Destination Port** – Check the TCP or UDP packet's destination port number(s).

**Schedule time** – User can setup the time to use the packet filter.

**Attention:** *If the DHCP server option is enabled, you must be very careful in assigning IP addresses of a filtered private IP range to avoid conflicts because you do not know which PC in the LAN is assigned which IP address. The easiest and safest way is that the filtered IP address is assigned to a specific PC that is not allowed to access an outside resource such as the Internet. You configure the filtered IP address manually for this PC, but it stays in the same subnet with the router.*

- **Ethernet MAC Filter**

A Ethernet MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the switch to only accept traffic from specified machines, or else to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules; you can add the filter rules to meet your requirements.

**Ethernet MAC Filter**

Default Rules **Forward** ▾

Parameters

Rule No.	Active	Action	Log	MAC Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

**Ethernet MAC Filter**

Default Rules **Forward** ▾

Parameters

Rule No.	Active	Action	Log	MAC Address
1	Yes	Drop	Yes	00:0C:76:73:00:51
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

**MAC Filter**

Parameters

Rule 1

Active	Yes ▾
Action When Matched	Drop ▾
Log	Yes ▾
Mac Address	<input type="text"/> Candidates ▶

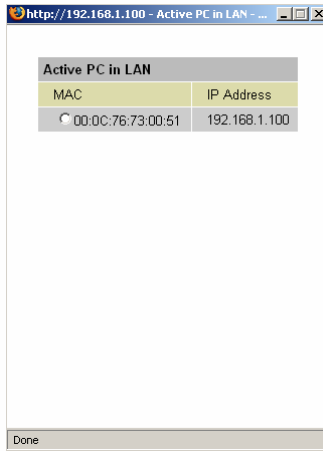
**Active** – Select Yes from the drop down list box to enable MAC address filtering.

**Action When Matched** – Select **Drop** or **Forward**.

**Log** – Choose **Yes** if you wish to generate logs when the filter rule is applied to a packet.

**MAC Address** – Enter the MAC addresses you wish to manage.

**Candidates** – it automatically detects devices connected to the router through the Ethernet.



- Wireless MAC Filter**

The MAC Address supports up to 30 wireless network machines and helps you to manage your network control to accept traffic from specific authorized machines or to restrict unwanted machine(s) to access your LAN.

There are no pre-define MAC Address filter rules; you can add the filter rules to meet your requirements

**Wireless MAC Filter**

Default Rules

Parameters

	Rule No.	Active	Action	Log	MAC Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

**Wireless MAC Filter**

Default Rules

Parameters

	Rule No.	Active	Action	Log	MAC Address
<input checked="" type="checkbox"/>	1	Yes	Drop	Yes	00:0E:2E:00:11:5F
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

MAC Filter	
Parameters	
Rule 1	
Active	Yes ▾
Action When Matched	Drop ▾
Log	Yes ▾
Mac Address	<input type="text"/> Candidates ▶
<input type="button" value="Return"/> <input type="button" value="Cancel"/>	

**Active** – Select Yes from the drop down list box to enable MAC address filtering.

**Action When Matched** – Select **Drop** or **Forward**.

**Log** – Choose **Yes** if you wish to generate logs when the filter rule is applied to a packet.

**MAC Address** – Enter the MAC addresses you wish to manage.

**Candidates** – it automatically detects devices connected to the router through the Ethernet.

## • Intrusion Detection

Check **Enable** if you wish to detect intruders accessing your computer without permission. The router automatically detects and blocks a DoS (Denial of Service) attack if a user enables this function. This kind of attack is not to access confidential data on the network; instead, it aims to disrupt specific equipment or the entire network. If this happens, users are not able to access network resources.

Intrusion Detection	
Parameters	
Intrusion Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Alert Mail	<input type="checkbox"/>
Alert Mail Time	30 minutes
Your E-mail(Must be xxx@yyy.zzz)	<input type="text"/>
Recipient's E-mail(Must be xxx@yyy.zzz)	<input type="text"/>
SMTP server	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Intrusion Detection** – Check **Enable** if you wish to detect intruders accessing your computer without permission.

**Alert Mail** – Select this check box to use Alert Mail.

**Alert Mail Time** – Set the time for receiving Alert mail.

**Your E-Mail** – Set your email address.

**Recipient's E-mail** – Set the Recipient's email address to which the e-mail notification is sent.

**SMTP server** – Set the SMTP (mail) server address.

## • Block WAN Request

Check **Enable** if you wish to exclude outside PING requests from reaching this router.

Block WAN Request	
Parameters	
Block WAN Request	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**URL Filter**

URL (Uniform Resource Locator – e.g. an address in the form of http://www.pentagram.eu or http://www.example.com) filter rules allow you to prevent users on your network from accessing particular websites from their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.

URL Filter								
	Rule No.	Active	PC IPs		Block Mode	Keywords Filtering	Domains Filtering	Restrict URL Features
			from	to				
<input checked="" type="radio"/>	1	Yes	192.168.1.101	192.168.1.200	Always Block	Disable	Disable	Block Java Applet, Cookies
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>								
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

URL Filter	
<b>Parameters</b>	
Rule 1	Active <input type="text" value="Yes"/>
<b>PC IP Address Range</b>	
from	<input type="text"/> to <input type="text"/>
Block Mode	<input checked="" type="radio"/> Always Block <input type="radio"/> Block from <input type="text" value="08"/> : <input type="text" value="00"/> to <input type="text" value="18"/> : <input type="text" value="00"/> <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
Keywords Filtering	<input type="checkbox"/> Enable <input type="button" value="Details"/>
Domains Filtering	<input type="checkbox"/> Enable <input type="button" value="Details"/>
Restrict URL Features	<input type="checkbox"/> Block Java Applet <input type="checkbox"/> Block ActiveX <input type="checkbox"/> Block Cookies <input type="checkbox"/> Block Proxy
<input type="button" value="Return"/> <input type="button" value="Cancel"/>	

**Active** – Select **Yes** from the drop down list box to enable or disable the URL Filter feature.

**Always Block** – Select to always check URL filter rules (i.e. at all hours of the day).

**Block from** – Specify the time period to check URL filter rules (e.g. during work hours).

**Keywords Filtering** – Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called "advertisement.gif"). When enabled, your specified keywords list is checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only. For example, the URL http://www.abc.com/abcde.html would be dropped since the keyword "abcde" occurs in the URL.

Keywords Filtering	
<b>Create</b>	
Keyword	<input type="text"/>
<input type="button" value="Apply"/>	
<b>Block WEB URLs which contain these keywords</b>	
Name	Keyword
<input type="button" value="Return"/>	

**Domains Filtering** – Checks the domain name in URLs accessed against your list of domains to block or allow. If it matches, the URL request is sent (Trusted) or dropped (Forbidden). The checking procedure is:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, it is checked with the forbidden list. If present, the connection attempt is dropped.
3. If the packet matches neither of the above, it is sent to the remote web server.
4. Please note that only the domain is specified, not the full URL. For example to block traffic to [www.sex.com](http://www.sex.com), enter “sex” or “sex.com” instead of “www.sex.com”. In the example below, the URL request for [www.abc.com](http://www.abc.com) is sent to the remote web server because it is listed in the trusted list, while the URL request for [www.sex.com](http://www.sex.com) or [www.sex.com](http://www.sex.com) is dropped because [sex.com](http://sex.com) is in the forbidden list.

Domains Filtering		
Create		
Domain Name	<input type="text"/>	
<input type="button" value="Apply"/>		
Forbidden Domains		
Name	Domain	
item1	sex	<input type="button" value="Delete"/>
<input type="button" value="Return"/>		

#### Restrict URL Features

- **Block Java Applet** – Blocks Web content which includes the Java Applet to prevent someone who wants to damage your system via the standard HTTP protocol.
- **Block ActiveX** – Blocks ActiveX
- **Block Cookies** – Blocks Cookies
- **Block Proxy** – Blocks Proxy

## Configuration / QoS (Quality of Service)

### Quality of Service Introduction

If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in PENTAGRAM's routers is such a breakthrough for home users and office users.

### QOS: Keeping Your Net Connection Fast and Responsive

Configurable by source IP address, destination IP address, protocol, and port, the Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring bandwidth-consumption data like gaming packets, latency-sensitive application like voice, or even mission critical files, move through the router at lightning speed, even under heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

### QOS Setup

Please choose the **QOS** in the **Configuration** item of the left window as depicted below.

QoS			
<b>Maximum ISP Bandwidth</b>			
Type:	Auto(ADSL Sync. Rate)	Upstream(LAN->WAN): 0 Kbps	Downstream(WAN->LAN): 0 Kbps
<b>QoS Rule List</b>			
	Application	Time Schedule	Direction
			Assigned Bandwidth Ratio
<b>Non-Assigned Bandwidth Ratio</b>			
Rate Type:	Fixed (Maximum)	LAN to WAN : 100%	WAN to LAN : 100%
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

After clicking the QOS item, you can Add/Edit/Delete a QOS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

QoS			
<b>Maximum ISP Bandwidth</b>			
Type:	Auto(ADSL Sync. Rate)	Upstream(LAN->WAN): 0 Kbps	Downstream(WAN->LAN): 0 Kbps
<b>QoS Rule List</b>			
	Application	Time Schedule	Direction
			Assigned Bandwidth Ratio
<input type="radio"/>	P2TP	Always On	LAN to WAN
			20% Minimum Guaranteed Rate with High priority
<input type="radio"/>	VoIP	Always On	LAN to WAN
			20% Minimum Guaranteed Rate with High priority
<input type="radio"/>	FTP Server	Always On	LAN to WAN
			20% Fixed Rate
<b>Non-Assigned Bandwidth Ratio</b>			
Rate Type:	Fixed (Maximum)	LAN to WAN : 40%	WAN to LAN : 100%
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

**Application** – A name that identifies an existing policy.

**Time Schedule** – Scheduling your QOS policy to be applied.

**Direction** – The traffic flow direction to be controlled by the QOS policy.

There are two settings to be provided in the Router:

- **LAN to WAN** – You want to control the traffic flow from the local network to the outside world. E.g., you have a FTP server inside the local network and you want to have a limited traffic rate controlled by the QOS policy. So, you need to add a policy with LAN to WAN direction setting.
- **WAN to LAN** – Control Traffic flow from the WAN to LAN. The connection maybe either issued from LAN to WAN or WAN to LAN.)

**Assigned Bandwidth Ratio** – This field shows the assigned bandwidth ratio in percentage for a QOS policy. If WAN connection to internet is established, the estimated transfer rate will be shown in kbps. You may specify a fixed transfer rate or Minimum Guaranteed Rate with priority for non-used bandwidth.

**Non-Assigned Bandwidth Ratio** – This field shows the available bandwidth ratio, for LAN to WAN and WAN to LAN, that has not yet assigned.

**Add** – Press this button to add a new QOS policy.

**Edit / Delete** – Before using these buttons to edit or delete a policy, please select one policy you want to edit/delete from the radio option.

**Apply** – After you have configured the policies, you can press this button to apply the configuration. If you want to make the change persistent in flash, choose **Save Config to Flash** in the left windows to save it into flash.

When you press **Add** or **Edit** buttons described above, the following page will show up in your browser. You can use it to define a QOS policy.

QoS	
Parameters	
Controlled Traffic Flow	<input checked="" type="radio"/> LAN to WAN <input type="radio"/> WAN to LAN
Application	FTP Server
Packet Type	TCP
Assigned Data Rate	Rate Type: Fixed (Maximum) Data Ratio: 20 % Priority for Non-used Bandwidth: Normal
DSCP Marking LAN to WAN	Disabled
Local Machine IPs	from 192.168.1.1 to
Remote Machine IPs	from to
Local Application Ports	from to
Remote Application Ports	from to
Schedule Time	<input checked="" type="radio"/> Always <input type="radio"/> Schedule from 08 : 00 to 18 : 00 <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
<input type="button" value="Return"/> <input type="button" value="Cancel"/>	

**Controlled Traffic Flow** – Specify the traffic flow you want to control. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

**Packet type** – The packet type will be controlled. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

- **ANY** – No specified protocol type is specified.
- **TCP**
- **UDP**
- **ICMP**
- **GRE** – For PPTP VPN Connections.

**Assigned Data rate** – Assign the data ratio for this policy to be controlled. For examples, we want to only allow 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is  $20\% \times 256 \times 0.9 = 46$  kbps. (For 0.9

is an estimated factor for the effective data transfer rate for a ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8).

**Data Ratio** – percentage for the data rate to be controlled by this policy. As above FTP server examples, it is 20.

**Rate Type** – We provide 2 types here:

- **Fixed (Maximum):** specify a fixed data rate for this policy. It also is the maximal rate for this policy. As above FTP server example, you may want to “throttle” the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.
- **Guaranteed (Minimum):** specify a minimal data rate for this policy. For example, you want to provide a guaranteed data rate for your outside customers to access your internal FTP server with, say at least, 20% of your total bandwidth. You can use this type. Then, if there is available bandwidth that is not used, it will be given to this policy by following priority assignment.

**Priority for Non-used Bandwidth** – Specify the priority for the bandwidth that is not used. For examples, you may specify two different QOS policies for different applications. Both applications need a minimal bandwidth and need more bandwidth, beside the assigned one, if there is any available/non-used one available. So, you may specify which application can have higher priority to acquire the non-used bandwidth.

- **High**
- **Normal** – The default is normal priority.
- **Low**

For the sample priority assignment for different policies, it is saved in a First-In-First-Out way.

**DSCP Marking** – Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify traffic based on DSCP value and send packets to next Router.

DSCP Mapping Table	
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

**Local Machine IPs** – The IP address values for Local LAN machines you want to control. (For IP packets from LAN to WAN, it is the source IP address. For IP packages from WAN to LAN, it is the destination IP address.)

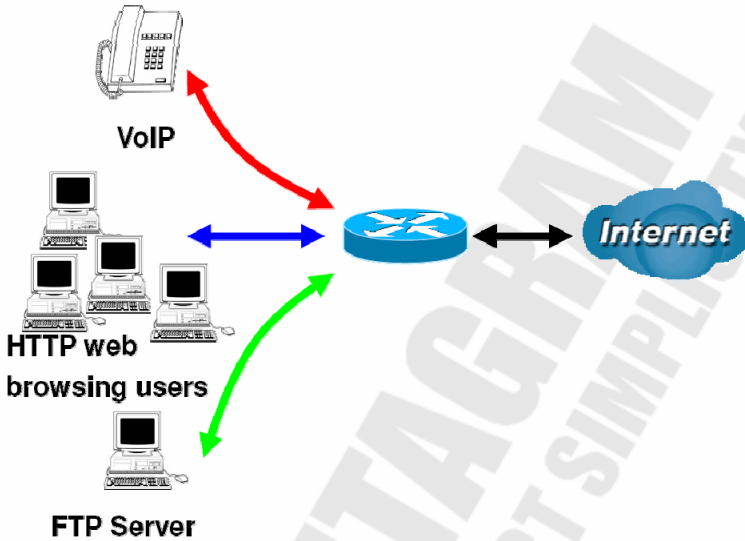
**Remote Machine IPs** – The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

**Local Application Ports** – The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)

**Remote Application Ports** – The Application port values for remote machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the destination port value. For TCP/UDP packets from WAN to LAN, it is the source port value.)

**Schedule Time** – Schedule your QOS policy.

**QOS example for your Network**  
**Connection Diagram**



**ADSL Subscription Rate**  
 Upstream: 256 kbps  
 Downstream: 2048 Mbps

**Example QOS Plan**

Application	IP or Ports	Control Flow	Data Rate	Time Schedule
VoIP User	192.168.1.1	Outgoing	Minimal 20% with high priority for non-used bandwidth with SDCP marking Class 1 Gold Service	Always
FTP Sever	192.168.1.100	Incoming and Outgoing	Outgoing: minimal 30%. Data rate. Incoming: minimal 30%. Data rate. Both with low priority for non-used bandwidth.	Only Working Hours 9:00 to 17:00 Monday to Friday.
HTTP web browsing users	80	Incoming and Outgoing	Outgoing : limited 20%. Data rate. Incoming: limited 30%. Data rate.	Always

## Example QoS Setup

QoS				
<b>Maximum ISP Bandwidth</b>				
Type:	Auto(ADSL Sync. Rate) ▾	Upstream(LAN->WAN): 0 Kbps	Downstream(WAN->LAN): 0 Kbps	
<b>QoS Rule List</b>				
	Application	Time Schedule	Direction	Assigned Bandwidth Ratio
<input type="radio"/>	VoIP	Always On	LAN to WAN	20% Minimum Guaranteed Rate with High priority
<input type="radio"/>	FTP_Server_Out	Day Time	LAN to WAN	30% Minimum Guaranteed Rate with Low priority
<input type="radio"/>	FTP_Server_In	Day Time	WAN to LAN	30% Minimum Guaranteed Rate with Low priority
<input type="radio"/>	HTTP_Browsing_Out	Always On	LAN to WAN	20% Fixed Rate
<input type="radio"/>	HTTP_Browsing_In	Always On	WAN to LAN	30% Fixed Rate
<b>Non-Assigned Bandwidth Ratio</b>				
Rate Type:	Fixed (Maximum) ▾	LAN to WAN : 30%	WAN to LAN : 40%	
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

- **VoIP application**

Voice is latency-sensitive application. Most VoIP devices are use SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.

QoS	
<b>Parameters</b>	
Controlled Traffic Flow	<input checked="" type="radio"/> LAN to WAN <input type="radio"/> WAN to LAN
Application	VoIP
Packet Type	Any ▾
Assigned Data Rate	Rate Type: Guaranteed (Minimum) ▾ Data Ratio: 20 % Priority for Non-used Bandwidth: High ▾
DSCP Marking LAN to WAN	Gold service(L) ▾
Local Machine IPs	from 192.168.1.1 to
Remote Machine IPs	from to
Local Application Ports	from to
Remote Application Ports	from to
Schedule Time	<input checked="" type="radio"/> Always <input type="radio"/> Schedule from 08 : 00 to 18 : 00 <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
<input type="button" value="Return"/> <input type="button" value="Cancel"/>	

Above settings will help to improve quality of your VoIP service when traffic is full loading.

- **FTP Server Application**

Some of companies will setup FTP server for customer downloading or home user sharing their files by using FTP.

LAN to WAN direction:

QoS			
Parameters			
Controlled Traffic Flow	<input type="radio"/> LAN to WAN <input type="radio"/> WAN to LAN		
Application	FTP_Server_Out		
Packet Type	Any		
Assigned Data Rate	Rate Type: Guaranteed (Minimum)	Data Ratio: 30 %	Priority for Non-used Bandwidth: Low
DSCP Marking LAN to WAN	Disabled		
Local Machine IPs	from 192.168.1.100	to	
Remote Machine IPs	from	to	
Local Application Ports	from	to	
Remote Application Ports	from	to	
Schedule Time	<input type="radio"/> Always		
	<input checked="" type="radio"/> Schedule from	08	: 00 to 18 : 00
<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat			
Return		Cancel	

WAN to LAN direction:

QoS			
Parameters			
Controlled Traffic Flow	<input type="radio"/> LAN to WAN <input checked="" type="radio"/> WAN to LAN		
Application	FTP_Server_In		
Packet Type	Any		
Assigned Data Rate	Rate Type: Guaranteed (Minimum)	Data Ratio: 30 %	Priority for Non-used Bandwidth: Low
DSCP Marking LAN to WAN	Disabled		
Local Machine IPs	from 192.168.1.100	to	
Remote Machine IPs	from	to	
Local Application Ports	from	to	
Remote Application Ports	from	to	
Schedule Time	<input type="radio"/> Always		
	<input checked="" type="radio"/> Schedule from	08	: 00 to 18 : 00
<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat			
Return		Cancel	

With above settings that help to limit utilization of upstream of FTP. Time schedule also help you to only limit utilization at day time.

- HTTP Web Browsing**

You can control the internet web browsing by specify the HTTP 80 (8080 for some proxy server).

LAN to WAN direction:

QoS			
Parameters			
Controlled Traffic Flow	<input checked="" type="radio"/> LAN to WAN <input type="radio"/> WAN to LAN		
Application	HTTP_Browsing_Out		
Packet Type	Any		
Assigned Data Rate	Rate Type: Fixed (Maximum)	Data Ratio: 20 %	Priority for Non-used Bandwidth: Normal
DSCP Marking LAN to WAN	Disabled		
Local Machine IPs	from	to	
Remote Machine IPs	from	to	
Local Application Ports	from	to	
Remote Application Ports	from 80	to	
Schedule Time	<input checked="" type="radio"/> Always		
	<input type="radio"/> Schedule from	08 : 00 to 18 : 00	
<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat			
Return		Cancel	

WAN to LAN direction:

QoS			
Parameters			
Controlled Traffic Flow	<input type="radio"/> LAN to WAN <input checked="" type="radio"/> WAN to LAN		
Application	HTTP_Browsing_In		
Packet Type	Any		
Assigned Data Rate	Rate Type: Fixed (Maximum)	Data Ratio: 30 %	Priority for Non-used Bandwidth: Normal
DSCP Marking LAN to WAN	Disabled		
Local Machine IPs	from	to	
Remote Machine IPs	from	to	
Local Application Ports	from	to	
Remote Application Ports	from 80	to	
Schedule Time	<input checked="" type="radio"/> Always		
	<input type="radio"/> Schedule from	08 : 00 to 18 : 00	
<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat			
Return		Cancel	

## Configuration / Virtual Server

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as "well-known ports". Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

The reason is that when using NAT, your publicly accessible IP address is used by and points to your router, which needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for information on NAT.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and are designated as "well-known ports". The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports, or private ports, are numbered from 49152 through 65535. Examples of well-known and registered port numbers are shown below, for further information, please see IANA's website at: <http://www.iana.org/assignments/port-numbers>

### Well-known and Registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Virtual Server						
Parameters						
Item	Type	Public Port Start	Public Port End	Mapped Private IP Address	Mapped Private Port	
1	TCP	23	23	192.168.1.2	23	
2	UDP	500	500	192.168.1.68	500	

DMZ  Enable
 DMZ IP Address:

**Item** – Item number

**Type** – Select TCP if you wish to search for connection-based application services on the remote server using the port number.

**Port Start & Port End** – Enter the public port number & range you wish to configure. IP Address: Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

**Add** – Click to add a new virtual server rule. Click again and the next figure appears.

**Edit** – Check the Rule No. you wish to edit and then click “Edit”.

**Delete** – Check the Rule No. you wish to delete, then click “Delete”.

Virtual Server	
Parameters	
Item	1
Service select	User Defined
Protocol	User Defined
Public Start Port	FTP (TCP:21)
Public End Port	SSH (TCP:22)
Mapped Private IP Address	Telnet (TCP:23)
Mapped Private Port	SMTP (TCP:25)
	HTTP (TCP:80)
	POP3 (TCP:110)
	NNTTP (TCP:119)
	NTP (TCP:123)
	HTTFS (TCP:443)
	IKE (UDP:500)
	T.120 (TCP:1503)
	H.323 (TCP:1720)
	PPTP (TCP:1723)

(Leave blank or input 0 indicating Virtual Server Service.)

**Item** – Item number

**Service select** – Select the service you wish to configure

**Protocol** – Automatic when you choose Service select

**Start Port & End Port** – Enter the public port number & range you wish to configure.

**IP Address** – Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

Since NAT acts as a “natural” Internet firewall, your router protects your network from access by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request to the router for a specified port is received, it is forwarded to the corresponding internal server.

For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

Virtual Server						
Parameters						
	Item	Type	Public Port Start	Public Port End	Mapped Private IP Address	Mapped Private Port
☺	1	TCP	80	80	192.168.1.2	80

In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by the particular application. Most applications use TCP or UDP, however you can specify other protocols using the drop-down **Protocol** menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

**DMZ** – The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets are checked by the Firewall and NAT algorithms, then passed to the DMZ host when a packet received does not use a port number in use by any other Virtual Server entries.

**Note:** *Using port forwarding does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for “All” protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.*

**Attention:** *If you disable the NAT option in the WAN-ISP section, the Virtual Server function becomes invalid.*

**Attention:** *If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign a static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.*

## Configuration / Advanced

Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

There are six items within the Advanced section: **Static Route**, **Static ARP**, **Dynamic DNS**, **VLAN Control**, **Device Management** and **IGMP**.

- **Static Route**

Click on **Static Route** and then choose **Create** to add a routing table.

Static Route					
Static Routing					
#	Valid	Destination	Netmask	Gateway/Interface	
Create					
Static Route					
Add Rule1					
Destination					
Netmask					
Gateway				Interface	Please Select ▾
Cost	0				
Apply Cancel					

**Destination** – The destination subnet IP address.

**Netmask** – Subnet mask of the destination IP addresses based on above destination.

**Gateway** – The gateway IP address to which packets are forwarded.

**Interface** – Select the interface through which packets are forwarded.

**Cost** – Represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.

- **Static ARP**

Click on **Static ARP** and then choose **Create** to add a static ARP table.

Static ARP			
Static ARP			
#	IP Address	MAC Address	
Create			
Static ARP			
Add Entry1			
IP Address		MAC_Address	
Apply Cancel			

Enter **IP Address** and **MAC\_Address** of host which will be added to static ARP table.

## • Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

You first need to register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>

Dynamic DNS	
Parameters	
Dynamic DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Dynamic DNS Server	<input type="text" value="www.dyndns.org (custom)"/>
Wildcard	<input type="checkbox"/> Enable
Domain Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Period	<input type="text" value="28"/> <input type="text" value="Day(s)"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

There are more than 5 DDNS services supported.

**Disable** – Check to disable the Dynamic DNS function.

**Enable** – Check to enable the Dynamic DNS function. The fields following are activated and required.

**Dynamic DNS Server** – Select the DDNS service you have established an account with.

**Host** – Enter one domain name you have registered.

**Domain Name, Username and Password** – Enter your registered domain name and your username and password for this service.

**Period** – Set the time period between updates, for the router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router performs an update when your dynamic IP address changes.

**Wildcard** – Select this check box to enable the DYNDNS Wildcard.

- **VLAN Control**

VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment. While clients and servers may be located anywhere on a network, they are grouped together by VLAN technology, and broadcasts are sent to devices within the VLAN.

#### VLAN Group Control

Parameters									
	VLAN Group Name	VLAN ID	Ethernet port #1	Ethernet port #2	Ethernet port #3	Ethernet port #4	wireless LAN	Link VLAN Group to WAN Connection interface	WAN Tagging
1	VLAN_GROUP1	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
2	VLAN_GROUP2	3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
3	VLAN_GROUP3	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
4	VLAN_GROUP4	5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
5	VLAN_GROUP5	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
6	VLAN_GROUP6	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
7	VLAN_GROUP7	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
8	VLAN_GROUP8	9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
LAN Tagging									
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>									

LAN Tagging: Insert or keep VLAN tag of the packets flow through the specific ethernet port.

WAN Tagging: Insert or keep VLAN tag of the packets flow through the specific Bridged WAN interface. (Only for Bridge)

**VLAN Group Name** – There are eight groups that user can setup by themselves.

**VLAN ID** – Group name ID

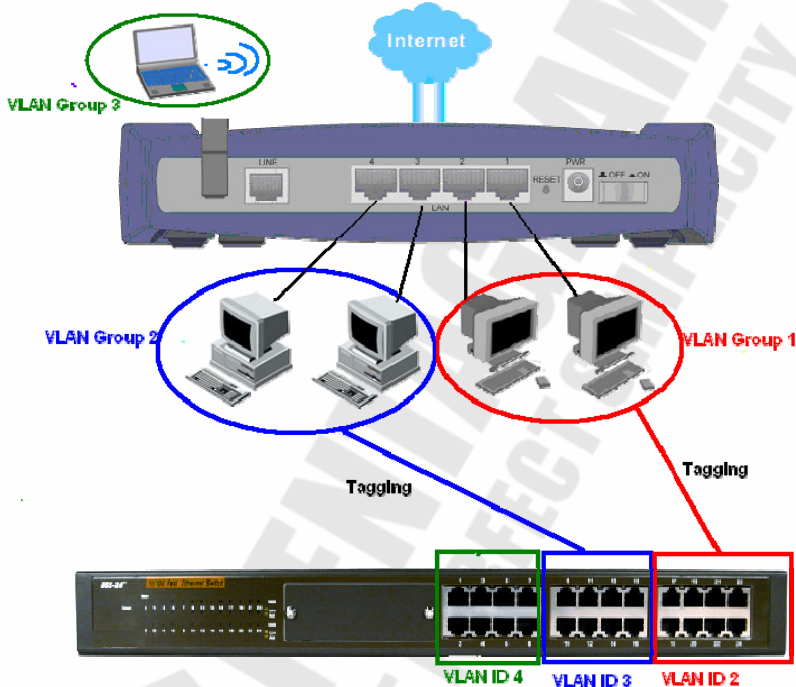
**LAN Tagging** – Tagging VLAN ID to the specific VLAN group for Ethernet interface.

**Ethernet port** – Port name of Router

**Link VLAN Group to WAN connection Interface** – Select the WAN connection interface that VLAN group link.

VLAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. Please refer to the following example.

1. If VLAN Group 1 is consisted of hosts linked to port1 and port2, VLAN Group 2 is consisted of hosts linked port3 and port4, and VLAN Group 3 is consisted wireless LAN.



2. After checking the box to enable VLAN function, you will check the table according to the needs as show below.

VLAN Group Control									
Parameters									
	VLAN Group Name	VLAN ID	Ethernet port #1	Ethernet port #2	Ethernet port #3	Ethernet port #4	wireless LAN	Link VLAN Group to WAN Connection interface	WAN Tagging
1	VLAN_GROUP1	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Main WAN connection(Management)	<input type="checkbox"/>
2	VLAN_GROUP2	3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WAN Bridge Connection #1 (0/101)	<input type="checkbox"/>
3	VLAN_GROUP3	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	WAN Bridge Connection #1 (0/101)	<input type="checkbox"/>
4	VLAN_GROUP4	5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
5	VLAN_GROUP5	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
6	VLAN_GROUP6	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
7	VLAN_GROUP7	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
8	VLAN_GROUP8	9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>
LAN Tagging									
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Apply		Cancel							

LAN Tagging: Insert or keep VLAN tag of the packets flow through the specific ethernet port.  
 WAN Tagging: Insert or keep VLAN tag of the packets flow through the specific Bridged WAN interface. (Only for Bridge)

## • Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.

Device Management			
<b>Embedded Web Server</b>			
HTTP Port	<input type="text" value="80"/>	(80 is default HTTP port)	
<b>Universal Plug and Play (UPnP)</b>			
UPnP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
UPnP Port	<input type="text" value="2800"/>		
<b>Telnet Configuration</b>			
Telnet	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
<b>SNMP Access Control</b>			
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
SNMP V1 and V2			
Read Community	<input type="text" value="public"/>	IP Address	<input type="text" value="0.0.0.0"/>
Write Community	<input type="text" value="password"/>	IP Address	<input type="text" value="0.0.0.0"/>
Trap Community	<input type="text"/>	IP Address	<input type="text"/>
SNMP V3			
Username	<input type="text"/>	Password	<input type="text"/>
Access Right	<input checked="" type="radio"/> Read <input type="radio"/> Read/Write		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

### Embedded Web Server:

**HTTP Port** – The port number of the router's embedded web server (for web-based configuration uses). The default value is the standard HTTP port, 80. You may specify an alternative if, for example, you are running a web server on a PC within your LAN.

**For Example:** User A changes HTTP port number to **100**, specifies their own IP address of **192.168.1.55**, and sets the logout time to be **100** seconds. The router only allows User A access from the IP address **192.168.1.55** to logon to the Web GUI by typing: *http://192.168.1.254:100* in their web browser. After 100 seconds, the device automatically logs out User A.

### Universal Plug and Play (UPnP):

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device. Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

**Disable** – Check to disable the router's UPnP functionality.

**Enable** – Check to enable the router's UPnP functionality.

**UPnP Port** – The default setting is 2800. It is highly recommended that you use this port value. If the value conflicts with other ports already in use you may wish to change the port.

### SNMP Access Control:

Simple Network Management Protocol—software on a PC within the LAN is required to use this function.

#### SNMP V1 and V2:

**Read Community** – Specify a name to be identified as the Read Community, and an IP address. This community string is checked against the string entered in the configuration file. Once the string name is matched, you can obtain this IP address and are able to view the data.

**Write Community** – Specify a name to be identified as the Write Community, and an IP address. This community string is checked against the string entered in the configuration file. Once a string name is matched, users from this IP address are able to view and modify data.

**Trap Community** – Specify a name and an IP address. This community string is checked against the string entered in the configuration file. Once a string name is matched, users from this IP address are sent SNMP Traps.

#### SNMP V3:

Specify a name and password for authentication, and define access rights from the identified IP address. Once authentication has succeeded, users from this IP address are able to view and modify data.

#### SNMP Version: SNMPv2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security" but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

#### The following MIBs are supported:

##### From RFC 1213 (MIB-II):

- ✓ System group
- ✓ Interfaces group
- ✓ Address Translation group
- ✓ IP group
- ✓ ICMP group
- ✓ TCP group
- ✓ UDP group
- ✗ EGP (not applicable)
- ✓ Transmission
- ✓ SNMP group

##### From RFC1650 (EtherLike-MIB):

- ✓ dot3Stats

##### From RFC 1493 (Bridge MIB):

- ✓ dot1dBase group
- ✓ dot1dTp group
- ✓ dot1dStp group (if configured as spanning tree)

##### From RFC 1471 (PPP/LCP MIB):

- ✓ pppLink group
- ✗ pppLqr group

##### From RFC 1472 (PPP/Security MIB):

- ✓ PPP Security Group)

##### From RFC 1473 (PPP/IP MIB):

- ✓ PPP IP Group

**From RFC 1474 (PPP/Bridge MIB):**

✓✓ PPP Bridge Group

**From RFC1573 (IfMIB):**

✓✓ ifMIBObjects Group

**From RFC1695 (atmMIB):**

✓✓ atmMIBObjects

**From RFC 1907 (SNMPv2):**

✓✓ only snmpSetSerialNo OID

- **IGMP**

IGMP, known as Internet Group Management Protocol, is used to management hosts from multicast group.

IGMP	
Parameters	
IGMP Proxy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IGMP Snooping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**IGMP Proxy** – Accepting multicast packet. Default is set to **Disable**.

**IGMP Snooping** – Allowing switched Ethernet to check and make correct forwarding decisions. Default is set to **Enable**

## Save Configuration to Flash Tab

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click **Save** to write your new configuration to FLASH.

### Save Config to FLASH

Write settings to FLASH

Apply

## Restart Tab

Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).

### Restart

After restarting. Please wait for several seconds to let the system

Restart Router with

- Save Config to FLASH
- Current Settings
- Factory Default Settings

Restart

Cancel

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings.

You may also reset your router to factory settings by holding in the small Reset pinhole button on the back of your router for 10-12 seconds while the router is turned on.

## ***Troubleshooting***

If the router is not function properly, first check this session for simple troubleshooting before contacting your Internet service provider (ISP) for support.

### ***Using LEDs to Diagnose Problems***

The **LEDs** are useful aides for finding possible problem causes.

#### **Power LED**

The **POWER LED** on the front panel does not light up.:

1. Make sure that the power adaptor is connected to the router and plugged in to an appropriate power source. Use only the supplied power adaptor;
2. Check that the router and the power source are both turned on and the router is receiving sufficient power;
3. Turn the router off and on;
4. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

#### **LAN LED**

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

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

#### **ADSL LED**

The **ADSL LED** on the front panel does not light up:

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

### ***Problems with the Web Interface***

I cannot access the web Interface:

1. Make sure you are using the correct IP address of the router. Check the IP address of the router;
2. Your computer's and the router's IP addresses must be on the same subnet for LAN access;
3. If you changed the router's LAN IP address, then enter the new one as the URL;
4. Remove any filters in LAN or WAN that block web service.

## ***Problems with the Login Username and Password***

I forgot my login username and/or password:

1. The default username is "**admin**". The default password is "**pentagram**". The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing;
2. Press the RESET button for 10-12 seconds, and then release it - the defaults have been restored and the router restarts;

## ***Problems with LAN Interface***

I cannot access the router from the LAN or ping any computer on the LAN:

1. Check the Ethernet LEDs on the front panel. A LAN LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting;
2. Make sure that the IP address and the subnet mask is consistent between the router and the workstation.
3. In some cases computer with Windows Vista or Windows XP SP3 cannot obtain an IP address from router's DHCP server. If you encounter this, follow this steps to resolve this problem (Microsoft Support page) <http://support.microsoft.com/kb/928233/en-us> (this article may be not available in user language).

## ***Problems with WAN Interface***

Initialization of the ADSL connection failed:

1. Check the cable connections between the ADSL port and the wall jack. The ADSL LED on the front panel of the router should be on;
2. Check that your VPI, VCI and type of encapsulation settings are the same as what you collected from your telephone company and ISP;
3. Restart the router. If you still have problems, you may need to verify your VPI, VCI and type of encapsulation settings with the telephone company and ISP.

I cannot get a WAN IP address from the ISP:

1. Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by the qualified and licensed electrician), and ensure that all line filters are correctly installed and right way around;
2. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnects.

Frequent loss of ADSL line sync (disconnections):

1. The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name;
2. The username and password apply to PPPoE and PPPoA connections only. Make sure that you have entered the correct **Service Name**, **Username** and **Password** (be sure to use the correct casing).

## ***Problems with the Internet Access***

I cannot access the Internet:

1. Make sure the router is turned on and connected to the network;
2. If the ADSL LED is off, refer to Section **ADSL LED** of this troubleshooting;
3. Verify your WAN settings;
4. Make sure you entered the correct user name and password;
5. For wireless stations, check that both the router and wireless station(s) are using the same ESSID, channel and encryption keys (if encryption is activated).

Internet connection disconnects:

1. If you use PPPoA or PPPoE encapsulation, check the idle time-out setting;
2. Contact your ISP.

If you have any troubles to configure or setup this ADSL Ethernet Router, please feel free to contact us.

