

User's Manual

PENTAGRAM Cerberus P 6311-07A



*The latest versions of manual, drivers and applications are available on
www.pentagram.eu*

2007-09-12

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
PACKAGE CONTENTS	5
FEATURES	6
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	10
CONFIGURE ROUTER VIA WEB BROWSER	14
LOGIN	14
NAVIGATION	15
QUICK START WIZARD	16
INTERFACE SETUP TAB	21
ADVANCED SETUP TAB	28
ACCESS MANAGEMENT TAB	41
MAINTENANCE TAB	49
STATUS TAB	53
HELP TAB	57
TROUBLESHOOTING	58
USING LEDS TO DIAGNOSE PROBLEMS	58
PROBLEMS WITH THE WEB INTERFACE	59
PROBLEMS WITH THE LOGIN USERNAME AND PASSWORD	59
PROBLEMS WITH LAN INTERFACE	59
PROBLEMS WITH WAN INTERFACE	59
PROBLEMS WITH THE INTERNET ACCESS	60





Introduction

Thank you for purchasing the Cerberus P 6311-07A Modem/Router by PENTAGRAM. Your new router is an all-in-one unit that combines an ADSL modem, ADSL router and Ethernet network switch to provide everything you need to get the machines on your network connected to the Internet over an ADSL broadband connection.

The Cerberus P 6311-07A 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.

Your new router also serves as an Internet firewall, protecting your network from access by outside users. Not only does it provide a natural firewall function with Network Address Translation (NAT), it also provides rich firewall features to secure your network. All incoming data packets are monitored and filtered. You can also configure your new router to block internal users from accessing the Internet.

The Integrated DHCP (Dynamic Host Control Protocol) client and server services allow multiple users to get IP addresses automatically when the router boots up. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from the DHCP server and reboot. Each time a local machine is powered up; the router recognizes it and assigns an IP address to instantly connect it to the LAN.

For advanced users, Virtual Service (port forwarding) functions allow the product to provide limited visibility to local machines with specific services for outside users. You can set an ISP (Internet Service Provider) provided IP address on the Cerberus P 6311-07A and then you can reroute specific services to individual computers on your local network. For instance, a dedicated web server can be connected to the Internet via the router and then incoming requests for web pages that are received by the router can be rerouted to your dedicated local web server, even though the server now has a different IP address.

Virtual Server can also be used to re-task services to multiple servers. For instance, you can set the router to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

Package Contents

1. PENTAGRAM Cerberus P 6311-07A
2. Power adapter 12 V, 1 A
3. Ethernet cable (RJ-45)
4. Telephone cable (RJ-11)
5. USB cable
6. CD
7. Quick Installation Guide

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.
- 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.
- Universal Plug and Play (UPnP) and UPnP NAT Traversal: 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 P 6311-07A 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.

- High Speed Internet Access: downstream rates of up to 24Mbps and upstream rates of up to 1Mbps. Cerberus ADSL2+ Lite 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), G.994.1 (G.hs, Multimode), ITU-T G.992.3 (ADSL2 G.dmt.bis), ITU-T G.992.4 (ADSL2 G.lite.bis), ITU-T G.992.5 (ADSL2+; Annex A, I, J, L & M), Reach Extended ADSL (RE ADSL).
- Multi-Protocol to Establish a Connection: The router supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483/2684 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516) and IPoA (RFC1577) to establish a connection with an ISP. The router also supports VC-based and LLC-based multiplexing.

Product Overview

Important Notes

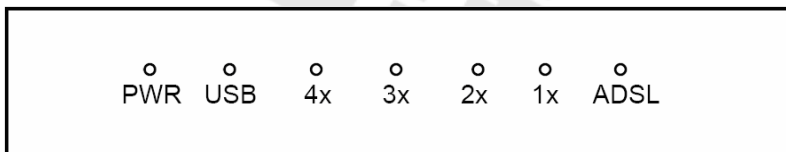


- Do not use the router in high humidity or high temperatures.
- Do not use the same power source for the router as other equipment.
- Do not repair or open the case by yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.



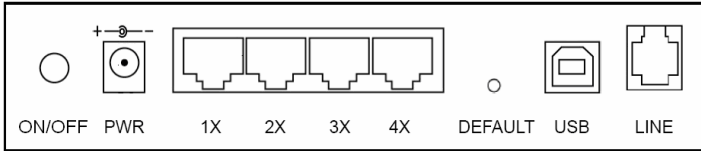
- Avoid using this product and all accessories outdoors.
- Place the router on a stable surface.
- Only use the power adaptor that comes with the package. Using a different voltage rating power adaptor may damage the router.

Front Panel



LED		Description
1	PWR	Lights when the power is ON.
2	USB	Lights when an active USB cable is connected with router.
3	LAN1	Steady glow when connected to an Ethernet device. Glow green for 100Mbps; Orange for 10Mbps. Blinking light when data is Transmitted / Received.
4	LAN2	
5	LAN3	
6	LAN4	
7	ADSL	Lights when successfully connected to an ADSL DSLAM Blinking when router is trying to connect to a DSLAM.

Back Panel



- ON/OFF** Power switch button.
- PWR** Connect the supplied power adapter to this jack.
- LAN (RJ-45)** Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
- DEFAULT** After the router is powered on, press this recessed button using the end of paper clip or other small pointed object to reset the router or to restore it to factory default settings.
- USB** Use this port to connect router to computer via USB.
- LINE (RJ-11)** Connect the supplied RJ-11 (telephone) cable to this port when connecting to the ADSL/telephone network.

Default Settings

Before changing configuration familiarize yourself with these default settings.

LAN/WLAN Ports	
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
DHCP Server	Enabled
DHCP Server IP Address Pool	100 IP addresses from 192.168.1.101
IP Address Lease Time	259200 seconds (72 hours)
User Name	admin
Password	pentagram

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 for ADSL LED to lit or start blinking.
- Press and hold **DEFAULT** button on the back panel of router for 5-10 seconds and then release it.
- After reset LEDs will return to their normal behavior and all settings will be reset to their default value. You can login to router configuration page using default username and password: admin / pentagram.

Connecting Cerberus to Computer.

You can connect ADSL router with PC through either Ethernet cable or USB cable.

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 USB Port

You can connect ADSL router with PC via USB cable when there is no Networking LAN Card present on your PC. USB cable acts as another LAN connection in this scenario. Once you establish Internet connection, you can browse the Web through the USB cable.

1. Connect ADSL Router and PC with USB cable.
2. Once "Detect New USB Device" window pops out, click **Cancel**.
3. Insert Driver CD and in menu click **Install USB Driver**.
4. Click four times **Next**. If Program Installation window pops up click **Continue anyway**.
5. Driver will be installed automatically.
6. Click **Finish** to end installation.

Network connection should work properly after system restart.

To check if USB device is installed properly, click **Start Menu** → **Control Panel** → **System** → **Hardware tab** → **Device Manager**.

Configure TCP/IP

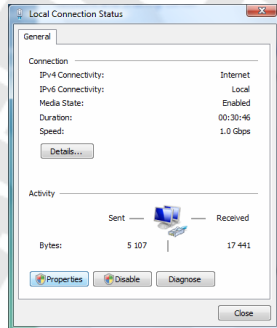
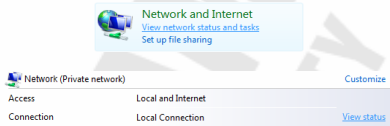
After connecting the computer to the router (by LAN adapter or USB interface) the TCP/IP protocol should be configured. The protocol should be automatically installed together with Network card drivers. It is advised that TCP/IP should be configured to receive IP address and all the necessary network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



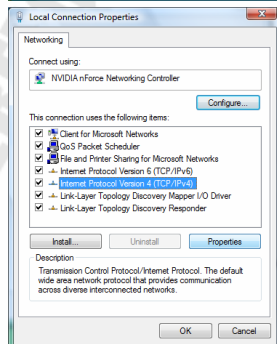
Windows Vista

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

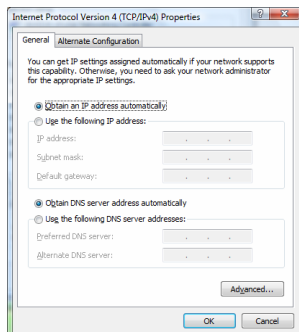
1. Click **Start** → **Control Panel**.
2. Click **View network status and tasks**.
3. Click **View status** for appropriate connection.
4. In **General** tab, Click the **Properties** button.



5. In **General** tab, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

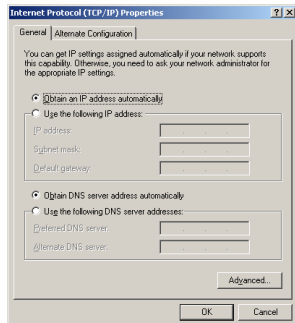
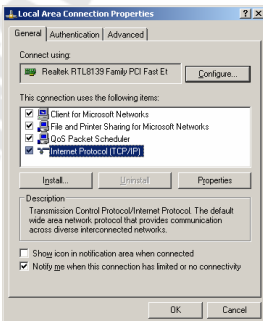
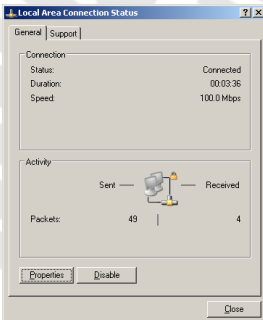


6. In **General** tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
7. Click **OK** to save settings and close **Internet Protocol Version 4 (TCP/IPv4) Properties** window.



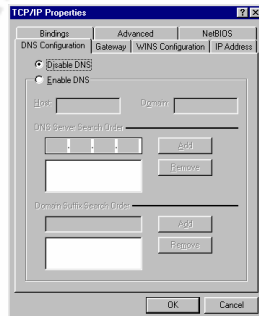
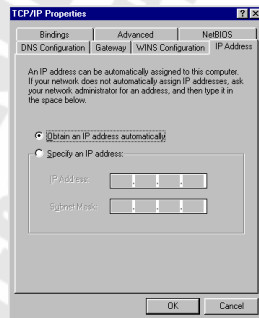
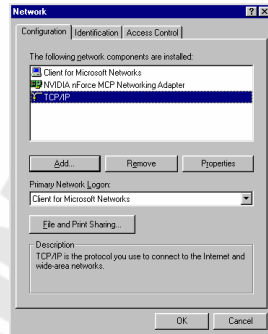
Windows 2000/XP

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. In **General** tab, Click the **Properties** button.
4. In **General** tab, select **Internet Protocol (TCP/IP)** and click **Properties**.
5. In **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. In **Configuration** tab, select **TCP/IP** for appropriate network adapter and click **Properties**.
3. In **IP Address** tab, select **Obtain an IP address automatically**.
4. In **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:

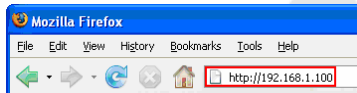
1. click **Start > Run**
2. type **cmd** (Win 2000/XP) or **command** (Win 95/98/ME) and press Enter
3. in command line type **ipconfig /all** and press Enter
4. check if the **IP Address** is **192.168.1.x**

Configure router via web browser

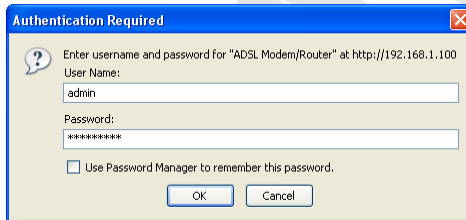
Cerberus P 6311-07A router can be configured via web browser, which is usually integrated with operating system. Router offers clear and simple interface.

Login

1. Launch the Web browser
2. Type the default router's IP address: **http://192.168.1.100** in the address bar



3. If system password is set, enter **User Name** and **Password** – default: **admin** / **pentagram**



Navigation

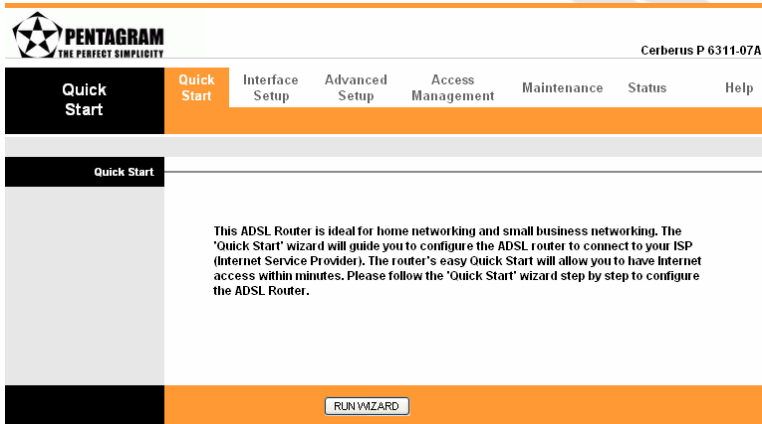
The screenshot displays the web configuration interface for the Cerberus P 6311-07A router. The browser window is Mozilla Firefox, and the address bar shows the IP address 192.168.1.100. The page features a navigation menu with the following options: Status (highlighted), Quick Start, Interface Setup, Advanced Setup, Access Management, Maintenance, and Help. Below the navigation menu, there are sub-tabs for Device Info, System Log, and Statistics. The main content area is divided into sections for Device Information, LAN, WAN, and ADSL. The Device Information section shows Firmware Version: 2.10.5.0(UE0.C29)3.6.0.0 and MAC Address: 00:06:4f:26:b9:e3. The LAN section shows IP Address: 192.168.1.100, Subnet Mask: 255.255.255.0, and DHCP Server: Enabled. The WAN section shows Virtual Circuit: PVCO, Status: Not Connected, Connection Type: PPPoA, IP Address: 0.0.0.0, Subnet Mask: 0.0.0.0, Default Gateway: 0.0.0.0, DNS Server: 0.0.0.0, and NAT: Enabled. The ADSL section shows ADSL Firmware Version: FwVer:3.6.0.0_A_TC3085 HwVer:T14F7_1.0, Line State: Down, Modulation: Multi-Mode, and Annex Mode: ANNEX_A. A table at the bottom of the ADSL section shows Downstream and Upstream statistics: SNR Margin (N/A), Line Attenuation (N/A), and Data Rate (0).

Steps to navigate the Web configuration from the Site Map are summarized below:

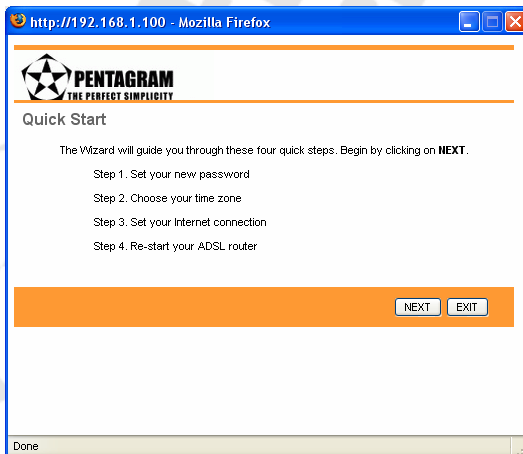
- **Quick Start** – wizard that helps to configure your router,
- **Interface Setup** – configure Internet and LAN functions,
- **Advanced Setup** – configure advanced features,
- **Access Management** – manage Internet access options,
- **Maintenance** – set a new password, set the time zone, upgrade or reload firmware and run diagnostic tests on the router,
- **Status** – router device information, system logs and performance statistics,
- **Help** – available help topics.

Quick Start Wizard

Click Quick Start to guide you to configure the device to connect your ISP and have Internet access within minutes. This Quick Start will guide you step by step to configure the password, time zone, and WAN settings of you device. This Wizard is a helpful guide for first time uses to the device. It is strongly recommended to use Quick Start to configure your ADSL settings.



Click on the **RUN WIZARD** button to start the Quick Start wizard. The Quick Start wizard will open a new browser window with the following screen:

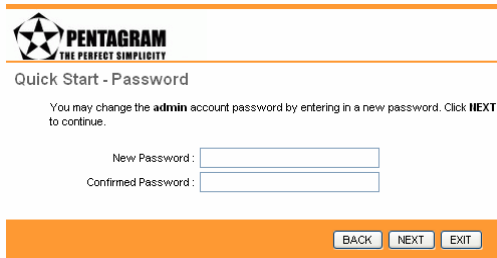



Please follow the quick start step by step to configure the device.

Click on **NEXT** to continue, or on **EXIT** to exit the wizard without saving.

Setting a New Password

This screen helps you set a new password, replacing the default password.



 **PENTAGRAM**
THE PERFECT SIMPLICITY

Quick Start - Password

You may change the **admin** account password by entering in a new password. Click **NEXT** to continue.

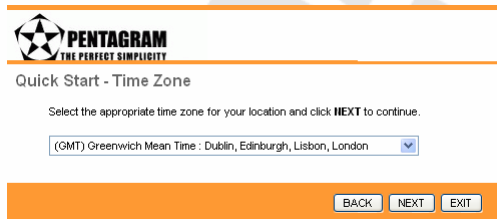
New Password:


Confirmed Password:

Enter new password in **New Password** and **Confirmed Password** fields.

Click on **BACK** to return to the previous screen, on **NEXT** to continue, or on **EXIT** to exit the wizard without saving.

Choose your Time Zone



 **PENTAGRAM**
THE PERFECT SIMPLICITY

Quick Start - Time Zone

Select the appropriate time zone for your location and click **NEXT** to continue.

(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Select the appropriate time zone for your location from the dropdown list.

Click on **BACK** to return to the previous screen, on **NEXT** to continue, or on **EXIT** to exit the wizard without saving.

Set your Internet Connection

Glossary:

- Multiplexing** - Two conventions identify what protocols a virtual circuit (VC) is carrying. Be sure to use the multiplexing method your ISP requires:
 - VC-Based Multiplexing** – In VC-based multiplexing, by prior mutual agreement, each protocol is assigned to a specific virtual circuit. For example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.
 - LLC-Based Multiplexing** – In LLC-based multiplexing, one VC carries multiple protocols with protocol-identifying information contained in each packet header. While this method requires extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol; for example, if charging heavily depends on the number of simultaneous VCs.
- VPI and VCI** - Be sure to use the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255. The valid range for the VCI is 32 to 65535. 0 to 31 is reserved for local management of ATM traffic.
- PPPoA** – Point-to-Point Protocol over ATM Adaptation Layer 5 (AAL5) (PPPoA) provides access control and billing functionality in a manner similar to dial-up services using PPP. The router encapsulates the PPP session based on RFC1483 and sends it through ATM PVC to the ISP's DSLAM.
- PPPoE** – Point-to-Point Protocol over Ethernet provides access control and billing functionality in a manner similar to dial-up services using PPP. The router bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM Permanent Virtual Circuit (PVC) that connects to the ADSL Access Concentrator, where the PPP session terminates. Single PVC can support any number of PPP sessions from your LAN.



Quick Start - ISP Connection Type

Select the Internet connection type to connect to your ISP. Click **NEXT** to continue.

- | | |
|--|--|
| <input type="radio"/> Dynamic IP Address | Choose this option to obtain a IP address automatically from your ISP. |
| <input type="radio"/> Static IP Address | Choose this option to set static IP information provided to you by your ISP. |
| <input checked="" type="radio"/> PPPoE/PPPoA | Choose this option if your ISP uses PPPoE/PPPoA. (For most DSL users) |
| <input type="radio"/> Bridge Mode | Choose this option if your ISP uses Bridge Mode. |

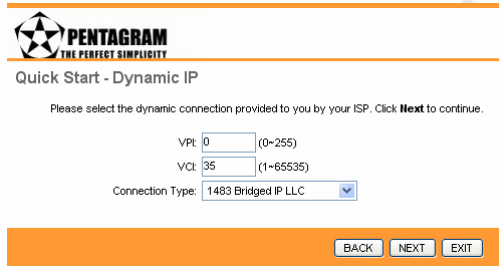
BACK **NEXT** **EXIT**

Select the Internet connection type you use to connect to your ISP. The following screen will vary depending on which connection type you chose.

Click on **BACK** to return to the previous screen, on **NEXT** to continue, or on **EXIT** to exit the wizard.

- **Dynamic IP Address**

A dynamic IP address connection requests a new IP address from your ISP each time you connect to it.

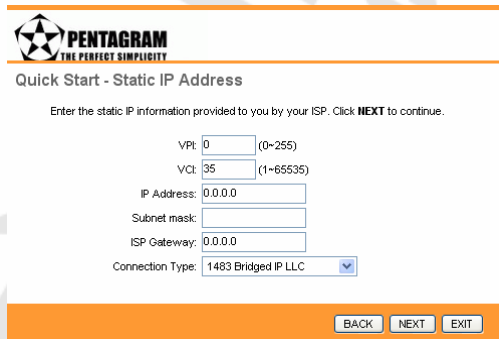


Enter **VPI** (Virtual Path Identifier), **VCI** (Virtual Channel Identifier) and select your **Connection Type** from the dropdown list. Your ISP should provide the above information.

Click on **BACK** to return to the previous screen, on **NEXT** to continue, or on **EXIT** to exit the wizard without saving.

- **Static IP Address**

A static IP address connection uses the same IP each time you connect to your ISP.



Enter **VPI** (Virtual Path Identifier), **VCI** (Virtual Channel Identifier), **IP Address**, **Subnet mask**, **ISP Gateway** and select your **Connection Type** from the dropdown list. Your ISP should provide the above information.

Click on **BACK** to return to the previous screen, on **NEXT** to continue, or on **EXIT** to exit the wizard without saving.

- **PPPoE/PPPoA**

Configure connection based on PPPoE / PPPoA protocol.

PENTAGRAM
THE PERFECT SIMPLICITY

Quick Start - PPPoE/PPPoA

Enter the PPPoE/PPPoA information provided to you by your ISP. Click **NEXT** to continue.

Username:

Password:

VPI: (0~255)

VCI: (1~65535)

Connection Type:

Enter **Username**, **Password**, **VPI** (Virtual Path Identifier), **VCI** (Virtual Channel Identifier) and select your **Connection Type** from the dropdown list. Note that you must enter the user name exactly as your ISP assigned it. If the assigned name is in the form of user@domain where domain identifies a service name, enter it exactly as given.

Click on **BACK** to return to the previous screen, on **NEXT** to continue, or on **EXIT** to exit the wizard without saving.

- **Bridge Mode**

RFC 1483 explains two methods for Multi-protocol Encapsulation over AAL5. The first method allows multiplexing of multiple protocols over just one ATM virtual circuit (LLC-based multiplexing). The second method assumes that each individual protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more information.

PENTAGRAM
THE PERFECT SIMPLICITY

Quick Start - Bridge Mode

Enter the bridge information provided to you by your ISP. Click **NEXT** to continue.

VPI: (0~255)

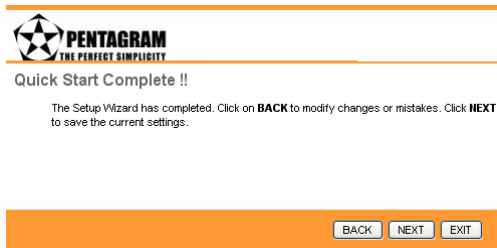
VCI: (1~65535)

Connection Type:

Enter **VPI** (Virtual Path Identifier), **VCI** (Virtual Channel Identifier) and select your **Connection Type** from the dropdown list. Your ISP should provide the above information.

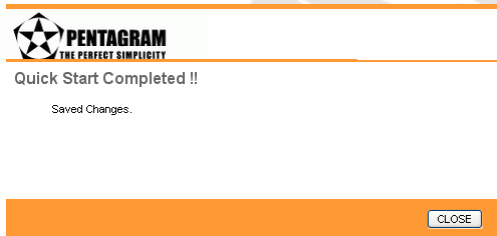
Click on **BACK** to return to the previous screen, on **NEXT** to continue, or on **EXIT** to exit the wizard without saving.

Finishing the Wizard



The Quick Start wizard now has all the information it needs. You **MUST** click **NEXT**, to save configuration!

Click on **BACK** to make changes or correct mistakes. Click on **NEXT** to save the current settings. Click on **EXIT** to exit the wizard without saving.



Your changes have been saved. Click on **CLOSE**. The Quick Start wizard window will close.


Interface Setup Tab

Glossary:

- **RIP (Routing Information Protocol):** Select this option to specify the RIP version, including **RIP1**, **RIP2-B** and **RIP2-M**. RIP2-B & RIP2-M are both sent in RIP-2 format, the difference is that RIP2-M using Multicast and RIP2-B using Broadcast format.
- **RIP Direction:** Select this option to specify the RIP direction. **None** is for disabling the RIP function. **Both** means the ADSL Router will periodically send routing information and accept routing information then incorporate into routing table. **IN only** means the ADSL router will only accept but will not send RIP packet. **OUT only** means the ADSL router will only send but will not accept RIP packet.
- **IGMP (Internet Group Multicast Protocol):** It is a session-layer protocol used to establish membership in a multicast group. The ADSL supports both IGMP version **IGMP-v1** & **IGMP-v2**. Select **None** to disable it.

Internet

The Internet screen allows you to set up how your router connects to the Internet. If you already ran the Quick Start wizard, the information you provided to the wizard should be entered into the fields already. After you finish the changes, click on the **SAVE** button to save your changes.



PENTAGRAM

THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Interface
Quick Start
Interface Setup
Advanced Setup
Access Management
Maintenance
Status
Help

Internet
LAN

ATM VC

Virtual Circuit: PVC0 PVCs Summary

Status: Activated Deactivated

VPI: 0 (range: 0-255)

VCI: 35 (range: 1-65535)

QoS

ATM QoS: LUBR

PCR: 0 cells/second

SCR: 0 cells/second

MBS: 0 cells

Encapsulation

ISP: Dynamic IP Address

Static IP Address

PPPoA,PPPoE

Bridge Mode

PPPoE/PPPoA

Username: ISP

Password: ***

Encapsulation: PPPoA VC-Mux

Half Bridge: Activated Deactivated

Connection Setting

Connection: Always On (Recommended)

Connect On-Demand (Close if idle for 0 minutes)

Connect Manually

TCP MSS Option: TCP MSS(0:default) 0 bytes

IP Address

Get IP Address: Static Dynamic

Static IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

NAT: Enable

Default Route: Yes No

TCP MTU Option: TCP MTU(0:default) 0 bytes

Dynamic Route: RIP1 Direction Both

Multicast: Disabled

SAVE

● ATM VC

ATM settings are used to connect to your ISP. Your ISP provides VPI, VCI, settings to you. In this Device, you can totally setup 8 PVCs on different encapsulations if you apply 8 different virtual circuits from your ISP. You need to activate the VC to take effect. For PVCs management, you can use ATM QoS to setup each PVC traffic line's priority.

Virtual Circuit – Select the VC number you want to setup.

Status – Select whether selected connection is **Activated** or **Deactivated**.

VPI – Virtual Path Identifier. The valid range for the VPI is 0 to 255.

VCI – Virtual Channel Identifier. The valid range for the VCI is 1 to 65635 (0 to 31 is reserved for local management of ATM traffic).

ATM QoS – Select the Quality of Service types for this Virtual Circuit. The ATM QoS types include **CBR** (Constant Bit Rate), **VBR** (Variable Bit Rate) and **UBR** (Unspecified Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR, SCR, and MBS.

PCR (Peak Cell Rate) – Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832 Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

SCR (Sustained Cell Rate) – Sustained Cell Rate (SCR) is the mean cell rate of a burst, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. SCR may not be greater than the PCR; the system default is 0 cells/sec.

MBS (Maximum Burst Size) – Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

CBR (Constant Bit Rate) – is for connections that support constant rates of data transfer. The only parameter you need to worry about in CBR is PCR.

UBR (Unspecified Data Rate) – is for connections that have variable traffic. The only parameter you need to worry about in UBR is PCR.

rtVBR (real time Variable Bit Rate) – is for connections that, while having variable traffic, require precise timing between traffic source and destination. PCR, SCR and MBS must all be set for rtVBR.

nrtVBR (non real time Variable Bit Rate) – is for connections that have variable traffic, do not require precise timing, but still require a set bandwidth availability. PCR, SCR and MBS must all be set for nrtVBR.

- **Encapsulation**

Select the encapsulation protocol your ISP uses. The following section will vary depending on which encapsulation protocol you select.

Encapsulation

ISP: Dynamic IP Address
 Static IP Address
 PPPoA/PPPoE
 Bridge Mode

- **Dynamic IP Address**

Select this option if your ISP provides you an IP address automatically. Please enter the Dynamic IP information accordingly.

Dynamic IP

Encapsulation: 1483 Routed IP VC-Mux

NAT: Enable

Default Route: Yes No

TCP MTU Option: TCP MTU(0:default) 0 bytes

Dynamic Route: RIP1 Direction Both

Multicast: Disabled

Encapsulation – Select your encapsulation type from the dropdown list.

NAT – Select whether NAT (Network Address Translation) is Enabled or Disabled.

Default Route – Select whether this PVC will be the default route for Internet data.

TCP MTU Option – Enter TCP MTU (Maximum Transmission Unit) Value here.

Dynamic Route – Select the RIP type and direction from the dropdown lists.

Multicast – Select the multicast protocol you wish to use from the dropdown list.

- **Static IP Address**

Select this option to set static IP information.

Static IP

Encapsulation: 1483 Routed IP VC-Mux

Static IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

NAT: Enable

Default Route: Yes No

TCP MTU Option: TCP MTU(0:default) 0 bytes

Dynamic Route: RIP1 Direction Both

Multicast: Disabled

Encapsulation – Select your encapsulation type from the dropdown list.

Static IP Address – Enter the static IP Address here.

IP Subnet Mask – Enter the IP Subnet Mask here.

Gateway – Enter the Gateway address here.

NAT – Select whether NAT (Network Address Translation) is Enabled or Disabled.

Default Route – Select whether this PVC will be the default route for Internet data.

TCP MTU Option – Enter TCP MTU (Maximum Transmission Unit) Value here.

Dynamic Route – Select the RIP type and direction from the dropdown lists.

Multicast – Select the multicast protocol you wish to use from the dropdown list.

- **PPPoA/PPPoE**

Select this option if your ISP requires you to use a PPPoA/PPPoE connection.

PPPoE/PPPoA	
Connection Setting	Username: <input type="text" value="ISP"/> Password: <input type="password" value="***"/> Encapsulation: PPPoA VCo-Mux <input type="button" value="v"/> Half Bridge: <input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
	Connection: <input checked="" type="radio"/> Always On (Recommended) <input type="radio"/> Connect On-Demand (Close if idle for <input type="text" value="0"/> minutes) <input type="radio"/> Connect Manually TCP MSS Option: TCP MSS(0:default) <input type="text" value="0"/> bytes
IP Address	Get IP Address: <input type="radio"/> Static <input checked="" type="radio"/> Dynamic Static IP Address: <input type="text" value="0.0.0.0"/> IP Subnet Mask: <input type="text" value="0.0.0.0"/> Gateway: <input type="text" value="0.0.0.0"/> NAT: <input type="button" value="Enable"/> <input type="button" value="Disable"/> Default Route: <input checked="" type="radio"/> Yes <input type="radio"/> No TCP MTU Option: TCP MTU(0:default) <input type="text" value="0"/> bytes Dynamic Route: RIP1 <input type="button" value="v"/> Direction Both <input type="button" value="v"/> Multicast: <input type="button" value="Disabled"/> <input type="button" value="Enabled"/>

Username – Enter your username for your PPPoE/PPPoA connection.

Password – Enter your password for your PPPoE/PPPoA connection.

Encapsulation – Select your encapsulation type from the dropdown list.

Half Bridge – external IP address obtained from ISP will be transferred to first computer which will connect to and obtain IP address from router. Only this computer will have access to internet.

Connection – Select whether your connection is always on or if it connects on demand or manually. If on demand, specify how many minutes the connection may be idle before it disconnects.

TCP MMS Option – Enter the TCP MSS (Maximum Segment Size) you wish to use here.

Get IP Address – Choose whether the router obtains the IP address statically or dynamically.

Static IP Address – Enter the static IP address here. Only if you chose Static above.

IP Subnet Mask – Enter the IP subnet mask here. Only if you chose Static above.

Gateway – Enter the gateway here. Only if you chose Static above.

NAT – Select whether NAT (Network Address Translation) is Enabled or Disabled.

Default Route – Select whether this PVC will be the default route for Internet data.

TCP MTU Option – Enter TCP MTU (Maximum Transmission Unit) Value here.

Dynamic Route – Select the RIP type and direction from the dropdown lists.

Multicast – Select the multicast protocol you wish to use from the dropdown list.

- **Bridge Mode**

The modem can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable 2 or more networks to communicate as if they are 2 segments of the same physical LAN. Please set the Connection type.

Bridge Mode	
	Encapsulation: <input type="button" value="1483 Bridged IP VCo-Mux"/> <input type="button" value="v"/>

Encapsulation – Select your encapsulation type from the dropdown list.

LAN

There are the IP settings of the LAN Interface for the device. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is provided to your internal network and cannot be seen on the Internet.

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Interface | Quick Start | **Interface Setup** | Advanced Setup | Access Management | Maintenance | Status | Help

Internet | **LAN**

Router Local IP

IP Address : 192.168.1.100
 IP Subnet Mask : 255.255.255.0
 Dynamic Route : RIP2-B | Direction : None
 Multicast : Disabled
 IGMP Snoop : Disabled Enabled

DHCP

DHCP : Disabled Enabled Relay

DHCP Server

Starting IP Address : 192.168.1.101 | [Current Pool Summary](#)
 IP Pool Count : 100
 Lease Time : 259200 seconds (0 sets to default value of 259200)

DNS

DNS Relay : Use Auto Discovered DNS Server Only
 Primary DNS Server : N/A
 Secondary DNS Server : N/A

- **Router Local IP**

Router Local IP

IP Address : 192.168.1.100
 IP Subnet Mask : 255.255.255.0
 Dynamic Route : RIP2-B | Direction : None
 Multicast : Disabled
 IGMP Snoop : Disabled Enabled

IP Address – Enter the IP address of your ADSL router in dotted decimal notation, for example, 192.168.1.100 (default setting).

IP Subnet Mask – Your ADSL router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing sub netting, use the subnet mask computed by the ADSL router.

Dynamic Route – Select the Dynamic Route from RIP1, RIP2-B, and RIP2-M. Please refer to Internet → Dynamic Route. The only difference is the interface.

Multicast – IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. Please refer to Internet → Multicast. The only difference is the interface.

IGMP Snoop – Choose whether to **Disable** or **Enable** IGMP Snoop function.

- **DHCP**

The DHCP Server gives out IP addresses when a device is booting up and request an IP to be logged on to the network. It must be set as a DHCP client to obtain the IP address automatically. By default, the DHCP Server is enabled. The DHCP address pool contains the range of the IP address that will automatically be assigned to the client on the network.

Disabled – DHCP server is Disabled

Enabled – DHCP server is Enabled

Relay – router acts as a relay to different computer/device.

Disabled

The screenshot shows the DHCP configuration interface. The 'DHCP' tab is selected. Below the tab, there are three radio buttons: 'Disabled' (which is selected), 'Enabled', and 'Relay'. The rest of the page content is obscured by a watermark.

Enabled

The screenshot shows the DHCP configuration interface with 'Enabled' selected. The 'DHCP Server' section is active, showing the following fields:

- Starting IP Address: 192.168.1.101
- IP Pool Count: 100
- Lease Time: 259200 seconds (0 sets to default value of 259200)

 The 'DNS' section is also visible, with 'DNS Relay' set to 'Use Auto Discovered DNS Server Only', and both 'Primary DNS Server' and 'Secondary DNS Server' set to 'N/A'.

Starting IP Address – Enter the starting IP address you wish to use as the DHCP server's IP assignment.

IP Pool Count – Enter the maximum user pool size you wish to allow.

Lease Time – Enter the amount of time you wish to lease out a given IP address.

DNS Relay – Select the DNS relay option you wish to use from the dropdown list.

Primary DNS – Enter the primary DNS server IP address you wish to use. For user discovered DNS only.

Secondary DNS – Enter the secondary DNS server IP address you wish to use. For user discovered DNS only.

Relay

A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enable, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.

The screenshot shows the DHCP Relay configuration interface. The 'DHCP Relay' tab is selected. Below the tab, there is a single text input field for 'DHCP Server IP for Relay Agent' with the value '0.0.0.0' entered.

DHCP Server IP for Relay Agent – The DHCP server IP Address runs on WAN side.

Advanced Setup Tab

Firewall

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Advanced | Quick Start | Interface Setup | **Advanced Setup** | Access Management | Maintenance | Status | Help

Firewall | Routing | NAT | QoS | VLAN | ADSL

Firewall

Firewall : Enabled Disabled

SPI : Enabled Disabled

(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)

SAVE CANCEL

Firewall – Select this option can automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

SPI – Select this option to Enable or Disable the SPI feature. (NOTE: If you enable SPI, all traffics initiate from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side).

Routing

This table lists IP address of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Gateway IP to identify the first Internet router it should contact to route the data most efficiently. Select this option will list the routing table information. You can press **ADD ROUTE** to edit the static route. (As below screen)

The screenshot shows the Pentagram router configuration interface. The top navigation bar includes 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. The 'Advanced Setup' section is expanded to show 'Firewall', 'Routing', 'NAT', 'QoS', 'VLAN', and 'ADSL'. The 'Routing Table List' is displayed as a table with the following data:

#	Dest IP	Mask	Gateway IP	Metric	Device	Use	Edit	Drop
1	192.168.1.0	24	192.168.1.100	1	enet0	290		
2	default	0	Node1	2	Idle	0		

Below the table is an 'ADD ROUTE' button.

ADD ROUTE – click this button to set Static Routing information.

The screenshot shows the 'Static Route' configuration form in the Pentagram router interface. The form includes the following fields and options:

- Destination IP Address:
- IP Subnet Mask:
- Gateway IP Address: PVC0
- Metric:
- Announced in RIP: (Yes)

At the bottom of the form are buttons for 'SAVE', 'DELETE', 'BACK', and 'CANCEL'.

Destination IP Address – This parameter specifies the IP network address of the final destination of packets routed by this rule.

IP Subnet Mask – Enter the subnet mask for this destination.

Gateway IP Address – Enter the IP address of the gateway. A gateway does the actual forwarding of the packets. Enter the gateway's IP address in the field or select which PVC you wish to act as a gateway. The gateway is an immediate neighbor of your ADSL Router that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Router; over Internet (WAN), the gateway must be the IP address of one of the remote nodes.

Metric – Metric represents the “cost” of transmission for routing purposes. IP Routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not to be precise, but it must between 1 and 15. In practice, 2 or 3 is usually a good number.

Announced in RIP – This parameter determines if the ADSL router includes the router to this remote node in its RIP broadcasts. If you choose Yes, the router in this remote node will be

propagated to other hosts through RIP broadcasts. If you choose No, this route is kept private and is not included in the RIP broadcasts.

When you are done making changes, click on **SAVE** to save your changes, **DELETE** to delete the rule with the parameters you set, **BACK** to return to the previous screen or **CANCEL** to discard changes.

NAT

What NAT Does

NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed. The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. You may also designate servers, such as a Web server and a telnet server, on your local network and make them accessible to the outside world. With no servers defined, your router filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

Inside/outside indicates where a host is located relative to the router. The computers hosts of your LAN are inside, while the Web servers on the Internet are outside. Global/local indicates the IP address of a host in a packet as the packet traverses a router. The local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host of a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA is the source address on the LAN, and the IGA is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ROUTER keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.

NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

One-to-One – In One-to-One mode, the TC3162 EVM maps one local IP address to one global IP address.

Many-to-One – In Many-to-One mode, the TC3162 EVM maps multiple local IP addresses to one global IP address.

Many-to-Many Overload – In Many-to-Many Overload mode, the TC3162 EVM maps multiple local IP addresses to shared global IP addresses.

Many-to-Many No Overload – In Many-to-Many No Overload mode, the TC3162 EVM maps each local IP address to a unique global IP address.

Server – This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. The following table summarizes these types.

TYPE	IP MAPPING	
One-to-One	ILA1	IGA1
Many-to-One (SUA/PAT)	ILA1	IGA1
	ILA2	IGA1
	...	
Many-to-Many Overload	ILA1	IGA1
	ILA2	IGA2
	ILA3	IGA1
	ILA4	IGA2
	...	
Many-to-Many No Overload	ILA1	IGA1
	ILA2	IGA2
	ILA3	IGA3
	ILA4	IGA4
	...	
Server	Server IP 1	IGA1
	Server IP 2	IGA1
	Server IP 3	IGA1

NAT (Network Address Translation) is a method for disguising the private IP addresses you use on your LAN as the public IP address you use on the Internet. You define NAT rules that specify exactly how and when to translate between public and private IP addresses. Simply select this option to setup the NAT function for your ADSL router.

The screenshot shows the Pentagram router's web interface. At the top, the Pentagram logo and 'THE PERFECT SIMPLICITY' tagline are visible on the left, and 'Cerberus P 6311-07A' is on the right. Below the logo is a navigation menu with 'Advanced' selected. Under 'Advanced', there are sub-menus: 'Quick Start', 'Interface Setup', 'Advanced Setup' (highlighted), 'Access Management', 'Maintenance', 'Status', and 'Help'. Under 'Advanced Setup', there are further sub-menus: 'Firewall', 'Routing', 'NAT' (highlighted), 'QoS', 'VLAN', and 'ADSL'. The main content area is titled 'NAT' and contains the following configuration options:

- Virtual Circuit:
- NAT Status: Activated
- Number of IPs: Single Multiple
- DMZ
- Virtual Server

Virtual Circuit – The Virtual Circuit (VC) properties of the ATM VC interface identify a unique path that your ADSL/Ethernet router uses to communicate via the ATM-based network with the telephone company central office equipment.

Nat Status – This field shows the current status of the NAT function for the current VC.

Number of IPs – This field is to specify how many IPs are provided by your ISP for current VC. It can be single IP or multiple IPs. Note: For VCs with single IP, they share the same DMZ & Virtual servers; for VCs with multiple IPs, each VC can set DMZ and Virtual servers. Furthermore, for VCs with multiple IPs, they can define the Address Mapping rules; for VCs

with single IP, since they have only one IP, there is no need to individually define the Address Mapping rule.

DMZ / Virtual Server / IP Address Mapping – opens corresponding page:

- **DMZ**

A **DMZ** (de-militarized zone) is a host between a private local network and the outside public network. It prevents outside users from getting direct access to a server that has company data. Users of the public network outside the company can access only the DMZ host.

The screenshot shows the web interface for Cerberus P 6311-07A. The top navigation bar includes 'PENTAGRAM THE PERFECT SIMPLICITY' and 'Cerberus P 6311-07A'. Below this is a main menu with 'Advanced', 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. The 'Advanced Setup' menu is expanded to show 'Firewall', 'Routing', 'NAT', 'QoS', 'VLAN', and 'ADSL'. The 'DMZ' section is active, showing 'DMZ setting for: Single IP Account', 'DMZ: Enabled (radio button selected) / Disabled (radio button unselected)', and 'DMZ Host IP Address: 0.0.0.0'. At the bottom, there are 'SAVE' and 'BACK' buttons.

DMZ setting for – Option selected in **Number of IPs** field in main NAT window.

DMZ – Toggle the DMZ function Enabled or Disabled.

DMZ Host IP Address – Enter the specified IP Address for DMZ host on the LAN side

When you are done making changes, click on **SAVE** to save your changes or on **BACK** to return to the previous screen.

- **Virtual Server**

The Virtual Server is the server or server(s) behind NAT (on the LAN), for example, Web server or FTP server, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Cerberus P 6311-07A

Advanced Quick Start Interface Setup **Advanced Setup** Access Management Maintenance Status Help

Firewall Routing **NAT** QoS VLAN ADSL

Virtual Server

Virtual Server for : Single IP Account

Rule Index: 1

Application: - -

Protocol: ALL

Start Port Number: 0

End Port Number: 0

Local IP Address: 0.0.0.0

Virtual Server Listing

Rule	Application	Protocol	Start Port	End Port	Local IP Address
1	-	-	0	0	0.0.0.0
2	-	-	0	0	0.0.0.0
3	-	-	0	0	0.0.0.0
4	-	-	0	0	0.0.0.0
5	-	-	0	0	0.0.0.0
6	-	-	0	0	0.0.0.0
7	-	-	0	0	0.0.0.0
8	-	-	0	0	0.0.0.0
9	-	-	0	0	0.0.0.0
10	-	-	0	0	0.0.0.0
11	-	-	0	0	0.0.0.0
12	-	-	0	0	0.0.0.0
13	-	-	0	0	0.0.0.0
14	-	-	0	0	0.0.0.0
15	-	-	0	0	0.0.0.0
16	-	-	0	0	0.0.0.0

SAVE DELETE BACK CANCEL

Virtual Server for - selected in **Number of IPs** field in main NAT window.

Rule Index – The Virtual server rule index for this VC. You can specify up to 10 rules. All the VCs with single IP will use the same Virtual Server rules.

Application – Enter application name or select one of predefined template.

Protocol – Select protocol for which selected rule will be active.

Start Port Number / End Port Number – Enter the specific Start and End Port number you want to forward. If

it is one port only, you can enter the End port number the same as Start port number. For example, set the FTP Virtual server, you can set the start and end port number to 21.

Local IP Address – Enter the IP Address for the Virtual Server in LAN side.

Virtual Server Listing – This is a listing of all virtual servers you have set.

When you are done making changes, click on **SAVE** to save your changes, **DELETE** to delete the rule with the parameters you set, **BACK** to return to the previous screen or **CANCEL** to discard changes.

● **IP Address Mapping**

The IP Address Mapping is for those VCs that with multiple IPs. The IP Address Mapping rule is per-VC based. (only for Multiple IPs' VCs).

Advanced Quick Start Interface Setup **Advanced Setup** Access Management Maintenance Status Help

Firewall Routing **NAT** QoS VLAN ADSL

IP Address Mapping

Address Mapping Rule : PVC0

Rule Index : 1

Rule Type : One-to-One

Local Start IP : 0.0.0.0

Local End IP : N/A

Public Start IP : 0.0.0.0 (0.0.0.0 for modem's WAN IP)

Public End IP : N/A

Address Mapping List

Rule	Type	Local Start IP	Local End IP	Public Start IP	Public End IP
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

SAVE DELETE BACK CANCEL

Address Mapping Rule – PVC to set.

Rule Index – The Virtual server rule index for this VC. You can specify up to 16 rules. All the VCs with single IP will use the same Virtual Server rules.

Rule Type – There are 4 types of **One-to-One**, **Many-to-One**, **Many-to-Many Overload** and **Many-to-Many No-Overload**.

Local Start IP / Local End IP – Enter the local IP address you plan to map to. Local Start IP is the starting local IP address & Local End IP is the ending local IP address. If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.

Public Start IP / Public End IP – Enter the Public IP Address you want to do NAT. Public Start IP is the starting Public IP Address and Public End IP is the ending Public IP Address. If you have a Dynamic IP, enter 0.0.0.0 as the Public Start IP.

When you are done making changes, click on **SAVE** to save your changes, **DELETE** to delete the rule with the parameters you set, **BACK** to return to the previous screen or **CANCEL** to discard changes.

QoS

QoS (Quality of Service) will provide better service of selected network traffic over various technologies. Deploying QoS management to guarantee that all application receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Advanced Quick Start Interface Setup **Advanced Setup** Access Management Maintenance Status Help

Firewall Routing NAT **QoS** VLAN ADSL

Quality of Service

QoS: Activated Deactivated
 Summary: [QoS Settings Summary](#)

Rule

Rule Index: 1

Active: Activated Deactivated

Application: [Dropdown]

Physical Ports: [Enet1] [Enet2] [Enet3] [Enet4]

Destination MAC: [Text Field]

IP: [Text Field]

Mask: [Text Field]

Port Range: [Text Field] - [Text Field]

Source MAC: [Text Field]

IP: [Text Field]

Mask: [Text Field]

Port Range: [Text Field] - [Text Field]

Protocol ID: [Dropdown]

Vlan ID Range: [Text Field] - [Text Field]

IPP/DSCP Field: IPP/TOS DSCP

IP Precedence Range: [Text Field] - [Text Field]

Type of Service: [Dropdown]

DSCP Range: [Text Field] - [Text Field] (Value Range: 0 ~ 63)

802.1p: [Text Field] - [Text Field]

Action

IPP/DSCP Field: IPP/TOS DSCP

IP Precedence Marking: [Dropdown]

Type of Service Marking: [Dropdown]

DSCP Marking: [Text Field] (Value Range: 0 ~ 63)

802.1p Marking: [Text Field]

Queue #: [Dropdown]

[ADD] [DELETE] [CANCEL]

QoS – Choose whether QoS will be **Activated** or **Deactivated**.

Summary – Click on **QoS Settings Summary** button to open summary window.

Rule – Parameters set in this paragraph describes which packets will apply to this rule.

- **Rule Index** – Select QoS rule to edit.
- **Active** – Choose whether selected QoS rule will be **Activated** or **Deactivated**.
- **Application** – Choose application protocol for this Rule: **IGMP, SIP, H.323, MGCP, SNMP, DNS, DHCP, RIP, RSTP, RTCP** or **RTP**.
- **Physical Ports** – Choose Ethernet ports that will use this rule.
- **Destination MAC** – Enter destination physical address (MAC).
- **IP** – Enter destination IP address.
- **Mask** – Enter destination subnet mask.

- **Port Range** – Enter destination port range.
- **Source MAC** – Enter source physical address (MAC).
- **IP** – Enter source IP address.
- **Mask** – Enter source subnet mask.
- **Port Range** – Enter source port range.
- **Protocol ID** – Select protocol: **TCP/UDP, TCP, UDP, ICMP** or **IGMP**.
- **Vlan ID Range** – Enter range of VLAN IDs.
- **IPP/DS Field** – Select packet priority standard: **IPP/TOS** (IP Precedence Range / Type of Service) or **DSCP** (DiffServ Code Point).
- **IP Precedence Range** – Select range of IPP/TOS values (0-7).
- **Type of Service** – Select additional ToS parameter.
- **DSCP Range** – Select range of DSCP values (0 ~ 63).
- **802.1p** – Select range of CoS values (0-7).

Action – This paragraph describes what action will be taken when rule parameters are true.

IPP/DS Field – Select packet priority standard: **IPP/TOS** or **DSCP**

IP Precedence Remarking – Will change **IPP/TOS** of a packet to selected value (0-7).

Type of Service Remarking – Will change additional **ToS** parameter of a packet to selected.

DSCP Remarking – Will change **DSCP** of a packet to selected value (0-63).

802.1p Remarking – Will change **CoS** value to selected (0-7). In second field you can specify type a packet: **Key Net Traffic (RIP, OSPF), Voice, Video, IGMP, Key Data.**

Queue # – Select queue to which packet will be send.

When you are done making changes, click on **SAVE** to save your changes, **DELETE** to delete the rule with the parameters you set or **CANCEL** to discard changes.

- **QoS Settings Summary**

In this window you can see all configured QoS rules



QoS Settings Summary

Rules									Actions		
#	Active	Physical Ports	Destination	Source	Protocol ID	VLAN ID	IPP/TOS (DSCP)	802.1p	IPP/TOS (DSCP) Remarking	802.1p Remarking	Queue #
			MAC IP/Mask Port Range	MAC IP/Mask Port Range							
-	N	-	-	-	-	-	-	-	-	-	-

e:ethernet, NS: Normal service, MD: Minimize delay, MT: Maximize throughput, MR: Maximize reliability, MC: Minimize monetary cost, HH: Highest, H: High, M: Medium, L: Low.

VLAN

Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization.

- Port-Based VLAN: each physical router port is configured with an access list specifying membership in a set of VLANs.
- ATM VLAN-using LAN Emulation (LANE) protocol to map Ethernet packets into ATM cells and deliver them to their destination by converting an Ethernet MAC address into an ATM address.

The key for the IEEE 802.1Q to perform the above functions is in its tags. 802.1Q-compliant switch ports can be configured to transmit tagged or untagged frames. A tag field containing VLAN (and/or 802.1p priority) information can be inserted into an Ethernet frame. If a port has an 802.1Q-compliant device attached (such as another switch), these tagged frames can carry VLAN membership information between switches, thus letting a VLAN span multiple switches. However, it is important to ensure ports with non-802.1Q-compliant devices attached are configured to transmit untagged frames. Many NICs for PCs and printers are not 802.1Q-compliant. If they received a tagged frame, they will not understand the VLAN tag and will drop the frame. Also, the maximum legal Ethernet frame size for tagged frames was increased in 802.1Q (and its companion, 802.3ac) from 1518 to 1522 bytes. This could cause network interface cards and older switches to drop tagged frames as "oversized".

The screenshot shows the Pentagram network management interface. At the top left is the Pentagram logo with the tagline "THE PERFECT SIMPLICITY". The top right corner displays "Cerberus P 6311-07A". A navigation bar contains several tabs: "Quick Start", "Interface Setup", "Advanced Setup" (which is highlighted in orange), "Access Management", "Maintenance", "Status", and "Help". Below this bar, a secondary row of tabs includes "Firewall", "Routing", "NAT", "QoS", "VLAN" (highlighted in orange), and "ADSL". The main content area has a "VLAN" header. Below the header, there is a "VLAN Function" section with two radio buttons: "Activated" (unselected) and "Deactivated" (selected). Below the radio buttons are two blue circular buttons with right-pointing arrows: "Assign VLAN PVID for each interface" and "Define VLAN Group".

- VLAN Function** – Select if VLAN will be **Activated** or **Deactivated**.
Assign VLAN PVID for each interface – Click to open **PVID Assign** screen.
Define VLAN Group – Click to open **VLAN Group Setting** screen.

- **PVID Assign**

In this screen you can assign PVID (VLAN ID) to each ATM VC or Ethernet (LAN) port.

The screenshot shows the web interface for the Cerberus P 6311-07A. At the top left is the Pentagram logo with the tagline "THE PERFECT SIMPLICITY". The top right corner displays the device name "Cerberus P 6311-07A". Below the logo is a navigation menu with tabs: "Advanced" (selected), "Quick Start", "Interface Setup", "Advanced Setup", "Access Management", "Maintenance", "Status", and "Help". Under "Advanced Setup", there are sub-tabs: "Firewall", "Routing", "NAT", "QoS", "VLAN" (selected), and "ADSL". The main content area is titled "PVID Assign" and contains two sections of input fields. The first section is for ATM VCs, with labels "ATM VC #:" followed by "PVID" and a text input field containing the value "1". This is repeated for VC #1 through VC #7. The second section is for Ethernet ports, with labels "Ethernet Port #:" followed by "PVID" and a text input field containing the value "1". This is repeated for Port #1 through Port #4. At the bottom of the screen, there is an orange bar containing three buttons: "SAVE", "CANCEL", and "NEXT".

When you are done making changes, click on **SAVE** to save your changes, **CANCEL** to discard changes or **NEXT** to go to **VLAN Group Setting** screen.

● **VLAN Group Setting**

Based on each VLAN group, you can configure each group's VLAN setting. You can configure up to 8 VLAN settings. Remember to select **Tagged** option only if device on the other side supports tagged packets, otherwise those packets will be dropped.

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Advanced | Quick Start | Interface Setup | **Advanced Setup** | Access Management | Maintenance | Status | Help

Firewall | Routing | NAT | QoS | **VLAN** | ADSL

VLAN Group Setting

VLAN Index:

Active: Yes No

VLAN ID: (Decimal)

ATM VCs:

Tagged	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port #	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	0	1	2	3	4	5	6

Ethernet:

Port #	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	1	2	3	4

VLAN Group Summary

Group	Active	ID	VLAN Group Ports	VLAN Tagged Ports
1	Yes	1	e1,e2,e3,e4,u,,p0,p1,p2,p3,p4,p5,p6,p7	

p.pvc, e.ethernet

VLAN Index – Select PVID you wish to change.

Active – Select **Yes** to activate or **No** to deactivate selected PVID.

VLAN ID – Frames will be assigned VLAN ID displayed here.

ATM – Select VC, which will be assigned to this VLAN group (**Port #**) and select which VC will sent tagged frames (**Tagged**).

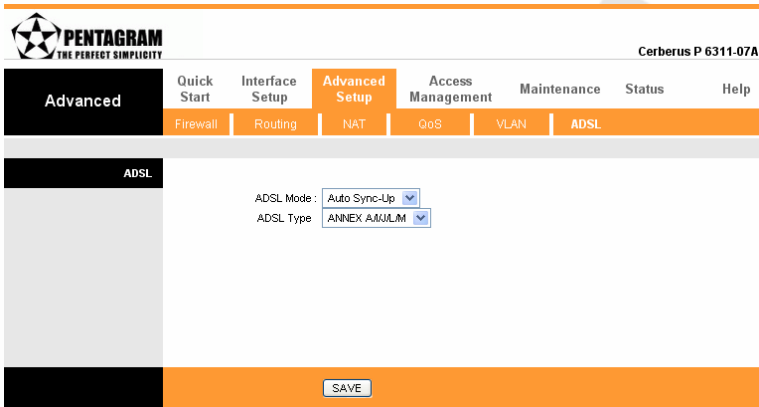
Ethernet – Select Ethernet port, which will be assigned to this VLAN group.

VLAN Group Summary – List of all configured PVIDs.

When you are done making changes, click on **SAVE** to save your changes, **DELETE** to delete the rule with the parameters you set or **CANCEL** to discard changes.

ADSL

Select this option to set ADSL Mode and ADSL Type information.



PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Advanced | Quick Start | Interface Setup | **Advanced Setup** | Access Management | Maintenance | Status | Help

Firewall | Routing | NAT | QoS | VLAN | ADSL

ADSL

ADSL Mode: Auto Sync-Up ▼
ADSL Type: ANNEX A/M/J/L/M ▼

SAVE

ADSL Mode – Select which mode your ADSL connection uses from the dropdown list. The option has **Auto Sync-up**, **ADSL2+**, **ADSL2**, **G.DMT**, **T1.413**, **G.LITE**.

ADSL Type – Select the ADSL type you use from the dropdown list: **ANNEX A**, **ANNEX I**, **ANNEX A/L**, **ANNEX M**, **ANNEX A/I/J/L/M**.

When you are done making changes, click on **SAVE** to save your changes.

Access Management Tab

ACL

Go to **Access Management** → **ACL** to enable remote management. Access Control Listing (ACL) is a management tool that acts as a filter for incoming or outgoing packets, based on application. You may use telnet or Web to remotely manage the ADSL Router. User just needs to enable Telnet or Web and give it an IP address that wants to access the ADSL Router. The default IP 0.0.0.0 allows any client to use this service to remotely manage the ADSL Router.

The screenshot shows the Pentagram router's web interface. The top navigation bar includes 'Access Management', 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management' (highlighted), 'Maintenance', 'Status', and 'Help'. Under 'Access Management', there are sub-tabs: 'ACL', 'Filter', 'SNMP', 'UPnP', 'DDNS', and 'CWMP'. The 'ACL' sub-tab is active.

The 'Access Control Setup' section has 'ACL' set to 'Deactivated'. The 'Access Control Editing' section shows 'ACL Rule Index' as 1, 'Active' as 'No', 'Secure IP Address' as 0.0.0.0, 'Application' as 'yWeb', and 'Interface' as 'Both'. The 'Access Control Listing' section shows a table with the following data:

Index	Active	Secure IP Address	Application	Interface
1	No	0.0.0.0	yWeb	Both

At the bottom, there are 'SAVE', 'DELETE', and 'CANCEL' buttons.

ACL – There has **Activated & Deactivated** option. The default setting is Deactivated which means all IP can access via router. If you choose Activated, you only can access via router by listed IP addresses.

ACL Rule Index – Index number from 1 and up to 16.

Active – Once you choose **Yes** then you can access the IP via router.

Application – Each of these labels denotes a service that you may use to remotely manage the Router. Choices are **Web, FTP, Telnet, SNMP, Ping, ALL**.

Interface – Select the access interface. Choices are **WAN, LAN** and **Both**.


UWAGA!

- You must set one ACL index to access your router via LAN interface. If you don't, your router cannot access other listed IP Address. (Refer to Index 1).
- Remember! Once you active your ACL function, you only can access via router by listed Secure IP Address.

When you are done making changes, click on **SAVE** to save your changes, **DELETE** to delete the rule with the parameters you set or **CANCEL** to discard changes.

Filter

The Router provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attackers. Appearance of this tab is dependent on option selected from **Filter Type Selection** list.



PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Access Management

Quick Start

Interface Setup

Advanced Setup

Access Management

Maintenance

Status

Help

ACL

Filter

SNMP

UPnP

DDNS

CWMP

Filter

Filter Type

Filter Type Selection: IP / MAC Filter

IP / MAC Filter Set Editing

IP / MAC Filter Set Index: 1

Interface: PVC0

Direction: Both

IP / MAC Filter Rule Editing

IP / MAC Filter Rule Index: 1

Rule Type: IP

Active: Yes No

Source IP Address: (0.0.0.0 means Don't care)

Subnet Mask:

Port Number: (0 means Don't care)

Destination IP Address: (0.0.0.0 means Don't care)

Subnet Mask:

Port Number: (0 means Don't care)

Protocol: TCP

Rule Unmatched: Forward

IP / MAC Filter Listing

IP / MAC Filter Set Index: 1 Interface: - Direction: -

#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-

SAVE
DELETE
CANCEL

● **IP / MAC Filter**

IP / MAC Filter enables you to filter data based on source MAC Address or source/destination IP Address or Port number.

Filter

Filter Type

Filter Type Selection: IP / MAC Filter

IP / MAC Filter Set Editing

IP / MAC Filter Set Index: 1

Interface: PVC0

Direction: Both

IP / MAC Filter Rule Editing

IP / MAC Filter Rule Index: 1

Rule Type: IP

Active: Yes No

Source IP Address: (0.0.0.0 means Don't care)

Subnet Mask:

Port Number: (0 means Don't care)

Destination IP Address: (0.0.0.0 means Don't care)

Subnet Mask:

Port Number: (0 means Don't care)

Protocol: TCP

Rule Unmatched: Forward

IP / MAC Filter Listing

IP / MAC Filter Set Index		Interface			Direction			
#	Active	Src Address	Mask	Dest IP Mask	Src Port	Dest Port	Protocol	Unmatched
1	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-

Filter

Filter Type

Filter Type Selection: IP / MAC Filter

IP / MAC Filter Set Editing

IP / MAC Filter Set Index: 1

Interface: PVC0

Direction: Both

IP / MAC Filter Rule Editing

IP / MAC Filter Rule Index: 1

Rule Type: MAC

Active: Yes No

MAC Address: 00:00:00:00:00:00

Rule Unmatched: Forward

IP / MAC Filter Listing

IP / MAC Filter Set Index		Interface			Direction			
#	Active	Src Address	Mask	Dest IP Mask	Src Port	Dest Port	Protocol	Unmatched
1	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-

IP / MAC Filter Set Index – The IP / MAC Filter Set Index from 1 to 12 and each index can set up to 6 IP / MAC Filter.

Interface – Choices from **PVC0** to **PVC7** and **LAN**.

Direction – Choices are **Both**, **Incoming** and **Outgoing**. Select which direction of data flow you wish to apply the filters to. Note that **Incoming** and **Outgoing** are from the point of view of your router, relative to the interface you select. **For WAN**, data coming from outside your system is considered Incoming and data leaving your system is Outgoing. **For LAN**, data leaving your system is considered Incoming and data entering your system is Outgoing.

IP / MAC Filter Rule Index – Select the IP / MAC Filter Rule Index you wish to modify.

Rule Type – Select filtering by **IP** or **MAC** address. Appearance of next paragraphs depends on option you select from this list.

Active – Toggle this rule index on or off with **Yes** or **No**, respectively.

Source IP Address – Enter the source IP address you wish to deny access to your system.

Subnet Mask – Enter the subnet mask of the source IP address.

Port Number – Enter the port number of the source IP address. Note that 0 means all that ports are allowed.

Destination IP Address – Enter the destination IP address that you wish to deny access to your system.

Subnet Mask – Enter the subnet mask of the destination IP address.

Port Number – Enter the port number of the destination IP address. Note that 0 means that all ports are allowed.

Protocol – Select the protocol to filter. Choices are **TCP**, **UDP**, and **ICMP**.

MAC Address (only when **MAC** is selected in **Rule Type** option) – enter source MAC address.

Rule Unmatched – Choices are **Forward** and **Next**. Select what happens to the data in question if the rule you are currently editing is unmatched.

- **Next** means that the data is then compared to the next IP filter rule.
- **Forward** means that the data will be allowed into your system. Note that a **Forward** rule should be the last rule, as no data will be compared to rules after a **Forward** rule.

IP / MAC Filter Set Index – Select the IP / MAC filter set you wish to view.

Please follow below steps to set your IP Filter:

- **IP / MAC Filter Set Editing:** Choose your **IP / MAC Filter Set Index**, Interface and Direction options. Remember, Interface and Direction functions are affected with IP / MAC Filter Set Index. EX: if your 1st index set of IP / MAC filter set PVC0 as Interface and Outgoing as Direction, so the list of 1st IP / MAC Filter will be PVC0 and Outgoing as their settings
- **IP / MAC Filter Rule Editing:** Select the **IP / MAC Filter Rule Index** (up to 6 numbers for each set index), select IP as a **Rule Type** and choose **Active** option. As an example, **Source IP Address** is 192.168.1.10, **Subnet Mask** is 255.255.255.255, **Destination IP Address & Subnet Mask** is 0.0.0.0, **Port Number** is 80. And, **Protocol** sets TCP. From this setting, it filters 192.168.1.14, so it cannot access the web. Notice, each IP / MAC Filter Set Index can has up to 6 filters IP. At “**Rule Unmatched**” option, you must choose **NEXT** until the last filter IP choose **Forward**.
- After every setting is done, click **SAVE** to continue next IP / MAC Filter Editing.

- **Application Filter**

Application Filter enables you to block popular Instant Messaging applications and Real Audio/Video.

Filter

Filter Type

Filter Type Selection:

Application Filter Editing

Application Filter: Activated Deactivated

ICQ: Allow Deny

MSN: Allow Deny

YMSG: Allow Deny

Real Audio/Video: Allow Deny

Application Filter – Select this option to Activate / Deactivate the Application filter.

ICQ – Select this option to **Allow / Deny** ICQ.

MSN – Select this option to **Allow / Deny** MSN.

YMSG – Select this option to **Allow / Deny** Yahoo messenger.

Real Audio/Video – Select this option to **Allow / Deny** Real Audio/Video.

- **URL Filter**

URL Filter enables you to block access to web sites based on keywords.

Filter

Filter Type

Filter Type Selection:

URL Filter Editing

Active: Yes No

URL Index:

URL:

URL Filter Listing

Index	URL
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

Active – Select Active to enable URL Filter.

URL Index – This is item number.

URL – Allow you to prevent users on your network from accessing particular websites by their URL.

SNMP

The **Simple Network Management Protocol (SNMP)** is used for exchanging information between network devices. It enables a host computer to access configuration, performance, and other system data that resides in a database on the modem. The host computer is called a **management station** and the modem is called an **SNMP agent**. The data that can be accessed via SNMP is stored in a **Management Information Database (MIB)** on the modem.

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Access Management	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	ACL	Filter	SNMP	UPnP	DDNS	CWMP	

SNMP

Get Community:

Set Community:

Get Community – Select to set the password for incoming **Get-** and **GetNext** request from management station.

Set Community – Select to set the password for incoming **Set** request from management station. The default password is **cerberus**.

When you are done making changes, click on **SAVE** to save your changes.

UPnP

UPnP (Universal Plug and Play) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. UPnP broadcasts are only allowed on the LAN.

UPnP hardware is identified as an icon in the Network Connections folder (in Windows XP & Windows ME). Each UPnP-compatible device that is installed on your network will appear as a separate icon.

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Access Management	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	ACL	Filter	SNMP	UPnP	DDNS	CWMP	

Universal Plug & Play

UPnP: Activated Deactivated

Auto-configured: Activated Deactivated (by UPnP-enabled Application)

UPnP – You can choose **“Activated”** or **“Deactivated”** option from this session.

Auto-Configured – UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. Choose “Activated” option to allow UPnP-enabled applications to automatically configure the ADSL Router so that they can communicate through the ADSL Router, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. If you don't want to make configuration changes through UPnP, just choose “Deactivated”.

Click **SAVE** to save the setting to the ADSL Router.

DDNS

The **Dynamic Domain Name System** allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a DNS-like address (for instance myhost.dns.org, where my host is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address. First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name. The Dynamic DNS service provider will give you a password or key.

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Access Management	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	ACL	Filter	SNMP	UPnP	DDNS	QWMP	

Dynamic DNS

Dynamic DNS: Activated Deactivated

Service Provider:

My Host Name:

E-mail Address:

Username:

Password:

Wildcard support: Yes No

Dynamic DNS – Choose the option for **Activated** or **Deactivated** DDNS.

Service Provider – The default Dynamic DNS service provider is **www.dyndns.org**.

My Host Name – Type the domain name assigned to your ADSL by your Dynamic DNS provider.

E-mail Address – Type your e-mail address.

Username – Type your user name.

Password – Type the password assigned to you.

Wildcard support – Select Yes or No to turn on DYNDNS Wildcard. Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

Click **SAVE** to save your changes.

CWMP

CWMP page allows you to set up connection parameters that cannot be seen by end users. CPE WAN Management Protocol (a.k.a. TR-069) is intended for communication between a CPE (Customer Premise Equipment) and Auto-Configuration Server (ACS). CWMP defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework.

The CWMP is intended to support a variety of functionalities to manage a collection of CPE, including the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Software/firmware image management
- Status and performance monitoring
- Diagnostics

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Access Management	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	ACL	Filter	SNMP	UPnP	DDNS	CWMP	

CWMP Setup

CWMP : Activated Deactivated

Login ACS

URL :

User Name :

Password :

Connection Request

Path :

Port :

UserName :

Password :

Periodic Inform

Periodic Inform : Activated Deactivated

Interval :

Login ACS – Enter **URL**, **User Name** and **Password** needed to log in to the ACS (Auto Configuration Server).

Connection Request – Enter **Path**, **Port**, **UserName** and **Password** needed for Connection Request.

Periodic Inform – Select whether Periodic Inform function will be **Activated** or **Deactivated** and then enter time **Interval**.

Maintenance Tab

Administration

There is only one account that can access Web-Management interface-**Administration**. Admin has read/write access privilege. In this web page, you can set new password for admin.

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Maintenance | Quick Start | Interface Setup | Advanced Setup | Access Management | **Maintenance** | Status | Help

Administration | Time Zone | Firmware | SysRestart | Diagnostics

Administrator

Username : admin

New Password :

Confirm Password :

SAVE CANCEL

New Password – Type the new password in this field.

Confirm Password – Type the new password again in this field.

Click **SAVE** to save your changes.

Note: If you ever forget the password to log in, you may press the **DEFAULT** button up to 6 second to restore the factory default settings. The Factory Default Settings for User Name & Password are **admin & pentagram**.

Time Zone

The system time is the time used by the device for scheduling services. You can manually set the time or connect to a NTP (Network Time Protocol) server. If an NTP server is set, you will only need to set the time zone. If you manually set the time, you may also set Daylight Saving dates and the system time will automatically adjust on those dates.

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Maintenance | Quick Start | Interface Setup | Advanced Setup | Access Management | **Maintenance** | Status | Help

Administration | **Time Zone** | Firmware | SysRestart | Diagnostics

Time Zone

Current Date/Time : 06/06/2006 06:06:06

Time Synchronization

Synchronize time with : NTP Server automatically
 PC's Clock
 Manually

Time Zone : (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Daylight Saving : Enabled Disabled

NTP Server Address : 0.0.0.0 (0.0.0.0: Default Value)

SAVE CANCEL

● **NTP Server automatically**

The screenshot shows the 'Time Synchronization' configuration page. At the top, it displays 'Current Date/Time : 06/06/2006 06:06:06'. Under 'Synchronize time with:', the radio button for 'NTP Server automatically' is selected. Below this, the 'Time Zone' is set to '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London'. The 'Daylight Saving' option is set to 'Disabled'. The 'NTP Server Address' is set to '0.0.0.0' with a note '(0.0.0.0: Default Value)'.

Current Date/Time – This field displays an updated Date and Time when you reenter this menu.

Time Zone – Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Daylight Saving – Choose “**Enabled**” or “**Disabled**” to use daylight savings time.

NTP Server Address – Type the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information.

Click on **SAVE** to save your changes or on **CANCEL** to discard changes.

● **PC’s Clock**

The screenshot shows the 'Time Synchronization' configuration page. At the top, it displays 'Current Date/Time : 06/06/2006 06:06:06'. Under 'Synchronize time with:', the radio button for 'PC's Clock' is selected. Below this, the 'Date' is set to '6 / 06 / 2006' (Month/Date/Year) and the 'Time' is set to '06 : 06 : 06' (hour:min:sec).

Router will synchronize its clock with computer.

Click on **SAVE** to save your changes or on **CANCEL** to discard changes.

● **Manually**

The screenshot shows the 'Time Synchronization' configuration page. At the top, it displays 'Current Date/Time : 06/06/2006 06:06:06'. Under 'Synchronize time with:', the radio button for 'Manually' is selected. Below this, the 'Date' is set to '6 / 06 / 2006' (Month/Date/Year) and the 'Time' is set to '06 : 06 : 06' (hour:min:sec).

Date – Enter current date.

Time – Enter current time.

Click on **SAVE** to save your changes or on **CANCEL** to discard changes.

Firmware

You can upgrade the firmware of the router and save/load configuration Romfile in this page. During firmware upgrade process all router setting are reset to default values. Thanks to Romfile it is possible to save router's configuration to file and to load this file after upgrade process. Make sure the firmware you want to use is on the local hard drive of the computer. **It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade!!** After a success upload, the system automatically restarts. Please wait for the device to finish restarting. This should take about 2 minutes or more. You need to log in again if you want to access the device.

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Maintenance | Quick Start | Interface Setup | Advanced Setup | Access Management | **Maintenance** | Status | Help

Administration | Time Zone | **Firmware** | SysRestart | Diagnostics


Firmware Romfile Upgrade

Current Firmware Version : 2.10.5.0(QE0.C29)3.6.0.0

New Firmware Location :

New Romfile Location :

Romfile Backup :

Status :
 It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.

Current Firmware Version – This field displays the current firmware version.

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

New Romfile Location – Type in the location of the Romfile you want to upload in this field or click **Browse...** to find it.

ROMFILE SAVE – Click this button to save router's configuration to file.

Click **UPGRADE** to begin the firmware and/or Romfile upload process.

SysRestart

The SysRestart screen allows you to restart your router with either its current settings still in place or the factory default settings.

System Restart with – 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. Otherwise, you can select **Current Settings**. You may also reset your router to factory settings by holding the **DEFAULT** button on the back panel of your router in for 10-12 second while the router is turned on.

Click **RESTART** to start this process.

Diagnostics

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

Virtual Circuit – Select which PVC you wish to test from the dropdown list. The router will automatically run diagnostic tests on that circuit. A green **PASS** means that the given test was passed, a red **FAIL** means that the test was failed and a green **SKIPPED** means that the test was skipped.

Status Tab

Device Info

The Device Info screen is a tool that you use to monitor your ADSL Router. It shows the Firmware Version, WAN, LAN, and MAC address information. Note that these fields are read-only and are not meant for diagnostic purposes. Except the Virtual Circuit, click the drop-down list and select the name of the Virtual Circuit on which the system status is to be shown.

PENTAGRAM
THE PERFECT SIMPLICITY

Cerberus P 6311-07A

Status Quick Start Interface Setup Advanced Setup Access Management Maintenance **Status** Help

Device Info System Log Statistics

Device Information

Firmware Version : 2.10.5.0(UE0.C29)3.6.0.0
MAC Address : 00:06:41:26:b9:e3

LAN

IP Address : 192.168.1.100
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WAN

Virtual Circuit :
Status : Not Connected
Connection Type : PPPoA
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
DNS Server : 0.0.0.0
NAT : Enabled

ADSL

ADSL Firmware Version : FwVer:3.6.0.0_A_TC3085 HwVer:T14.F7_1.0
Line State : Down
Modulation : Multi-Mode
Annex Mode : ANNEX_A

	Downstream	Upstream	
SNR Margin :	N/A	N/A	db
Line Attenuation :	N/A	N/A	db
Data Rate :	0	0	kbps

- **Device Information**

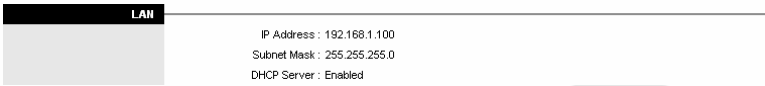
Device Information

Firmware Version : 2.10.5.0(UE0.C29)3.6.0.0
MAC Address : 00:06:41:26:b9:e3

Firmware Version – This field displays current firmware version.

MAC Address – The MAC (Media Access Control) or Ethernet address unique to your modem.

● LAN

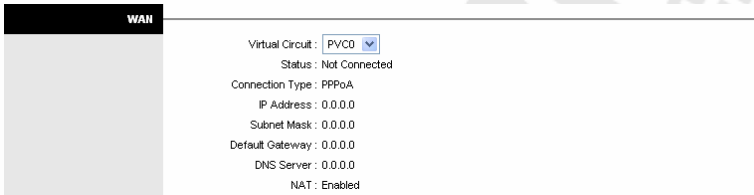


IP Address – The LAN port IP address.

Subnet Mask – The LAN port IP subnet mask.

DHCP Server – The status of **DHCP** Server (Enabled or Disabled).

● WAN



Virtual Circuit – Click the drop-down list and select the name of the Virtual Circuit on which the system status is to be shown.

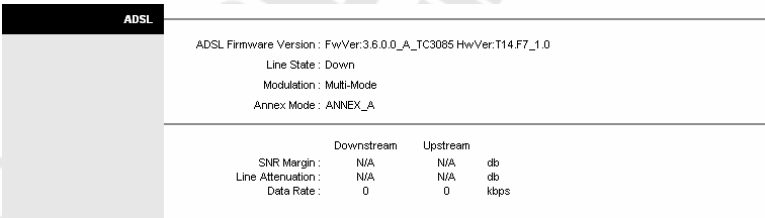
Status – Connected or Not Connected.

Connection Type – The WAN Connection Type.

IP Address / Subnet Mask / Default Gateway / DNS Server – Connection parameters.

NAT – The status of NAT Service (Enabled or Disabled).

● ADSL



ADSL Firmware Version – This field displays current ADSL firmware version.

Line State – This field displays the ADSL connection process and status.

Modulation – This field displays the ADSL modulation status for G.dmt or T1.413.

Annex Mode – This field displays the ADSL annex modes for Annex A.

Downstream / Upstream – Status of SNR Margin, Line Attenuation and Data Rate:

- **SNR Margin** – Amount of increased noise that can be tolerated while maintaining the designed BER (bit error rate). The SNR Margin is set by Central Office DSLAM. If the SNR Margin is increased, bit error rate performance will improve, but the data rate will decrease. Conversely, if the SNR Margin is decreased, bit error rate performance will decrease, but the data rate will increase.
- **Line Attenuation** – Attenuation is the decrease in magnitude of the ADSL line signal between the transmitter (Central Office DSLAM) and the receiver (Client ADSL Modem), measured in dB. It is measured by calculating the difference in dB

between the signal power level received at the Client ADSL Router and the reference signal power level transmitted from the Central Office DSLAM.

- **Data Rate** – This field displays the ADSL data rate.

System Log

The System Log displays data generated or acquired by routine system communication with other devices, such as the results of negotiations with the ISP's computers for DNS and gateway IP addresses. The device keeps a running log of events and activities occurring on the Router. You can click **Save Log** to display a Windows File Download dialog box that enables opening or saving the contents of the log to your PC. To remove all entries from the list, click **Clear Log**. New entries will begin accumulating. If the device is rebooted, the logs are automatically cleared.

The screenshot displays the web interface for the Cerberus P 6311-07A. At the top left is the Pentagram logo with the tagline "THE PERFECT SIMPLICITY". The top right corner shows the device model "Cerberus P 6311-07A". A navigation menu includes "Quick Start", "Interface Setup", "Advanced Setup", "Access Management", "Maintenance", "Status", and "Help". Below this, a sub-menu highlights "Device Info", "System Log", and "Statistics". The main content area is titled "System Log" and contains a large, empty rectangular box. At the bottom of the interface, there are two buttons: "CLEAR LOG" and "SAVE LOG".

Statistics

The ADSL Router keeps statistic of traffic that passes through it. You are able to view the amount of packets that passes through the Router on both the WAN port & the LAN port. The traffic counter will reset if the device is rebooted. You can select **Ethernet/ADSL** to view the statistics report of LAN/WAN.

The screenshot shows the Pentagram router's web interface. At the top left is the Pentagram logo with the tagline 'THE PERFECT SIMPLICITY'. The device model 'Cerberus P 6311-07A' is shown at the top right. A navigation menu includes 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status' (highlighted), and 'Help'. Below the menu, there are tabs for 'Device Info', 'System Log', and 'Statistics'. The 'Traffic Statistics' section is active, showing the 'Interface' set to 'Ethernet'. A table displays transmit and receive statistics for Ethernet, with all values at 0. A 'REFRESH' button is located at the bottom of the statistics area.

Transmit Statistics		Receive Statistics	
Transmit Frames	0	Receive Frames	0
Transmit Multicast Frames	0	Receive Multicast Frames	0
Transmit total Bytes	0	Receive total Bytes	0
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0

- ### Ethernet

The Ethernet screen gives you information on how much data your router has transmitted and received across the Ethernet connection.

This screenshot is identical to the one above, showing the Ethernet traffic statistics page with a 'REFRESH' button.

Transmit Statistics		Receive Statistics	
Transmit Frames	0	Receive Frames	0
Transmit Multicast Frames	0	Receive Multicast Frames	0
Transmit total Bytes	0	Receive total Bytes	0
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0

Click on **REFRESH** to update the screen.

- ### ADSL

The ADSL screen gives you information about how much data your router has transmitted or received across the ADSL connection.

The screenshot shows the ADSL traffic statistics page. The 'Interface' is set to 'ADSL'. The table displays transmit and receive statistics for ADSL, with all values at 0. A 'REFRESH' button is located at the bottom of the statistics area.

Transmit Statistics		Receive Statistics	
Transmit total PDUs	0	Receive total PDUs	0
Transmit total Error Counts	0	Receive total Error Counts	0

Click on **REFRESH** to update the screen.

Help Tab

Router's online help.

Help	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
Quick Start			<ul style="list-style-type: none"> ▶ Quick Start 				
Interface Setup			<ul style="list-style-type: none"> ▶ Internet Settings ▶ LAN Settings 				
Advanced Setup			<ul style="list-style-type: none"> ▶ Firewall ▶ Routing ▶ NAT ▶ QoS ▶ VLAN ▶ ADSL 				
Access Management			<ul style="list-style-type: none"> ▶ ACL ▶ IP Filter ▶ SNMP ▶ UPnP ▶ DDNS 				
Maintenance			<ul style="list-style-type: none"> ▶ Administration ▶ Time Zone ▶ Firmware ▶ SysRestart ▶ Diagnostics 				
Status			<ul style="list-style-type: none"> ▶ Device Info ▶ System Log ▶ Statistics 				

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 **PWR 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.

USB LED

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

1. Check the USB cable connections between your router and the computer or hub;
2. Check for faulty USB cables;
3. Make sure that drivers are installed properly;
4. If these steps fail to correct the problem, contact your local distributor for assistance.

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. Make sure that there is not a console session running;
3. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details;
4. For WAN access, you must configure remote management to allow server access from the WAN (or all);
5. Your computer's and the router's IP addresses must be on the same subnet for LAN access;
6. If you changed the router's LAN IP address, then enter the new one as the URL;
7. Remove any filters in LAN or WAN that block web service.

The web interface does not display properly:

1. Make sure you are using Internet Explorer 5.0 (or compatible) and later versions;
2. Delete the temporary web files and log in again.

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 DEFAULT button for five seconds, and then release it. When the ADSL LED begins to blink, 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.

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, type of encapsulation and type of multiplexing 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, type of encapsulation and type of multiplexing 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 encapsulation only. Make sure that you have entered the correct **Service Type, User Name 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;

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.



NOTES

