

Installation and Operation Manual

PENTAGRAM Cerberus P6371



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

2008-10-07



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

© **2008 PENTAGRAM**

All rights reserved; copying and reproduction is strictly forbidden.

INDEX

INTRODUCTION	5
FEATURES	5
PACKAGE CONTENTS	6
PRODUCT OVERVIEW	6
IMPORTANT NOTES	6
FRONT PANEL	6
BACK PANEL	7
DEFAULT SETTINGS	7
RESETTING ROUTER	7
CONNECTING CERBERUS TO COMPUTER	8
CONFIGURE TCP/IP	8
CONFIGURE ROUTER VIA WEB BROWSER	13
LOGIN	13
NAVIGATION	14
STATUS TAB	15
BASIC SETTINGS / QUICK SETUP	16
NETWORK / LAN	17
NETWORK / WAN	18
NETWORK / MAC CLONE	27
DHCP / DHCP SETTINGS	28
DHCP / DHCP CLIENTS LIST	29
DHCP / ADDRESS RESERVATION	29
FORWARDING / VIRTUAL SERVERS	30
FORWARDING / PORT TRIGGERING	31
FORWARDING / DMZ	33
FORWARDING / UPNP	33
SECURITY / FIREWALL	34
SECURITY / IP ADDRESS FILTERING	35
SECURITY / DOMAIN FILTERING	37
SECURITY / MAC ADDRESS FILTERING	38
SECURITY / REMOTE MANAGEMENT	39
SECURITY / ADVANCED SECURITY	40
STATIC ROUTING	41
IP & MAC BINDING / BINDING SETTINGS	42
IP & MAC BINDING / ARP LIST	43
DYNAMIC DNS	43
SYSTEM TOOLS / TIME SETTINGS	44
SYSTEM TOOLS / FIRMWARE UPGRADE	45
SYSTEM TOOLS / FACTORY DEFAULTS	45
SYSTEM TOOLS / BACKUP AND RESTORE	45
SYSTEM TOOLS / REBOOT	46
SYSTEM TOOLS / LOG	47
SYSTEM TOOLS / STATISTICS	47
TROUBLESHOOTING	49
USING LEDS TO DIAGNOSE PROBLEMS	49
PROBLEMS WITH RESOLVING IP ADDRESS FROM THE ROUTER'S DHCP SERVER IN WINDOWS VISTA	49
PROBLEMS WITH THE WEB INTERFACE	50
PROBLEMS WITH THE LOGIN USERNAME AND PASSWORD	50
PROBLEMS WITH LAN INTERFACE	50
PROBLEMS WITH THE INTERNET ACCESS	50
INTERNET CONNECTION DISCONNECTS:	50



Introduction

The Cerberus P 6371 Router integrates 4-port Switch, firewall and NAT-router. Its design is dedicated to Small Office/Home Office (SOHO) network solutions. The Cerberus P 6371 Router will allow you to connect your network better than ever, sharing Internet Access, files and fun, easily and securely.

Features

- Complies with IEEE 802.3, IEEE 802.3u standards.
- One 10/100M Auto-Negotiation RJ45 WAN port, 4 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX.
- Shares data and Internet access for users, supporting PPPoE, Dynamic IP, Static IP, L2TP, PPTP, BigPond Cable Internet access.
- Supports Virtual Server, Special Application and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing, VPN Pass-through.
- Connecting Internet on demand and disconnecting from the Internet when idle for PPPoE.
- Built-in NAT and DHCP server supporting static IP address distributing.
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering.
- Supports connecting/disconnecting from the Internet on a specified time of day.
- Supports access control, parents and network administrators can establish restricted access policies based on time of day for children or staff.
- Supports Flow Statistics.
- Supports ICMP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD filter.
- Ignores Ping packets from WAN or LAN ports.
- Supports firmware upgrade.

Package Contents

1. PENTAGRAM Cerberus P 6371 router
2. Power adapter 9 V, 0,8 A
3. Ethernet cable (RJ-45)
4. CD
5. Quick Installation Guide

Product Overview

Important Notes

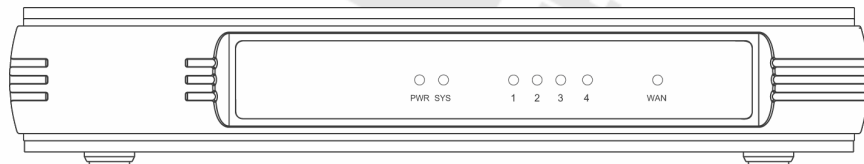


- Do not use the router in high humidity or high temperatures.
- Do not use the same power source for the router as other equipment.
- Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Avoid using this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



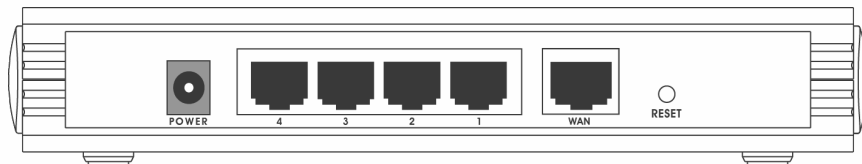
- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

Front Panel



LED	Action	Description
PWR	Not lit	No Power
	Lit up	Power on
SYS	Lit up	The router is initializing
	Flashing	The router is working properly
	Not lit	The router has a hardware error
WAN / 1-4	Not lit	There is no device linked to the corresponding port
	Lit up	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port

Back Panel



Label	Used for...
POWER	Connecting with supplied power adapter
LAN 1-4 (RJ-45)	Connecting with computers/devices through Ethernet cable
WAN (RJ-45)	Connecting with DSL/cable modem through Ethernet cable
RESET	Resetting the device.

Default Settings

Before changing configuration familiarize yourself with these default settings.

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	7200 seconds (2 hours)
User Name	admin
Password	pentagram

It is recommended to change User Name and Password as soon as possible.

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

Resetting router

- Use the **Factory Defaults** function on **System Tools -> Factory Defaults** page in the router's Web-based Utility, or
- Use the **RESET** button: First, turn off the router's power. Second, press and hold the default reset button then turn on the router's power, until the SYS LED lights up (about 3 seconds). Last, release the reset button and wait for the router to reboot.

Connecting Cerberus to Computer.

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.

Configure TCP/IP

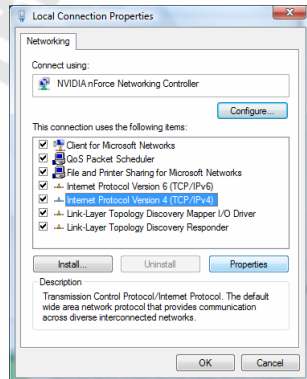
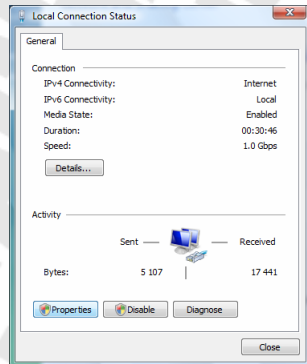
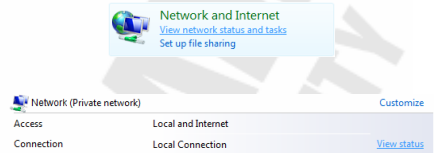
After connecting the computer to the router the TCP/IP protocol should be configured. The protocol should be automatically installed together with Network card drivers. It is advised that TCP/IP should be configured to receive IP address and all the necessary network parameters from DHCP server automatically.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



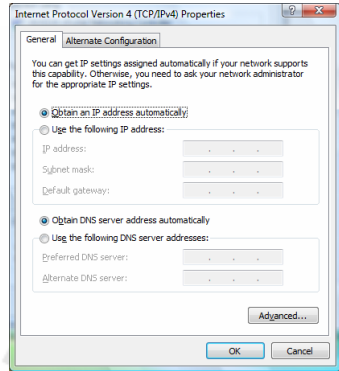
Windows Vista

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

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



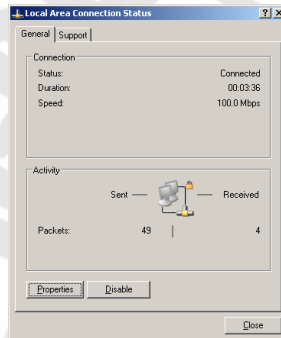
6. On **General** tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
7. Click **OK** to save settings and close **Internet Protocol Version 4 (TCP/IPv4) Properties** window.



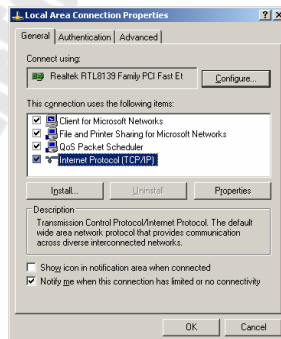
Note: In some cases Windows Vista cannot obtain an IP address from certain router's DHCP server. If you encounter this, follow this steps to resolve this problem (Microsoft Support page) <http://support.microsoft.com/kb/928233/en-us>

Windows 2000/XP

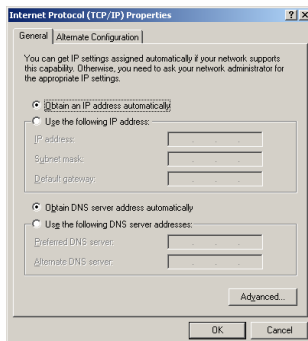
1. Click **Start** → **Settings** → **Control Panel**.
Double-click the **Network Connections** icon (2000/XP Classic view) or click **Network and Internet Connections** icon and then **Network Connections** icon (XP Default view).
2. Double-click the **Local Area Connection** icon.
3. On **General**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



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

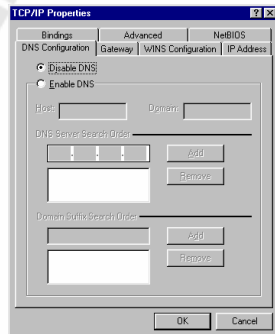
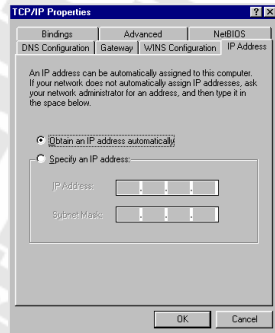
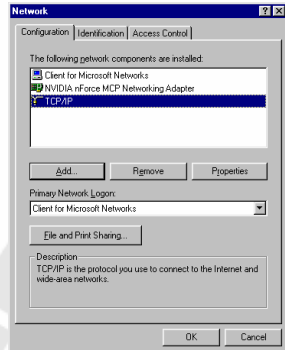


5. On **General** tab, select **Obtain an IP address automatically** and **DNS server address automatically**.
6. Click **OK** to save settings and close **Internet Protocol (TCP/IP) Properties** window.



Windows 95/98/Me

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



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

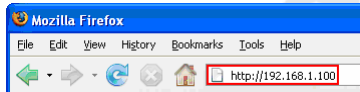
1. click **Start > Run**
2. type **cmd** (Win 2000/XP) or **command** (Win 95/98/ME) and press Enter
3. in command line type **ipconfig /all** and press Enter
4. check if the **IP Address** is **192.168.1.x**

Configure router via web browser

Cerberus P 6371 router can be configured via web browser, which is usually integrated with operating system. Router offers clear and simple interface.

Login


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



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



Navigation


PENTAGRAM
THE PERFECT SIMPLICITY
configuration panel

CERBERUS

P 6371

- Status
- ... Basic Settings ...
- Quick Setup
- Network
- ... Advanced Settings ...
- DHCP
- Forwarding
- Security
- Static Routing
- IP & MAC Binding
- Dynamic DNS
- ... Maintenance ...
- System Tools

Router Status

Firmware Version	3.5.1 Build 070321 Rel:50877na	
Hardware Version	Cerberus P 6371 V1.0.0 081520EF	

LAN

MAC Address:	00-19-ED-F8-2E-9E	
IP Address:	192.168.1.100	
Subnet Mask:	255.255.255.0	

WAN

MAC Address:	00-19-ED-F8-2E-9F	
IP Address:	87.206.51.127	Dynamic IP
Subnet Mask:	255.255.255.0	
Default Gateway:	87.206.51.1	<input type="button" value="Release"/>
DNS Server:	62.179.1.62, 62.179.1.63	

Traffic Statistics

	Received	Sent
Bytes:	1328847380	3028993109
Packets:	15081649	10002346

System Up Time: 3 day(s) 20:02:04

Router Status Help

The **Status** page displays the router's current status and configuration. All information is read-only.

LAN: The following is the information of LAN, as set on the **Network** -> **LAN** page.

- **MAC Address** - The physical address of the router, as seen from the LAN.
- **IP Address** - The LAN IP address of the router.
- **Subnet Mask** - The subnet mask associated with LAN IP address.

WAN: The following parameters apply to the WAN (Internet) port of the router. You can configure them on the **Network** -> **WAN** page.

- **MAC Address** - The physical address of the router, as seen from the Internet.
- **IP Address** - The current WAN (Internet) IP Address. If assigned dynamically, and no connection to Internet, this field will be blank or 0.0.0.0.
- **Subnet Mask** - The subnet mask associated with the WAN (Internet) IP Address.
- **Default Gateway** - The default gateway IP address of the WAN. When you use **Dynamic IP** as connection Internet type, the **Release** button will be displayed here. Click the **Release** button to obtain new IP parameters dynamically from the ISP.
- **DNS Server** - The DNS (Domain Name System) Server IP addresses currently used by the router are shown here. Multiple DNS IP settings are common. In most cases, the first available DNS Server is used.
- **Online Time** - The time that the router keep online. When you choose PPPoE as WAN connection type, the online time will be displayed here. Click the **Connect** or **Disconnect** button to connect to or disconnect from Internet.

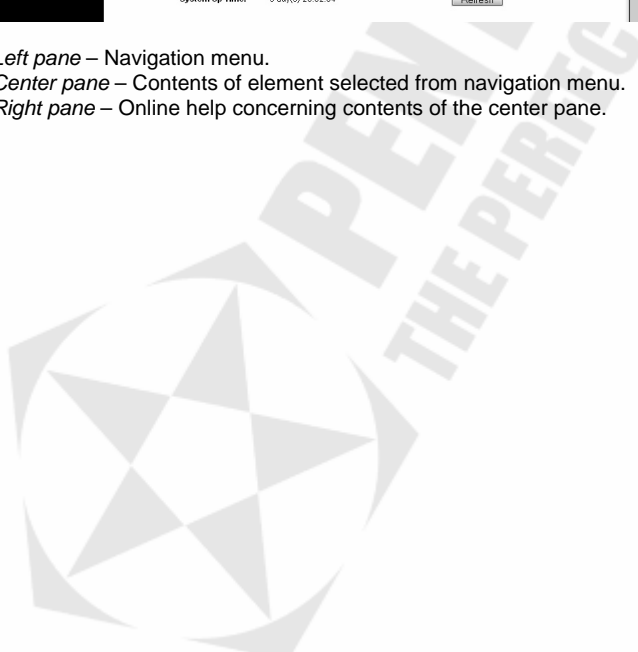
Traffic Statistics: The router traffic statistics.

- **Bytes** - The sum of bytes have been sent out or received from WAN (Internet) port.

Left pane – Navigation menu.

Center pane – Contents of element selected from navigation menu.

Right pane – Online help concerning contents of the center pane.



Status Tab

Router Status

Firmware Version: 3.5.1 Build 070321 Rel.50877na
Hardware Version: Cerberus P 6371 V1.0.0 081520EF

LAN

MAC Address: 00-19-E0-F8-2E-9E
IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0

WAN

MAC Address: 00-19-E0-F8-2E-9F
IP Address: 87.206.51.127 Dynamic IP
Subnet Mask: 255.255.255.0
Default Gateway: 87.206.51.1
DNS Server: 62.179.1.62, 62.179.1.63

Traffic Statistics

	Received	Sent
Bytes:	1328927089	3029057928
Packets:	15062298	10003411

System Up Time: 3 day(s) 20:10:52

Router Status

- **Firmware Version** – Firmware Version.
- **Hardware Version** – Hardware Version.

LAN

- **MAC Address** – MAC address used by router in LAN.
- **IP Address** – IP address used by router in LAN.
- **Subnet Mask** – LAN subnet mask.

WAN

- **MAC Address** – MAC address assigned for WAN port.
- **IP Address** – IP address assigned for WAN port.
- **Subnet mask** – Subnet mask assigned for WAN port.
- **Default Gateway** – The IP address of the default gateway.
- **DNS Server** – The IP address of the DNS server.

Basic Settings / Quick Setup

Quick Setup menu will help you to configure the basic network parameters.

Quick Setup

The quick setup will tell you how to configure the basic network parameters.

To continue, please click the **Next** button.

To exit, please click the **Exit** button.

To begin configuration, click the **Next** button.

Quick Setup - Choose WAN Connection Type

Quick Setup - Choose WAN Connection Type

Please choose WAN Connection Type:

- PPPoE
 Dynamic IP
 Static IP
-

Select WAN Connection Type your ISP is using and click the **Next** button to configure it (not applicable for **Dynamic IP**).

- **Quick Setup - PPPoE**

Quick Setup - PPPoE

Account Name:
Password:

Enter **Account Name** and **Password** provided by your ISP and click the **Next** button, to continue.

- **Quick Setup - Static IP**

Quick Setup - Static IP

IP Address:	<input type="text" value="0.0.0.0"/>
Subnet Mask:	<input type="text" value="0.0.0.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/> (Optional)
Primary DNS:	<input type="text" value="0.0.0.0"/> (Optional)
Secondary DNS:	<input type="text" value="0.0.0.0"/> (Optional)

Enter **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary/Secondary DNS** server address provided by your ISP and click the **Next** button to continue.

Quick Setup - Finish**Quick Setup - Finish**

Congratulations! The router is now connecting you to the Internet. For detail settings, please contact other menus if necessary.

Click the **Finish** button to save changes and exit Quick setup.

Network / LAN**LAN**

MAC Address:	00-19-E0-F8-2E-9E
IP Address:	<input type="text" value="192.168.1.100"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/> ▼

MAC Address – MAC address used by router in LAN.

IP Address – Enter IP address which will be used by router in LAN.

Subnet Mask – Select LAN subnet mask.

Network / WAN

Appearance of this page depends on option selected from **WAN Connection Type** list.

- **Dynamic IP**

Select this **WAN Connection Type**, if your ISP is running a DHCP server.

WAN

WAN Connection Type:

Host Name:

IP Address: 87.206.51.127

Subnet Mask: 255.255.255.0

Default Gateway: 87.206.51.1

MTU Size (in bytes): (The default is 1500, do not change unless necessary.)

Use These DNS Servers

Primary DNS:

Secondary DNS: (Optional)

Get IP with Unicast DHCP (It is usually not required.)

Host Name - This field is required to be filled by some service provider.

IP Address - The IP address assigned by your ISP dynamically.

Subnet Mask - The subnet mask assigned by your ISP dynamically.

Default Gateway - The default gateway assigned dynamically by your ISP.

Click the **Renew** button to renew the IP parameters from your ISP.

Click the **Release** button to release the IP parameters.

MTU Size - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Use These DNS Servers - If your ISP gives you one or two DNS IP addresses, select this option and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from ISP.

Primary DNS / Secondary DNS - (Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP. **Note:** If you get 'Address not found' errors when you go to a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Get IP with Unicast DHCP - A few ISPs' DHCP servers do not support the broadcast applications. If you can't get the IP Address normally, you can choose Unicast. (You generally need not check this option).

Click the **Save** button to save this settings.

- **Static IP**

Select this **WAN Connection Type**, if your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting.

WAN

WAN Connection Type:

IP Address:

Subnet Mask:

Default Gateway: (Optional)

MTU Size (in bytes): (The default is 1500, do not change unless necessary.)

Primary DNS: (Optional)

Secondary DNS: (Optional)

IP Address - Enter the IP address in dotted-decimal notation provided by your ISP.

Subnet Mask - Enter the subnet Mask in dotted-decimal notation provided by your ISP.

Default Gateway - (Optional) Enter the default gateway in dotted-decimal notation provided by your ISP.

MTU Size - The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Primary DNS / Secondary DNS - (Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP.

Click the **Save** button to save this settings.

- **PPPoE**

Select this **WAN Connection Type**, if your ISP provides a PPPoE connection.

WAN

WAN Connection Type:

User Name:

Password:

Wan Connection Mode:

Connect on Demand

Max Idle Time: minutes (0 means remain active at all times.)

Connect Automatically

Time-based Connecting

Period of Time: from : (HH:MM) to : (HH:MM)

Connect Manually

Max Idle Time: minutes (0 means remain active at all times.)

User Name/Password - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

Connect on Demand - You can configure the router to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates. **Note:** Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.

Connect Automatically - Connect automatically after the router is disconnected. To use this option, click the radio button.

Time-based Connecting - You can configure the router to make it connect or disconnect based on time. Enter the start time in HH:MM for connecting and end time in HH:MM for disconnecting in the **Period of Time** fields. **Note:** Only when you have set the system time on **System Tools -> Time page**, the **Time-based Connecting** function can take effect.

Connect Manually - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect your Internet connection, and not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link requested. **Note:** Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.

Click the **Connect** button to connect immediately.

Click the **Disconnect** button to disconnect immediately.

Click the **Save** button to save this settings.

Click the **Advanced** button to set up the advanced options:

PPPoE Advanced Settings

MTU Size (in bytes):	<input type="text" value="1480"/>	(The default is 1480, do not change unless necessary.)
Service Name:	<input type="text"/>	
AC Name:	<input type="text"/>	
	<input type="checkbox"/> Use IP address specified by ISP	
ISP specified IP Address:	<input type="text" value="0.0.0.0"/>	
Detect Online Interval:	<input type="text" value="0"/>	Seconds (0 ~ 120 seconds, 0 means not detecting.)
	<input type="checkbox"/> Use the following DNS Servers	
Primary DNS:	<input type="text" value="0.0.0.0"/>	
Secondary DNS:	<input type="text" value="0.0.0.0"/>	(Optional)

MTU Size (in bytes) - The default MTU size is 1480 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.

Service Name/AC Name - The service name and AC (Access Concentrator) name, it should not be done unless you are sure it is necessary for your ISP.

ISP Specified IP Address - If you know that your ISP does not automatically transmit IP address to the router during login, click **Use the IP Address specified by ISP** checkbox and enter the IP address in dotted-decimal notation, which was provided by your ISP.

Detect Online Interval - The default value is 0, you can input the value between 0 and 120. The router will detect Access Concentrator online every interval seconds. If the value is 0, it means not detecting.

Use These DNS Servers - If your ISP gives you one or two DNS IP addresses, select this option and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from ISP.

Primary DNS / Secondary DNS - (Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP. **Note:** If you get 'Address not found' errors when you go to a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Click the **Save** button to save this settings.

Click the **Return** button when finished.

- **802.1X + Dynamic IP**

Select this **WAN Connection Type**, if your ISP provides IEEE802.1X connection.

WAN

WAN Connection Type:

User Name:

Password:

Host Name:

IP Address:

Subnet Mask:

Default Gateway:

MTU Size (in bytes): (The default is 1500, do not change unless necessary)

Use These DNS Servers

Primary DNS:

Secondary DNS: (Optional)

Get IP with Unicast DHCP (It is usually not required.)

User Name - Enter the user name for 802.1x authentication provided by your ISP

Password - Enter the password for 802.1x authentication provided by your ISP.

Click the **Login** button to start 802.1x authentication.

Click the **Logout** button to end 802.1x authentication.

Host Name - This field is required to be filled by some service provider.

IP Address - The IP address assigned by your ISP dynamically.

Subnet Mask - The subnet mask assigned by your ISP dynamically.

Default Gateway - The default gateway assigned dynamically by your ISP.

Click the **Renew** button to renew the IP parameters from your ISP.

Click the **Release** button to release the IP parameters.

MTU Size - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 bytes. For some ISPs you need reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Use These DNS Servers - If your ISP gives you one or two DNS IP addresses, select this option and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from ISP.

Primary DNS / Secondary DNS - (Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP. **Note:** If you get '*Address not found*' errors when you go to a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Get IP with Unicast DHCP - A few ISPs' DHCP servers do not support the broadcast applications. If you can't get the IP Address normally, you can choose Unicast. (You generally need not check this option).

Click the **Save** button to save this settings.

- **802.1X + Static IP**

Select this **WAN Connection Type**, if your ISP provides IEEE802.1X connection.

WAN

WAN Connection Type:

User Name:

Password:

IP Address:

Subnet Mask:

Default Gateway: (Optional)

MTU Size (in bytes): (The default is 1500, do not change unless necessary.)

Primary DNS: (Optional)

Secondary DNS: (Optional)

User Name - Enter the user name for 802.1x authentication provided by your ISP

Password - Enter the password for 802.1x authentication provided by your ISP.

Click the **Login** button to start 802.1x authentication.

Click the **Logout** button to end 802.1x authentication.

IP Address - Enter the IP address in dotted-decimal notation provided by your ISP.

Subnet Mask - Enter the subnet Mask in dotted-decimal notation provided by your ISP.

Default Gateway - (Optional) Enter the default gateway in dotted-decimal notation provided by your ISP.

MTU Size - The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Primary DNS / Secondary DNS - (Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP. **Note:** If you get 'Address not found' errors when you go to a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Click the **Save** button to save this settings.

- **BigPond Cable**

Select this **WAN Connection Type**, if your ISP provides BigPond Cable (or Heart Beat Signal) connection.

WAN

WAN Connection Type: ▼

User Name:

Password:

Auth Server:

Auth Domain:

MTU Size (in bytes): (The default is 1500, do not change unless necessary.)

Connect on Demand
Max Idle Time: minutes (0 means remain active at all times.)

Connect Automatically

Connect Manually
Max Idle Time: minutes (0 means remain active at all times.)

Disconnected

User Name/Password - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

Auth Server - Enter the authenticating server IP address or host name.

Auth Domain - Type in the domain suffix server name based on your location, eg.

NSW / ACT - **nsw.bigpond.net.au**

VIC / TAS / WA / SA / NT - **vic.bigpond.net.au**

QLD - **qld.bigpond.net.au**

MTU Size (in bytes) - The default MTU size is 1500 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.

Connect on Demand - You can configure the router to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates. **Note:** Sometimes the connection cannot be disconnected

although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.

Connect Automatically - Connect automatically after the router is disconnected. To use this option, click the radio button.

Connect Manually - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect your Internet connection, and not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link requested. **Note:** Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.

Click the **Connect** button to connect immediately.

Click the **Disconnect** button to disconnect immediately.

Click the **Save** button to save this settings.

- **L2TP**

Select this **WAN Connection Type**, if your ISP provides L2TP connection.

WAN

WAN Connection Type:

User Name:

Password:

Disconnected!

Dynamic IP Static IP

Server IP Address Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 0.0.0.0, 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0, 0.0.0.0

MTU Size (in bytes): (The default is 1460, do not change unless necessary.)

Max Idle Time: minutes (0 means remain active at all times.)

Wan Connection Mode:

Connect on Demand

Connect Automatically

Connect Manually

User Name/Password – Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

Click the **Connect** button to connect immediately.

Click the **Disconnect** button to disconnect immediately.

Dynamic IP/ Static IP – Choose either as you are given by your ISP. When **Static IP** is selected you can enter **IP Address**, **Subnet Mask**, **Gateway** and **DNS** in fields below.

Server IP Address/Name – Enter IP Address or host name of the server provided by your ISP.

IP Address - Enter the IP address in dotted-decimal notation provided by your ISP.

Subnet Mask - Enter the subnet Mask in dotted-decimal notation provided by your ISP.

Gateway - Enter the gateway in dotted-decimal notation provided by your ISP.

DNS - Enter the DNS IP address in dotted-decimal notation provided by your ISP.

Internet IP Address – IP Address used in Internet.

Internet DNS – IP Addresses of DNS Servers used in Internet.

MTU Size (in bytes) - The default MTU size is 1460 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.

Connect on Demand – You can configure the router to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates. **Note:** Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.

Connect Automatically - Connect automatically after the router is disconnected. To use this option, click the radio button.

Connect Manually - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect your Internet connection, and not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link requested. **Note:** Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.

Click the **Save** button to save this settings.

- **PPTP**
Select this **WAN Connection Type**, if your ISP provides PPTP connection.

WAN

WAN Connection Type:

User Name:

Password:

Disconnected!

Dynamic IP Static IP

Server IP Address/Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 0.0.0.0, 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0, 0.0.0.0

MTU Size (in bytes): (The default is 1420, do not change unless necessary.)

Max Idle Time: minutes (0 means remain active at all times.)

Wan Connection Mode: Connect on Demand
 Connect Automatically
 Connect Manually

User Name/Password – Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

Click the **Connect** button to connect immediately.

Click the **Disconnect** button to disconnect immediately.

Dynamic IP/ Static IP – Choose either as you are given by your ISP. When **Static IP** is selected you can enter **IP Address, Subnet Mask, Gateway** and **DNS** in fields below.

Server IP Address/Name – Enter IP Address or host name of the server provided by your ISP.

IP Address - Enter the IP address in dotted-decimal notation provided by your ISP.

Subnet Mask - Enter the subnet Mask in dotted-decimal notation provided by your ISP.

Gateway - Enter the gateway in dotted-decimal notation provided by your ISP.

DNS - Enter the DNS IP address in dotted-decimal notation provided by your ISP.

Internet IP Address – IP Address used in Internet.

Internet DNS – IP Addresses of DNS Servers used in Internet.

MTU Size (in bytes) - The default MTU size is 1420 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.

Connect on Demand – You can configure the router to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If

you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates. **Note:** Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.

Connect Automatically - Connect automatically after the router is disconnected. To use this option, click the radio button.

Connect Manually - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect your Internet connection, and not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link requested. **Note:** Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.

Click the **Save** button to save this settings.

Network / MAC Clone

Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable or DSL modem during installation. Usually, you do not need to change anything here.

MAC Clone

WAN MAC Address:	<input type="text" value="00-19-E0-F8-2E-9F"/>	<input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	<input type="text" value="00-1E-8C-65-2A-D7"/>	<input type="button" value="Clone MAC Address"/>

WAN MAC Address - This field displays the current MAC address of the WAN port, which is used for the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit).

Restore Factory MAC - Click this button and the factory MAC address will fill in the **WAN MAC Address** field.

Your PC's MAC Address - This field displays the MAC address of the PC that is currently managing the router.

Clone MAC Address - If the MAC address in **Your PC's MAC Address** field is desired, you can click this button and this MAC address will fill in the **WAN MAC Address** field.

Click the **Save** button to save this settings.

DHCP / DHCP Settings

The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the router on the LAN. **Note:** To use the DHCP server function of the router, you must configure all computers on the LAN as "Obtain an IP Address automatically" mode. This function will take effect until the router reboots.

DHCP Settings

DHCP Server:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Start IP Address:	<input type="text" value="192.168.1.101"/>
End IP Address:	<input type="text" value="192.168.1.200"/>
Address Lease Time:	<input type="text" value="2880"/> minutes (1~2880 minutes, the default value is 120)
Default Gateway:	<input type="text" value="0.0.0.0"/> (optional)
Default Domain:	<input type="text"/> (optional)
Primary DNS:	<input type="text" value="0.0.0.0"/> (optional)
Secondary DNS:	<input type="text" value="0.0.0.0"/> (optional)

DHCP Server - **Enable** or **Disable** the server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.

Start IP Address - This field specifies the first of the addresses in the IP Address pool. 192.168.1.101 is the default start IP address.

End IP Address - This field specifies the last of the addresses in the IP Address pool. 192.168.1.200 is the default end IP address.

Address Lease Time - The **Address Lease Time** is the amount of time a network user will be allowed connection to the router with their current DHCP Address. Enter the amount of time, in minutes, that the user will be "leased" this DHCP Address. The range of the time is 1~2880 minutes. The default value is 120 minutes.

Default Gateway - (Optional.) Suggest to input the IP Address of the LAN port of the router, default value is 192.168.1.100.

Default Domain - (Optional.) Input the domain name of your network.

Primary DNS - (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.

Secondary DNS - (Optional.) You can input the IP Address of another DNS server if your ISP provides two DNS servers.

Click the **Save** button to save this settings.

DHCP / DHCP Clients List

DHCP Clients List

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	ee10d7	00-03-FF-64-2A-D7	192.168.1.102	44:30:04
2	ee10d8	00-1E-8C-65-2A-D7	192.168.1.101	Permanent

Client Name - The name of the DHCP client.

MAC Address - The MAC address of the DHCP client.

Assigned IP - The IP address that the router has allocated to the DHCP client.

Lease Time - The time of the DHCP client leased.

DHCP / Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

Address Reservation

ID	MAC Address	Reserved IP Address	Status	Modify
1	00-1E-8C-65-2A-D7	192.168.1.101	Enabled	Modify Delete

MAC Address - The MAC Address of the PC.

Reserved IP Address - The IP address assign to MAC Address.

Status - The status of this entry, either **Enabled** or **Disabled**.

Modify – Click **Modify** to open **Add or Modify a Address Reservation Entry** page or **Delete** to delete entry.

Add New... – Click this button to open **Add or Modify a Address Reservation Entry** page.

Enable All – Click this button to make all entries enabled.

Disable All – Click this button to make all entries disabled.

Delete All - Click this button to delete all entries.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Note: Changes made on this page won't take effect until the router reboots.

Add or Modify a Address Reservation Entry

Add or Modify a Address Reservation Entry

MAC Address:	<input type="text"/>
Reserved IP Address:	<input type="text"/>
Status:	<input type="text" value="Enabled"/> ▾

MAC Address - The MAC Address of the PC that you want to reserve IP address for.
Reserved IP Address - The IP address which will be assign to entered MAC Address.
Status - Select **Enabled** or **Disabled** for this entry on the pull-down list.
 Click the **Save** button to save this settings.

Forwarding / Virtual Servers

Virtual servers can be used for setting up public services on your LAN. A virtual server is defined as a service port, and all requests from Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP address because its IP address may change when using the DHCP function.

Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify
1	59355	192.168.1.101	ALL	Enabled	Modify Delete

Service Port - The numbers of External Ports.
IP Address - The IP address of the PC running the service application.
Protocol - The protocol used for this application, either **TCP**, **UDP**, or **All**.
Status - The status of this entry, either **Enabled** or **Disabled**.
Modify - Click **Modify** to open **Add or Modify a Virtual Server Entry** page or **Delete** to delete entry.
Add New... - Click this button to open **Add or Modify a Virtual Server Entry** page.
Enable All - Click this button to make all entries enabled.
Disable All - Click this button to make all entries disabled.
Delete All - Click this button to delete all entries.
 Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Note: If you set the virtual server of service port as *80*, you must set the web management port on the **Security / Remote Management** page to be any value except 80 such as 8080. Otherwise the remote management will be disabled.

Add or Modify a Virtual Server Entry

Add or Modify a Virtual Server Entry

Service Port:	<input type="text"/>	(<input type="checkbox"/> XX-XX or XX)
IP Address:	<input type="text"/>	
Protocol:	<input type="text" value="ALL"/>	
Status:	<input type="text" value="Enabled"/>	
Common Service Port:	<input type="text" value="-Select One-"/>	

Service Port - The numbers of External Ports. You can enter a service port or a range of service ports (the format is XXX - YYY, XXX is Start port, YYY is End port).

IP Address - The IP address of the PC running the service application.

Protocol - The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).

Status - Select **Enabled** or **Disabled** for this entry on the pull-down list.

Common Service Port - Some common services already exist in the pull-down list.

Click the **Save** button to save this settings.

Forwarding / Port Triggering

Some applications require multiple connections, like Internet games, video conferencing, Internet telephoning and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications that can work with a NAT router. Once configured, operation is as follows: A local host makes an outgoing connection to an external host using a destination port number defined in the **Trigger Port** field. The router records this connection, opens the incoming port or ports associated with this entry in the **Port Triggering** table, and associates them with the local host. When necessary the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.

Port Triggering

ID	Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status	Modify
1	6112	ALL	6112	ALL	Enabled	Modify Delete

Trigger Port - The port for outgoing traffic. An outgoing connection using this port will *Trigger* this rule.

Trigger Protocol - The protocol used for **Trigger Ports**, either **TCP**, **UDP**, or **All** (all protocols support by the router).

Incoming Ports - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule.

Incoming Protocol - The protocol used for **Incoming Ports** Range, either **TCP**, **UDP**, or **All** (all protocols support by the router).

Status - The status of this entry, either **Enabled** or **Disabled**.

Modify – Click **Modify** to open **Add or Modify a Port Triggering Entry** page or **Delete** to delete entry.

Add New... – Click this button to open **Add or Modify a Port Triggering Entry** page.

Enable All – Click this button to make all entries enabled.

Disable All – Click this button to make all entries disabled.

Delete All - Click this button to delete all entries.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Add or Modify a Port Triggering Entry

Add or Modify a Port Triggering Entry

Trigger Port:	<input type="text"/>
Trigger Protocol:	ALL ▾
Incoming Ports:	<input type="text"/>
Incoming Protocol:	ALL ▾
Status:	Enabled ▾
Common Applications:	--Select One-- ▾

Trigger Port - Enter a port number used by the application to send an outgoing request.

Trigger Protocol - Select the protocol used for **Trigger Port** from the pull-down list, either TCP, UDP, or All.

Incoming Ports - Enter the range of port numbers used by the remote system when it responds to the PC's request. You can input at most 5 groups of ports (or port section). Every group of ports must be apart with ",". For example, 2000-2038, 2046, 2050-2051, 2085, 3010-3030.

Incoming Protocol - Select the protocol used for **Incoming Ports** range from the pull-down list, either **TCP**, **UDP**, or **All**.

Status - Select **Enabled** or **Disabled** for this entry on the pull-down list.

Common Applications - Some common applications already exist in the pull-down list. Select one to fill all fields with settings for this application.

Click the **Save** button to save this settings.

Note:

- When the trigger connection is released, the according opening ports will be closed.
- Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
- Incoming Ports range cannot overlap each other.

Forwarding / DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded should have a new static IP address assigned to it (in **DHCP / Address Reservation** page) because its IP address may change when using the DHCP function.

DMZ

Current DMZ Status: Enable Disable

DMZ Host IP Address:

Current DMZ Status – Click the respective radio button to **Enable** or **Disable** DMZ.
DMZ Host IP Address - Enter the local host IP address in this field.
 Click the **Save** button to save this settings.

Note: After you set the DMZ host, the firewall related to the IP address will not work.

Forwarding / UPnP

The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

Note: Enabling UPnP may cause router to be vulnerable to *Flash UPnP* attacks.

UPnP

Current UPnP Status: **Disabled**

Current UPnP Settings List

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
<input type="button" value="Refresh"/>						

Current UPnP Status – Click the respective button to **Enable** or **Disable** UPnP. As allowing this may present a risk to security, this feature is disabled by default.

App Description - The description provided by the application in the UPnP request.

External Port - External port, which the router opened for the application.

Protocol - Which type of protocol is opened.

Internal Port - Internal port, which the router opened for local host.

IP Address - The internal host's IP address of the LAN.

Status - Either **Enable** or **Disable**, **Enable** means that port is still active, otherwise, the port is inactive.

Click the **Refresh** button to update the **Current UPnP Settings List**.

Click the **Save** button to save this settings.

Security / Firewall

Using the Firewall page, you can turn the general firewall switch on or off. The default setting for the switch is off. Turning the general firewall switch to off disables IP Filtering, DNS Filtering, MAC Filtering and Advanced Security even if their individual settings are enabled.

Firewall

Enable Firewall (the general firewall switch)

Enable IP Address Filtering

Default IP Address Filtering Rules:

Allow the packets not specified by any filtering rules to pass through the router

Deny the packets not specified by any filtering rules to pass through the router

Enable Domain Filtering

Enable MAC Address Filtering

Default MAC Address Filtering Rules:

Allow these PCs with enabled rules to access the Internet

Deny these PCs with enabled rules to access the Internet

Enable Firewall - The general firewall switch is on or off.

Enable IP Address Filtering - Set IP Address Filtering is enabled or disabled. There are two default filtering rules of IP Address Filtering, either **Allow** or **Deny** not listed packets to pass through the router.

Enable Domain Filtering - Set Domain Filtering is enabled or disabled.

Enable MAC Filtering - Set MAC Address Filtering is enabled or disabled. You can select the default filtering rules of MAC Address Filtering to either **Allow** or **Deny** listed PC's to access Internet.

Security / IP Address Filtering

The **IP Address Filtering** feature allows you to control Internet Access by specific users on your LAN based on their IP addresses. Before adding a domain filtering entry, you must ensure that **Enable Firewall** and **Enable IP Address Filtering** have been selected on the **Firewall** page.

IP Address Filtering

Firewall Settings (You can change it on Firewall page)

Enable Firewall: **Enabled**

Enable IP Address Filtering: **Disabled**

Default Filtering Rules: **Deny the packets not specified by any filtering rules to pass through the router**

ID	Effective time	LAN IP	LAN Port	WAN IP	WAN Port	Protocol	Action	Status	Modify
1	0000-2400	192.168.1.102	-	-	-	ALL	Deny	Enabled	Modify Delete

ID to ID

Firewall Settings – Status of options configured on **Firewall** page.

Effective Time - Range time (HHMM format) for the entry to take effect.

LAN IP Address - LAN IP address or a range of LAN IP addresses.

LAN Port - LAN Port or a range of LAN ports.

WAN IP Address - WAN IP address or a range of WAN IP.

WAN Port - WAN port or a range of WAN ports.

Protocol - Used protocol, either **TCP**, **UDP**, or **All** (all protocols supported by the router).

Action – Selected **Action (Allow or Deny)** through the router) for this entry only.

Status - The status of this entry, either **Enabled** or **Disabled**.

Modify – Click **Modify** to open **Add or Modify a IP Address Filtering Entry** page or **Delete** to delete entry.

Add New... – Click this button to open **Add or Modify a IP Address Filtering Entry** page.

Enable All – Click this button to make all entries enabled.

Disable All – Click this button to make all entries disabled.

Delete All - Click this button to delete all entries.

Move - You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in the second box you want to move to, then click this button to change the entry's order.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Add or Modify a IP Address Filtering Entry

Add or Modify an IP Address Filtering Entry

Effective time:	<input type="text" value="0000"/> - <input type="text" value="2400"/>
LAN IP Address:	<input type="text"/> - <input type="text"/>
LAN Port:	<input type="text"/> - <input type="text"/>
WAN IP Address:	<input type="text"/> - <input type="text"/>
WAN Port:	<input type="text"/> - <input type="text"/>
Protocol:	<input type="text" value="ALL"/> ▾
Action:	<input type="text" value="Deny"/> ▾
Status:	<input type="text" value="Enabled"/> ▾

Effective Time - Enter a range of time in *HHMM* format, which points to the range time for the entry to take effect. For example, 0803 - 1705, the entry will take effect from 08:03 to 17:05.

LAN IP Address - Enter a LAN IP address or a range of LAN IP addresses in the field, in dotted-decimal notation format. For example, 192.168.1.20 - 192.168.1.30. Keep the field open, which means all LAN IP addresses have been put into the field.

LAN Port - Enter a LAN Port or a range of LAN ports in the field. For example, 1030 - 2000. Keep the field open, which means all LAN ports have been put into the field.

WAN IP Address - Enter a WAN IP address or a range of WAN IP addresses in the field, in dotted-decimal notation format. For example, 61.145.238.6 - 61.145.238.47. Keep the field open, which means all WAN IP addresses have been put into the field.

WAN Port - Enter a WAN port or a range of WAN ports in the field. For example, 25 - 110. Keep the field open, which means all WAN ports have been put into the field.

Protocol - Select which protocol is to be used, either TCP, UDP, or All (all protocols supported by the router).

Action - Select either **Allow** or **Deny** through the router.

Status - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.

Click the **Save** button to save this settings.

Security / Domain Filtering

The **Domain Filtering** page allows you to control access to certain websites on the Internet by specifying their domains or key words. Before adding a domain filtering entry, you must ensure that **Enable Firewall** and **Enable Domain Filtering** have been selected on the **Firewall** page.

Domain Filtering

Firewall Settings (You can change it on Firewall page)

Enable Firewall: [Enabled](#)

Enable Domain Filtering: [Disabled](#)

ID	Effective time	Domain Name	Status	Modify
1	0000-2400	www.aabbcc.com	Enabled	Modify Delete

Firewall Settings – Status of options configured on **Firewall** page.

Effective Time - Range time (HHMM format) for the entry to take effect.

Domain Name - Domain or key word.

Status - The status of this entry, either **Enabled** or **Disabled**.

Modify – Click **Modify** to open **Add or Modify a Domain Filtering Entry** page or **Delete** to delete entry.

Add New... – Click this button to open **Add or Modify a Domain Filtering Entry** page.

Enable All – Click this button to make all entries enabled.

Disable All – Click this button to make all entries disabled.

Delete All - Click this button to delete all entries.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Add or Modify a Domain Filtering Entry

Add or Modify a Domain Filtering entry

Effective time: -

Domain Name:

Status:

Effective Time - Enter a range of time in *HHMM* format, which points to the range time for the entry to take effect. For example, 0803 - 1705, the entry will take effect from 08:03 to 17:05.

Domain Name - Enter the domain or key word as desired in the field. For example: *www.xxyy.com.cn*, or *.net*. A blank in the domain field means all websites on the Internet.

Status - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.

Click the **Save** button to save this settings.

Security / MAC Address Filtering

Similar to **IP Address Filtering** page, the **MAC Address Filtering** page allows you to control to access Internet by users on your local network based on their MAC Address. Before adding a domain filtering entry, you must ensure that **Enable Firewall** and **Enable Domain Filtering** have been selected on the **Firewall** page.

MAC Address Filtering

Firewall Settings (You can change it on Firewall page)

Enable Firewall: [Enabled](#)

Enable MAC Address Filtering: [Enabled](#)

Default Filtering Rules: [Deny these PCs with enabled rules to access the Internet](#)

ID	MAC Address	Description	Status	Modify
1	00-03-FF-64-2A-D8	test	Enabled	Modify Delete

Firewall Settings – Status of options configured on **Firewall** page.

MAC Address – Selected MAC Address.

Description – Short description for entry.

Status - The status of this entry, either **Enabled** or **Disabled**.

Modify – Click **Modify** to open **Add or Modify a MAC Address Filtering Entry** page or **Delete** to delete entry.

Add New... – Click this button to open **Add or Modify a MAC Address Filtering Entry** page.

Enable All – Click this button to make all entries enabled.

Disable All – Click this button to make all entries disabled.

Delete All - Click this button to delete all entries.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Add or Modify a MAC Address Filtering Entry

Add or Modify a MAC Address Filtering Entry

MAC Address:	<input type="text"/>
Description:	<input type="text"/>
Status:	<input type="text" value="Enabled"/> ▼

MAC Address - Enter the appropriate MAC address into this field. The format of the MAC address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.

Description - Enter a simple description of the station in this field. For example: John's PC.

Status - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.

Click the **Save** button to save this settings.

Security / Remote Management

This feature allows you to manage your router from a remote location, via the Internet.

Remote Management

Web Management Port:	<input type="text" value="80"/>
Remote Management IP Address:	<input type="text" value="0.0.0.0"/>

Web Management Port - Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For greater security, you can change the remote management web interface to a custom port by entering that number in this box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.

Remote Management IP Address - This is the current address you will use when accessing your router from the Internet. The default IP address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP address to another IP address as desired.

To access the router, you need to enter your router's WAN IP Address into your browser's address bar, followed by a colon and the custom port number. For example, if your router's WAN address is 202.96.12.8 and you use port number 8080, enter `http://202.96.12.8:8080` in your browser. You will be asked for the router's password. After successfully entering the password, you will be able to access the router's web-based utility.

Note: Be sure to change the router's default password to a very secured password.

Security / Advanced Security

Using the Advanced Security page, you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood.

Advanced Security

Packets Statistics Interval (5 - 60): Seconds

DoS Protection: Disable Enable

Enable ICMP-FLOOD Attack Filtering

ICMP-FLOOD Packets Threshold (5 - 3600): Packets/s

Enable UDP-FLOOD Filtering

UDP-FLOOD Packets Threshold (5 - 3600): Packets/s

Enable TCP-SYN-FLOOD Attack Filtering

TCP-SYN-FLOOD Packets Threshold (5 - 3600): Packets/s

Ignore Ping Packet From WAN Port

Forbid Ping Packet From LAN Port

Packets Statistic interval (5-60) - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval is a sampling interval that affects how data is sampled before it is checked for signs of flooding. This value is used to filter against SYN Flood, UDP Flood and ICMP-Flood attacks.

DoS protection - Enable or Disable DoS protection. This option disables all DoS filters when **Disable** is selected.

Enable ICMP-FLOOD Attack Filtering - Enable or Disable the ICMP-FLOOD Attack Filtering.

ICMP-FLOOD Packets threshold (5-3600) - The default value is 50. Enter a value between 5 ~ 3600 packets. When the current ICMP-FLOOD Packets number is beyond the set value the router will startup the blocking function immediately.

Enable UDP-FLOOD Filtering - Enable or Disable the UDP-FLOOD Filtering.

UDP-FLOOD Packets threshold (5-3600) - The default value is 50. Enter a value between 5 ~ 3600 packets. When the current UDP-FLOOD Packets number is beyond the set value the router will startup the blocking function immediately.

Enable TCP-SYN-FLOOD Attack Filtering - Enable or Disable the TCP-SYN-FLOOD Attack Filtering.

TCP-SYN-FLOOD Packets threshold (5-3600) - The default value is 50. Enter a value between 5 ~ 3600 packets. When the current TCP-SYN-FLOOD Packets number is beyond the set value the router will start the blocking function.

Ignore Ping Packet from WAN Port - Enable or Disable ignore ping packet from WAN port. The default is disabled. If this option is enabled the ping packet cannot access the router from the Internet.

Forbid Ping Packet from LAN Port - Enable or Disable forbidding the ping packet from accessing the router through the LAN ports. The default value is disabled. If this option is enabled the ping packet cannot access the router from the LAN. (Defends against some viruses).

Click the **Save** button to save this settings.

Blocked DoS Host List – Click this button to open **Blocked Host List** page, which shows **Host IP Address** and **Host MAC Address** for each host blocked by the router..

Note:

- All of the function in the **Advanced Security** page won't take effect unless the **Firewall** function is enabled.
- The **DoS Protection** won't take effect unless you enable the **Firewall** and **Current Statistics Status** (which is shown in **System Tools / Statistics** page) at the same time.

Static Routing

A static route is a pre-determined path that network information must travel to reach a specific host or network. To add or delete a route, work in the area under the Static Routing page.

Static Routing

ID	Destination IP Address	Subnet Mask	Default Gateway	Status	Modify
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>					
<input type="button" value="Previous"/> <input type="button" value="Next"/>					

Destination IP Address - The Destination IP Address is the address of the network or host which will use this static route.

Subnet Mask - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.

Default Gateway - This is the IP address of the default gateway device that allows for contact between the router and the network or host.

Status - The status of this entry, either **Enabled** or **Disabled**.

Modify – Click **Modify** to open **Add or Modify a Static Route Entry** page or **Delete** to delete entry.

Add New... – Click this button to open **Add or Modify a Static Route Entry** page.

Enable All – Click this button to make all entries enabled.

Disable All – Click this button to make all entries disabled.

Delete All - Click this button to delete all entries.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Add or Modify a Static Route Entry

Destination IP Address - The Destination IP Address is the address of the network or host that you want to assign to a static route.

Subnet Mask - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.

Default Gateway - This is the IP address of the default gateway device that allows for contact between the router and the network or host.

Status - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.

Click the **Save** button to save this settings.

IP & MAC Binding / Binding Settings

To manage the computers well in the LAN, you could control access among computers by ARP Binding.

IP & MAC Binding Setting

ARP Binding: Disable Enable

ID	MAC Address	IP Address	Bind	Modify
1	00-1E-8C-65-2A-D7	192.168.1.101	<input checked="" type="checkbox"/>	Edit Delete

Page

ARP Binding – Select respective radio button to **Enable** or **Disable** ARP Binding function and click the **Save** button.

MAC Address - The MAC address of the controlled computer in the LAN.

IP Address - The assigned IP address of the controlled computer in the LAN.

Bind – Select check-box to enable or deselect to disable the ARP binding.

Modify – Click **Edit** to open **IP & MAC Binding Setting** page or **Delete** to delete entry.

Add New... – Click this button to open **IP & MAC Binding Setting** page. Another way to add hosts to binding list is to use the **Load** or **Load All** button on **ARP list**.

Enable All – Click this button to make all entries enabled.

Find - Click this button to search for entries based on host **MAC Address** or **IP Address**.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page or select page number on the **Page** pull-down list.

IP & MAC Binding Setting

IP & MAC Binding Setting

Bind:

MAC Address:

IP Address:

Bind – Select check-box to enable or deselect to disable the ARP binding.

MAC Address - The MAC address of the controlled computer in the LAN.

IP Address - The assigned IP address of the controlled computer in the LAN.

Click the **Save** button to save this settings.

IP & MAC Binding / ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on the ARP list also.

ARP List

ID	MAC Address	IP Address	Status	Configure
1	00-14-F1-E9-5A-05	87.206.51.1	UnBound	<input type="button" value="Load"/> <input type="button" value="Delete"/>
2	00-1E-8C-65-2A-D7	192.168.1.101	UnBound	<input type="button" value="Load"/> <input type="button" value="Delete"/>

MAC Address - The MAC address of the controlled computer in the LAN.

IP Address - The assigned IP address of the controlled computer in the LAN.

Status - Enabled or Disabled of the MAC address and IP address binding.

Configure – Click the **Load** button to load the item to the **IP & MAC Binding** list or **Delete** to Delete the item.

Bind All - Bind the all current items, available after enabling **ARP Binding** on the **Binding Settings** page.

Load All - Load all item to the **IP & MAC Binding** list.

Note: An item could not be loaded to the **IP & MAC Binding** list if the **IP address** of the item has been loaded before. Error warning will prompt as well. Likewise, **Load All** only loads the items without interference to the **IP & MAC Binding** list.

Dynamic DNS

The router offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org. The Dynamic DNS client service provider will give you a password or key.

DDNS

Service Provider:	Dyndns (www.dyndns.org) <input type="button" value="Go to register.."/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
Domain Name:	<input type="text"/>
	<input type="checkbox"/> Enable DDNS
Connection Status:	DDNS not launching !
	<input type="button" value="Login"/> <input type="button" value="Logout"/>
	<input type="button" value="Save"/>

Service Provider – Select your DDNS Service provider on the pull-down list.

User Name - Enter the User Name for your DDNS account.

Password - Enter the Password for your DDNS account.

Domain Name – Enter the Domain Name that you have gotten from dynamic DNS service provider.

Enable DDNS – Select this check-box to enable DDNS function.

Connection Status - The status of the DDNS service connection is displayed here.

Click the **Login** button to login the DDNS service.

Click the **Logout** button to logout the DDNS service.

Click the **Save** button to save this settings.

System Tools / Time Settings

You can set time manually or get GMT from Internet for the router on this page.

Time Settings

Time zone: (GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels ▼

Date: 5 12 2008 (MM/DD/YY)

Time: 10 44 51 (HH/MM/SS)

Using Daylight Saving Time:

DST begin: 0 0 0 (MM/DD/HH)

DST end: 0 0 0 (MM/DD/HH)

Preferable NTP Server: 0.0.0.0 0.0.0.0

(Get GMT when connected to Internet)

Time Zone - Select your local time zone from this pull-down list.

Date - Enter date in this fields (MM/DD/YY format).

Time - Enter time in this fields (HH/MM/SS format)

Using Daylight Saving Time – Select this option to enable use of Daylight Saving Time.

DST begin - Enter date when Daylight Saving Time begins in this fields (MM/DD/HH format).

DST end - Enter date when Daylight Saving Time ends in this fields (MM/DD/HH format).

Preferable NTP Server – Enter IP Address of the primary and secondary NTP Server.

Get GMT – Click this button to get GMT from Internet if you have connected to Internet. **Note:** Unsaved changes will be lost.

Click the **Save** button to save this settings.

Note:

- This setting will be used for some time-based functions such as firewall, if without time limited, these functions will not take effect, so, make sure to specify your time zone once you login to the router successfully.
- The time will be lost if the router is turned off.
- The router will obtain GMT automatically from Internet when it connects to Internet.
- The DST end will be considered a next year time if it is less than the DST begin.

System Tools / Firmware Upgrade

Firmware

File:	<input type="text"/>	<input type="button" value="Przełóżaj..."/>
Firmware Version:	3.5.1 Build 070321 Rel.50877na	
Hardware Version:	Cerberus P 6371 V1.0.0 081520EF	

File - Enter the file name or click the **Browse...** button to find the firmware file which you want to upload.

Firmware Version - Displays the current firmware version.

Hardware Version - Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

Note: The firmware should correspond to the hardware. Upgrade process will last for a moment and the router will restart automatically then. Keep the power of the router on during the process, in case of any damage.

System Tools / Factory Defaults

Factory Defaults

Click following button to reset all configuration settings to their default values

Restore - Click this button to reset all configuration settings to their default values.

Note: Any settings you have saved will be lost when the default settings are restored.

System Tools / Backup and Restore

Backup & Restore Configuration

Backup:	<input type="button" value="Backup"/>		
File:	<input type="text"/>	<input type="button" value="Przełóżaj..."/>	<input type="button" value="Restore"/>

Backup - Click this button to save all configuration settings to your local computer as a file.

File - click the **Browse...** button to find the configuration file which you want to restore and click the **Restore** button.

Note: The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. The restoring process lasts for 20 seconds and restart automatically then. Keep the power of the router on during the process, in case of any damage.

System Tools / Reboot

Reboot

Click this button to reboot the router.

Reboot - Click this button to reboot the router.

Some settings of the router will take effect only after rebooting, which include:

- Change LAN IP Address. (system will reboot automatically).
- MAC Clone (system will reboot automatically).
- DHCP service function.
- Static address assignment of DHCP server.
- Change Web Service Port of the router.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router's settings to the factory defaults (system will reboot automatically).

System Tools / Password

It is strongly recommended that you change the factory default user name and password of the router. All users who try to access the router's web-based utility will be prompted for the router's user name and password.

Password

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

Old User Name – Type old User Name in this field.

Old Password – Type old Password in this field.

New User Name – Type new User Name in this field.

New Password – Type new Password in this field.

Confirm New Password – Retype new Password in this field.

Click the **Save** button to save this settings.

Click the **Clear All** button to clear all fields.

Note: The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

System Tools / Log

The router can keep logs of all traffic. You can query the logs to find out what happened to the router.

Log

Index	Log
1	320112:System: Logs were cleared.
2	321316:DHCP: 1:0x0003ff642ad7, 192.168.1.102, ACK in request.
3	321475:DHCP: 1:0x0003ff642ad7, 192.168.1.102, ACK in request.

Time = 2008-05-12 10:49:18 337442s
H-Ver = Cerberus P 6371 V1.0.0 081520EF : S-Ver = 3.5.1 Build 070321 Rel.50877na
L = 192.168.1.100 : M = 255.255.255.0
W1 = DHCP : W = 87.206.51.127 : M = 255.255.255.0 : G = 87.206.51.1
Free=3087, Busy=11, Bind=8, In=0/2, Bc=0/0, Dns=0, cl=96, fc=0/0, sq=0/0

Click the **Refresh** button to refresh the logs.
Click the **Clear All** button to clear all logs.

System Tools / Statistics

The Statistics page shows the network traffic of each PC on LAN, including total traffic and traffic of the last **Packets Statistic interval** seconds.

Statistics

Current Statistics Status: **Enabled**

Packets Statistics Interval(5-60): Seconds
 Auto-refresh

Sorted Rules:

IP Address/ MAC Address	Total		Current					Modify
	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	SYN Tx	
192.168.1.101 00-1E-8C-65-2A-D7	25137347	178375013	1	167	0/13	0/25	0/45	Reset Delete
192.168.1.102 00-03-FF-64-2A-D7	76	29223	0	0	0/0	0/0	0/0	Reset Delete

Current Statistic Status - Enable or Disable. The default value is disabled. To enable, click the Enable button. If disabled, the function of **DoS protection** in **Security / Advanced Security** will be disabled.

Packets Statistic Interval - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.

Auto-refresh – Select this checkbox to refresh automatically.

Refresh - Click this button to refresh immediately.

Sorted Rules - Here displays sort as desired. Click the **Reset All** button to reset, or **Delete All** button to delete all statistics.

IP Address/MAC Address – The IP and MAC Addresses displayed with statistics.

Total: Packets – The total amount of packets received and transmitted by the router.

Total: Bytes – The total amount of bytes received and transmitted by the router.

Current: Packets – The total amount of packets received and transmitted in the last Packets Statistics interval seconds.

Current: Bytes – The total amount of bytes received and transmitted in the last Packets Statistics interval seconds.

Current: ICMP Tx – The total amount of the ICMP packets transmitted to WAN in the last Packets Statistics interval seconds.

Current: UDP Tx – The total amount of the UDP packets transmitted to WAN in the last Packets Statistics interval seconds.

Current: TCP SYN Tx – The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistics interval seconds.

Modify – Click on **Reset** to reset, or **Delete** to delete statistics for this entry.



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.

PWR 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.

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.

WAN LED

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

1. Check the Ethernet cable connections between your router and ISP's access device;
2. Check that the ISP's access device is turned on and receiving sufficient power;

Problems with resolving IP Address from the router's DHCP Server in Windows Vista

In some cases Windows Vista cannot obtain an IP address from certain router's DHCP server. If you encounter this, follow this steps to resolve this problem (Microsoft Support page)

<http://support.microsoft.com/kb/928233/en-us>

Problems with the Web Interface

I cannot access the web Interface:

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

Problems with the Login Username and Password

I forgot my login username and/or password:

1. The default username is "**admin**". The default password is "**pentagram**". The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing;
2. If you ever forget the password to log in, you may need to restore the factory default settings. Use the **RESET** button: First, turn off the router's power. Second, press and hold the default reset button then turn on the router's power, until the SYS LED lights up (about 3 seconds). Last, release the reset button and wait for the router to reboot.

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 the Internet Access

I cannot access the Internet:

1. Make sure the router is turned on and connected to the network;
2. If the WAN LED is off, refer to Section **WAN 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 PPPoE, check the idle time-out setting;
2. Contact your ISP.



