

Installation and Operation Manual

EN

PENTAGRAM Cerberus [P 6367]

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

v.2.101102.1502

Important information

Safety precautions

- Do not use or store the device in dusty places, where the humidity is high or in extreme temperatures.
- Do not operate the device with wet hands to avoid the risk of device damage or electric shock.
- Do not clean the device with chemicals, such as benzine or detergents – always clean the device with a soft, dry cloth.
- Disconnect the device from the computer prior to cleaning.
- Do not modify or fix the device yourself in any way, it might void the guarantee.
- Do not drop or shake the device.
- Avoid using this product and all accessories outdoors.
- Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.

Information concerning waste electronic equipment

The markings on the device and in the attached documentation indicate that it cannot be disposed of along with unsegregated general black bag waste when withdrawn from use. The device must be recycled or processed in another way to recover reusable materials and neutralize hazardous components.

The users should contact recycling/recovery authorities to determine how the device is to be disposed of in an environment-friendly manner.



NOTE: *All information and technical data is subject to change without previous notice and/or indication in this manual.*

Copyright ©2010 PENTAGRAM

All rights reserved; copying and reproduction is strictly forbidden.

INDEX

IMPORTANT INFORMATION.....	2
SAFETY PRECAUTIONS.....	2
INFORMATION CONCERNING WASTE ELECTRONIC EQUIPMENT.....	2
INTRODUCTION.....	5
PACKAGE CONTENTS.....	5
ROUTER WORK MODES.....	6
3G ROUTER MODE.....	6
WIRELESS AP MODE.....	6
WISP MODE.....	7
WIRELESS MODE.....	7
OPERATING THE DEVICE.....	8
FRONT PANEL.....	8
REAR PANEL.....	9
SIDE BUTTONS.....	9
ROUTER'S POWER SUPPLY.....	9
CONNECTING COMPUTERS TO THE CERBERUS.....	10
Wired connections (LAN interface).....	10
Wireless connections (WLAN interface).....	10
Configuring network properties.....	10
Windows Vista/7.....	11
Windows 2000/XP.....	12
Windows 95/98/Me.....	13
CONFIGURING THE ROUTER - FOREWORD.....	14
DEFAULT SETTINGS.....	14
RESTORING DEFAULT SETTINGS.....	14
CONFIGURATION USING THE CONFIGURATION PAGE.....	15
LOGGING ON.....	15
NAVIGATION.....	15
SETUP WIZARD.....	16
WISP Settings [WISP Mode].....	16
Connection Method [WISP or Wireless Router Mode].....	17
Connection Method [3G Router Mode].....	17
Wireless Basic Settings.....	18
Wireless Security Settings.....	18
Finishing the wizard.....	19
ADVANCED SETTINGS [3G ROUTER, WISP OR WIRELESS ROUTER MODE]..	19
LAN Settings [3G Router, WISP or Wireless Router Mode].....	19
WAN Settings [3G Router Mode].....	20
WAN Settings [WISP or Wireless Router Mode].....	21
Dynamic IP.....	21
Static IP.....	21
ADSL Virtual Dial-up (via PPPoE).....	22
L2TP.....	22
PPTP.....	23
MAC Address Clone [Wireless Router Mode].....	23

DNS Settings.....	24
LAN Settings [Wireless AP Mode].....	24
WLAN SETTINGS.....	25
Basic Settings.....	25
Security Settings.....	27
WPA-Personal.....	27
WPA2-Personal.....	28
Mixed WEP.....	29
Advanced Settings.....	30
WPS Settings.....	31
WDS Settings.....	32
Access Control.....	32
Connection Status.....	33
DHCP SERVER [3G ROUTER, WISP OR WIRELESS ROUTER MODE].....	33
DHCP Server.....	33
DHCP List and Binding.....	34
VIRTUAL SERVER [3G ROUTER, WISP OR WIRELESS ROUTER MODE].....	35
Port Range Forwarding.....	35
DMZ Settings.....	36
UPNP Settings.....	36
TRAFFIC CONTROL.....	37
Traffic Control.....	37
Traffic Statistics.....	38
3G WAN TRAFFIC [3G ROUTER MODE].....	38
3G WAN Traffic.....	38
SECURITY SETTINGS [3G ROUTER, WISP OR WIRELESS ROUTER MODE]....	39
Client Filter.....	39
URL Filter.....	40
MAC Filter.....	41
Prevent Network Attack.....	41
Remote WEB Management.....	42
WAN Ping.....	42
ROUTING SETTINGS.....	43
SYSTEM TOOLS.....	43
Time Settings.....	43
DDNS [3G Router, WISP or Wireless Router Mode].....	44
Backup/Restore Settings.....	44
Restore to Factory Default Settings.....	45
Firmware Upgrade.....	45
Reboot the Router.....	45
Change Password.....	46
System Log.....	46
LOGOUT.....	46
COMPATIBLE 3G MODEMS.....	47

Introduction

PENTAGRAM Cerberus [P 6367] wireless router is a universal network device, capable of performing different roles basing on currently selected work mode. PENTAGRAM Cerberus [P 6367] is an excellent foundation for a wireless network at home or a small business. With the Cerberus, your Internet connection sharing, file transfer and gaming experience can be even better and safer than before.

PENTAGRAM Cerberus [P 6367] can support a 802.11n (Draft 2) wireless network with a maximum data rate of 150 Mbps. With a rich feature set, it can also interoperate with 802.11b products (up to 11 Mbps) and 802.11g products (up to 54 Mbps) in home or office environments, and with public hotspots. Additionally, your wireless network can be secured using WEP, WPA (TKIP) or WPA2 (AES) protocol.

Router doesn't have built-in any kind of modem, so it must work with cable/xDSL/3G modem ISP provided for its Internet service.

NOTE:

- *ISP's cable/xDSL modem must allow connection with local network via network cable (twisted-pair). Modems with only USB port are not supported.*
- *Router supports only 3G modems with USB interface. Other modems are not supported.*
- *Compatible 3G modem list can be found near the end of this manual. We cannot guarantee compatibility with modems not on this list. Support for additional modems can be added in newer revisions of the Firmware.*

Package contents

1. PENTAGRAM Cerberus [P 6367]
2. 5V \mp 1.2A power adapter
3. USB cable - straight
4. USB cable - "Y" type
5. Network cable (twisted pair)
6. CD
7. Quick Installation Guide
8. Protective case

If any of the package contents are missing, please contact your vendor.

Router work modes

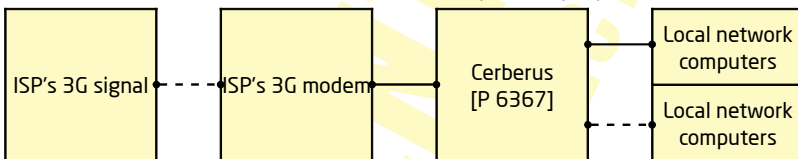
Router can work in one of the four modes. Router's work mode should be selected basing on the used Internet connection, access device (modem) supplied by ISP and role the router will perform in the local network. Below, you can find description of all four modes, which should make choice much easier. To change currently used mode, use **MODE** button located at the side of the device.

LEGEND:

- • — wired connection
- - - - • - wireless connection

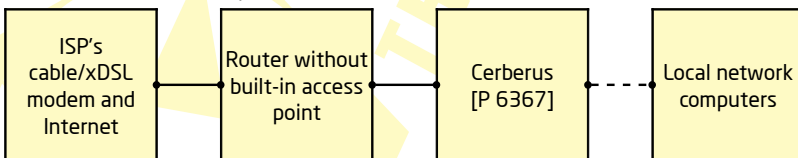
3G Router Mode

This is default work mode of the router, in which router acts as the Internet gateway. Connection with Internet is accomplished with use of the 3G modem connected to router's USB port. Local network computers connects to router via wireless Wi-Fi network. Additionally, one computer can be connected to router via network cable (twisted-pair).



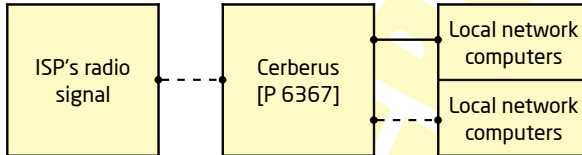
Wireless AP Mode

In this mode router acts as the wireless network access point (AP) and is connected via network cable (twisted-pair) to a router performing role of the Internet gateway. Connection with Internet network is accomplished with use of the ISP's modem, to which router-gateway is connected. Local network computers connects to router via wireless Wi-Fi network.



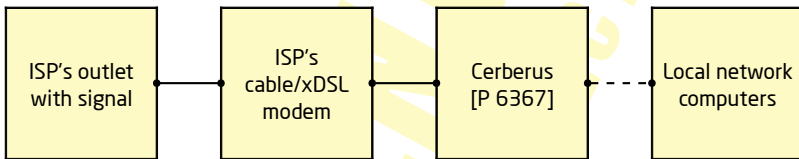
WISP Mode

In this mode router acts as the wireless network access point (AP), which amplifies and relays to the wireless stations wireless signal received from ISP. Connection with the Internet is accomplished via ISP's wireless (Wi-Fi) network. Local network computers connects to router via wireless Wi-Fi network. Additionally, one computer can be connected to router with network cable (twisted-pair).



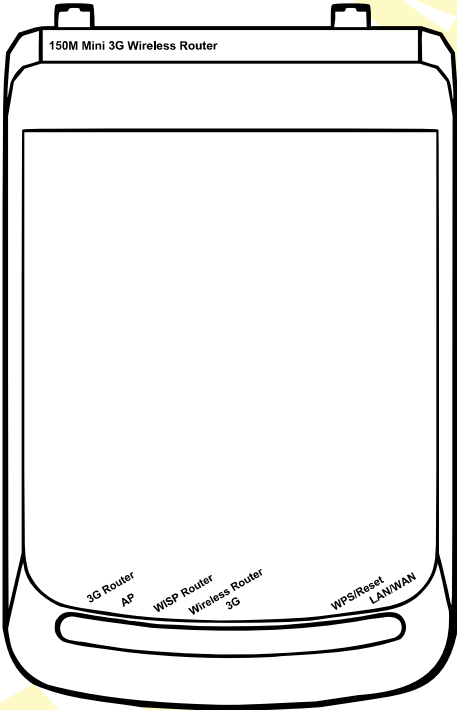
Wireless Mode

In this mode router acts as the Internet gateway. Connection with Internet is accomplished with use of the ISP's cable/xDSL modem connected to router via network cable (twisted-pair). Local network computers connects to router via wireless Wi-Fi network.



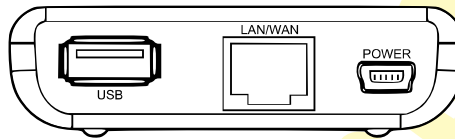
Operating the device

Front panel



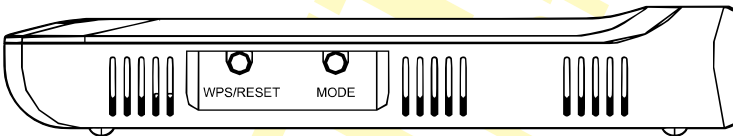
LED	Action	Description
3G Router	Lit up	Router is working in 3G Router mode
AP	Lit up	Router is working in Wireless AP mode
WISP Router	Lit up	Router is working in WISP Router mode
Wireless Router	Lit up	Router is working in Wireless Router mode
3G	Not lit	Not connected or not supported 3G modem
	Lit up	3G modem connected to the USB port
	Flashing	Data transfer between router and 3G modem
WPS/Reset	Flashing	Device is negotiating with client in WPS PBC mode
LAN/WAN	Not lit	No device connected to the LAN/WAN port
	Lit up	Network device connected to the LAN/WAN port
	Flashing	Network activity of the corresponding port

Rear Panel



Label	Application
USB	Connecting 3G modem NOTE: Connecting power to this socket will cause router damage, which is not covered by warranty.
LAN/WAN (8P8C)	Connecting via network cable (twisted-pair) to: <ul style="list-style-type: none"> • local network computer (3G Router or WISP Router mode), or • ISP's cable/xDSL modem (Wireless Router mode), or • router-gateway (Wireless AP mode)
POWER	Connecting power cable; see Router's power supply section below

Side buttons



WPS/RESET - Press and hold this button for approx. 10 seconds to restore the device to its factory settings. Press and hold this button for about one second to enter WPS PBC mode. More detailed information regarding WPS configuration can be found in router's **Installation and Operation Manual**.

MODE - Press this button to change router's work mode.

Router's power supply

There are two ways to connect powers supply to the router:

- Power grid**
 - connect supplied power adapter to power outlet,
 - connect large plug of supplied straight USB cable to power adapter's USB socket,
 - connect small plug of the USB cable to router's **POWER** socket.
- Computer's USB Port**
 - connect both large plugs of supplied "Y" USB cable to computer's USB ports,
 - connect small plug of the USB cable to router's **POWER** socket.

Connecting computers to the Cerberus

Computers and other network devices can be connected to the Cerberus in two ways as described below.

Wired connections (LAN interface)

NOTE: Router's LAN/WAN port can be used for LAN connections only in **3G Router** or **WISP Router** modes.

LAN/WAN port of the router support Auto MDI/MDIX functionality, which enables and disables crossover automatically, as required. With the autonegotiation feature, the router also automatically selects the highest connection speed available. For 10/100 Mbps transfers, a Cat. 5 twisted-pair cable is required, terminated with 8P8C connectors (often, but incorrectly called RJ-45) according to TIA/EIA-568-A or TIA/EIA-568-B standard. One end of the cable should be connected to a computer's network adapter, and the other to the router's LAN/WAN port. If the connection is correct, the LED indicator corresponding to the LAN/WAN port will light up.

Wireless connections (WLAN interface)

In order to connect a computer to the Cerberus using a wireless network, the WLAN adapter must be installed correctly in the system, and the router must be located within the operating range of the wireless adapter and belong to the same subnet. Detailed instructions regarding connecting to wireless networks should be included in wireless adapter operation manual.

Configuring network properties

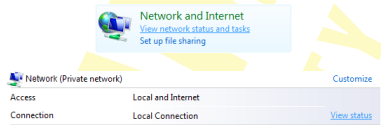
Before a connection (wired or wireless) can be established between your computer and the router, TCP/IP must be configured in the operating system (this protocol should be installed automatically by the system when installing network adapter drivers). It is recommended to configure TCP/IP so that the IP address and other connection settings are obtained from the router's DHCP server. This configuration is described below for various Windows systems.

NOTE:

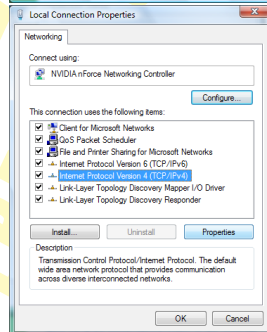
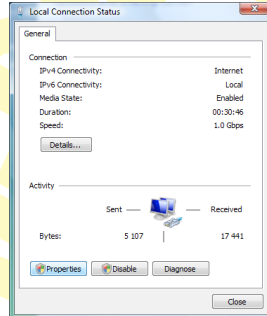
- In some cases, a computer running Windows 7, Windows Vista or Windows XP Service Pack 3 may not obtain an IP address from the router's DHCP server. To solve this issue, please follow the instructions provided on the Microsoft technical support website at <http://support.microsoft.com/kb/928233/en-us>.
- You need administrative privileges to perform network configuration. During configuration, it may be necessary to click **Allow** (Windows Vista) or **Yes** (Windows 7) in the **User Account Control** dialog, and provide an administrative user name and password if the current user does not have administrative privileges.

Windows Vista/7

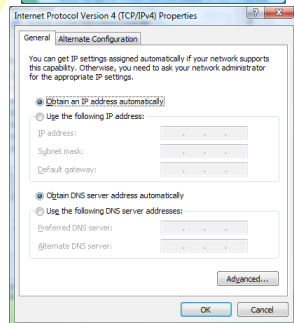
1. Click **Start > Control Panel**.
2. Click **View network status and tasks**.
3. Click **View status** (Vista) or click the connection type (7) for your connection.
4. On the **General** tab, click **Properties**.



5. On the **Networking** tab, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

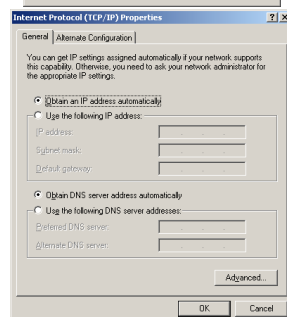
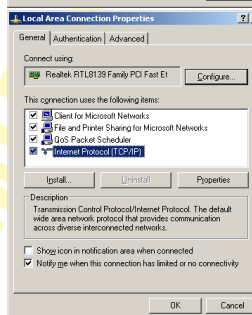
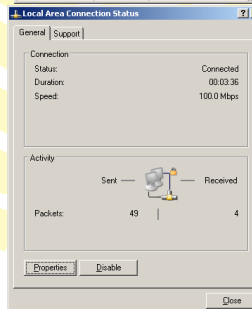


6. On the **General** tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
7. Click **OK** to save the settings and close the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog.



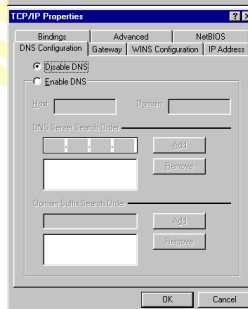
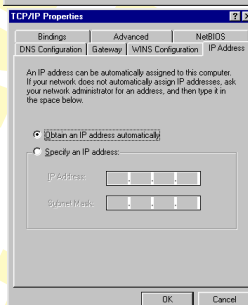
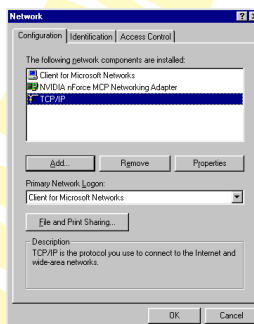
Windows 2000/XP

1. Click **Start > Settings > Control Panel**.
2. Double-click the **Network Connections** icon (2000/XP classic view) or **Network and Internet Connections** and then **Network Connections** (XP default view).
3. Double-click **Local Area Connection**.
4. On the **General** tab, click **Properties**.
5. On the **General** tab, select **Internet Protocol (TCP/IP)** and click **Properties**.
6. On the **General** tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
7. Click **OK** to save the settings and close the **Internet Protocol (TCP/IP) Properties** dialog.



Windows 95/98/Me

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



To verify whether your adapter has a valid IP address:

1. Use **+R** hotkey or click **Start > Run** (Windows 98/ME/ 2000/XP) or **Start > All programs > Accessories > Run** (Windows Vista/7) to display the **Run** dialog.
2. Type **cmd** (Win 2000/XP/Vista/7) or **command** (Win 98/ME) and press Enter.
3. Type **ipconfig /all** (Windows 2000/XP/Vista/7) or **winipcfg** (Windows 98/ME) in the command line and press Enter.
4. Check whether the IP Address entry for the appropriate network adapter matches the address pool of the router's DHCP server, e.g. **192.168.1.101**.

Configuring the router - foreword

Router's configuration settings are available on it's configuration page, which can be accessed using any Web browser.

NOTE: *It is advised to carry out the initial router configuration from a computer connected to the router via Ethernet cable.*

Default settings

Before configuring the router, we recommend reviewing the default settings for key router parameters shown below.

IP address	192.168.1.100
Subnet mask	255.255.255.0
SSID	PENTAGRAM_P6367
DHCP server	Enabled
DHCP server address pool	100 IP addresses from 192.168.1.101 to 192.168.1.200
IP address lease time	86400 seconds (24 hours)
User name	admin
Password	pentagram

NOTE:

- *We recommend that you change the access password for the router's configuration page as soon as possible.*
- *If you ever forget the access password for the router, please reset the device to its default settings.*
- *To avoid possible conflicts with other Wi-Fi networks, its recommended to change router's network SSID to something more unique.*

Restoring default settings

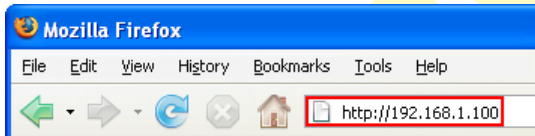
The router can be restored to its default settings in two ways:

- by clicking the **Restore** button on the **System Tools > Restore to Factory** tab on the router's configuration page; or
- by pressing and holding the **RESET/WPS** button on the back of the device for approx. 10 seconds.

Configuration using the configuration page

Logging on

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



3. If the system password is set, enter your username and password (default: **admin** / **pentagram**).

Navigation

After successful logging in, the router's configuration page will be displayed. It's divided into four sections - mode selection **1**, selected mode navigation menu **2**, selected tab content **3** and help to currently selected tab **4**.

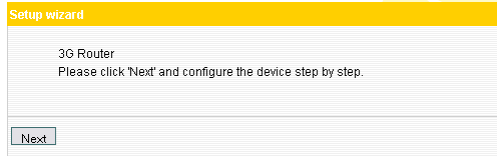


Mode name in square brackets in section title means that the page described is available only for this mode. No square brackets means that the page is available in every mode.

Default page for every mode is **Setup Wizard** which is useful for quick configuration of most important router's settings.

Setup Wizard

Make sure that mode you want to configure is selected at the top bar of configuration page and then click **Setup Wizard** item in the navigation menu on the left side of the page. When Setup wizard welcoming screen appears, click **Next** to begin the Wizard configuration.



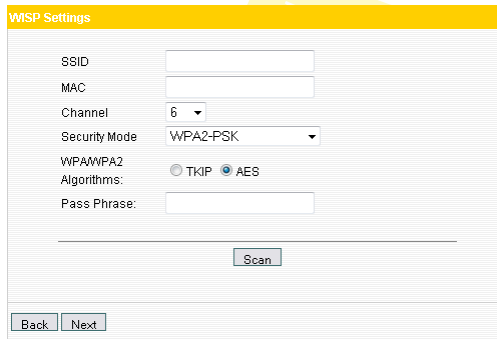
Setup wizard

3G Router
Please click 'Next' and configure the device step by step.

Next

WISP Settings [WISP Mode]

Click **Scan** to scan the wireless signals in WISP settings interface, and select the channel you want to use.



WISP Settings

SSID:

MAC:

Channel: 6

Security Mode: WPA2-PSK

WPAWPA2 Algorithms: ☐ TKIP ☒ AES

Pass Phrase:

Scan

Back Next

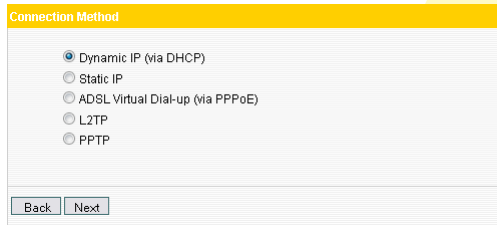
SSID: SSID (Service Set Identifier) is the unique name of the wireless network. Enter the SSID of the WISP AP that needs to be connected to this device.

MAC Address: Input the wireless MAC address of the wireless AP that needs to be connected to this device. Sometimes, MAC address is also named BSSID.

Channel: Specify the effective channel (from 1 to 13\Auto) of the wireless network. The channel you select must be the same with that of the AP provided by your ISP.

Security Mode: The security mode and pass phrase you set should be the same as that of the AP. More details please refer to [Security Settings](#) chapter on page 27.

Connection Method [WISP or Wireless Router Mode]



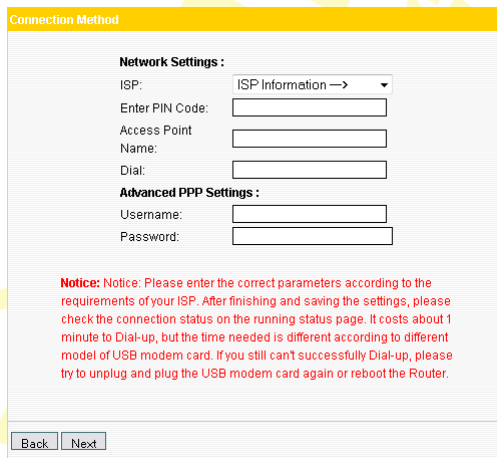
Connection Method

☒ Dynamic IP (via DHCP)
☐ Static IP
☐ ADSL Virtual Dial-up (via PPPoE)
☐ L2TP
☐ PPTP

Back Next

In WISP or Wireless Router mode, there are five access modes: **Dynamic IP (via DHCP)**, **Static IP**, **ADSL Virtual Dial-up (via PPPoE)**, **L2TP** and **PPTP**. The default mode is **Dynamic IP**. If your ISP provides you the Dynamic IP access mode, please select **Dynamic IP** and click **Next**. If you are provided the static IP access mode, please select **Static IP** and fill in the parameters provided by your ISP or network administrator and then click **Next**. If you are provided the PPPoE access mode, please input the user name and password provided by your ISP and click **Next**. In **L2TP** and **PPTP** modes, you need to input the IP address, user name, and password.

Connection Method [3G Router Mode]



Connection Method

Network Settings :

ISP: ISP Information →

Enter PIN Code:

Access Point Name:

Dial:

Advanced PPP Settings :

Username:

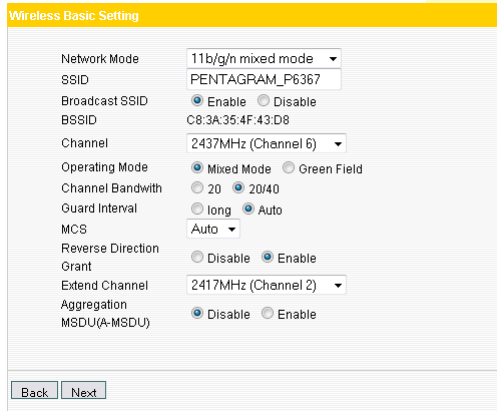
Password:

Notice: Notice: Please enter the correct parameters according to the requirements of your ISP. After finishing and saving the settings, please check the connection status on the running status page. It costs about 1 minute to Dial-up, but the time needed is different according to different model of USB modem card. If you still can't successfully Dial-up, please try to unplug and plug the USB modem card again or reboot the Router.

Back Next

Select the Internet Service Provider (ISP) of your 3G modem card from the **ISP** list. If you don't find the 3G modem card you are using from the list, please select **OTHER** and input the correct parameters, if you are not sure about them, please inquire the technicians of your ISP. For parameters not provided by your ISP, just leave the corresponding fields blank.

Wireless Basic Settings



Wireless Basic Setting

Network Mode	11b/g/n mixed mode
SSID	PENTAGRAM_P6367
Broadcast SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
BSSID	C8:3A:35:4F:43:D8
Channel	2437MHz (Channel 6)
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel Bandwidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> Auto
MCS	Auto
Reverse Direction Grant	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extend Channel Aggregation	2417MHz (Channel 2)
MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Back Next

Network Mode: Select one mode according to the using environment, and you are recommended to use the **11b/g/n mixed mode**.

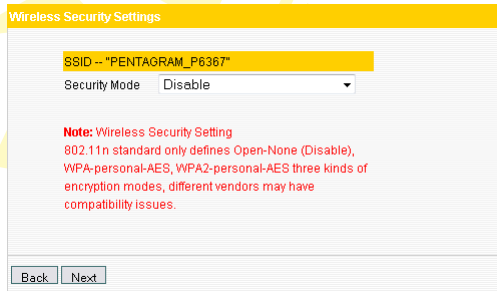
SSID: SSID (Service Set Identifier) is the unique name of the wireless network. You can change it to other names.

Broadcast SSID: Select **Enable** to enable the device's SSID to be visible by your wireless devices. The default is enabled.

Channel: The wireless frequency used by wireless network. You are not recommended to use the same channel that used by other SSIDs for using the same or neighboring channels would cause mutual interference and reduce the router's transmission rate.

Please refer to **Basic Settings** chapter on page **25** for other settings.

Wireless Security Settings



Wireless Security Settings

SSID -- "PENTAGRAM_P6367"

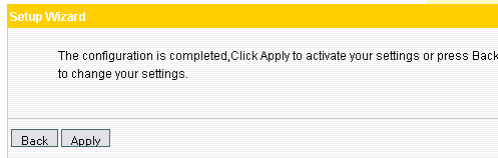
Security Mode

Note: Wireless Security Setting
802.11n standard only defines Open-None (Disable),
WPA-personal-AES, WPA2-personal-AES three kinds of
encryption modes, different vendors may have
compatibility issues.

Back Next

It is suggested that you choose **WPA2-Personal** for **Security Mode** and **AES** for **WPA Algorithms**, you only need to input 8~63-bit **Pass Phrase** combined with numbers, letters and characters. Click **Next** to save the configuration. More details please refer to the following section.

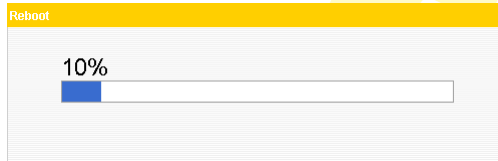
Finishing the wizard



Setup Wizard

The configuration is completed, Click Apply to activate your settings or press Back to change your settings.

Click **Apply** to save the settings.



Reboot

10%

A progress bar showing 10% completion of the reboot process.

The Router is rebooting to bring the configuration into effect, please **DO NOT** power off it.

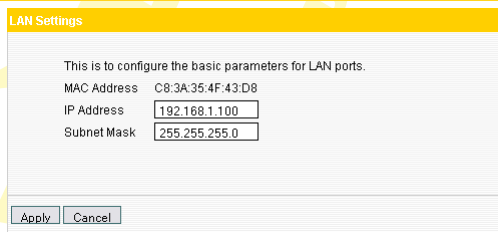
Advanced Settings [3G Router, WISP or Wireless Router Mode]

LAN Settings [3G Router, WISP or Wireless Router Mode]

This section mainly describes how to configure the TCP/IP parameters of local network.

In **3G Router** mode, **WISP** mode, **Wireless Router** mode, please configure the LAN port parameters as the diagram below.

NOTE: In **Wireless Router** mode, you can only configure the device by using the wireless access way.



LAN Settings

This is to configure the basic parameters for LAN ports.

MAC Address C8:3A:35:4F:43:D8

IP Address

Subnet Mask

MAC Address: It displays the router's LAN MAC address, which can not be changed.

IP Address: The Router's LAN IP address (not your PC's IP address). The default value is 192.168.1.100 .

Subnet Mask: The Router's LAN subnet mask. The default value is 255.255.255.0 .

NOTE: If you change the IP, you need to use the new one to log in to the Web interface.

WAN Settings [3G Router Mode]

WAN Settings

Network Settings :

ISP:

Enter PIN Code:

Access Point Name:

Dial:

Advanced PPP Settings :

Username:

Password:

Internet Connection Option:

☒ Connect Automatically

☐ Connect Manually

☐ Connect on Demand

Max Idle Time: (60-3600 seconds)

☐ Connect on Fixed Time

IMPORTANT: Please set the time in system Tools, before you select this Internet connection.

Time From to

Time format, Hours:0~23; Minute:0~59

Select the corresponding ISP to identify the 3G modem card and auto-match the 3G network parameters, which makes it convenient for 3G network users. If you don't find your ISP name in the list, please select **OTHER** and input the parameters provided by your ISP.

Click **System Status** to view the connection status between current 3G WAN port and your ISP. When it shows **Connected**, you can share the 3G network service.

Internet Connection Modes:

There are four Connection modes, please select one according to your needs:

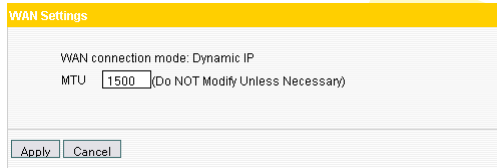
- **Connect Automatically:** Connect automatically to the Internet after rebooting the system or connection failure.
- **Connect Manually:** When the network is disconnected, users can connect it manually.
- **Connect on Demand:** Dial up automatically when there's data transmission.
- **Connect on Fixed Time:** Connect to the Internet during the time you specified automatically.

NOTE: We recommend that you use the **Connect on demand** mode, in this mode the router will disconnect the 3G modem card connection when the computer is turned off or there's no traffic being transferred, so even you forget to turn off the router, it won't waste the money in the UIM. For your convenience, the router will dial up automatically when the computer needs to have access to the Internet. When there's no traffic, you need to log out all programs that can be connected to the external network, such as, thunder, BT and so on.

WAN Settings [WISP or Wireless Router Mode]

Depending on your access ways, there are five ways of WAN configuration.

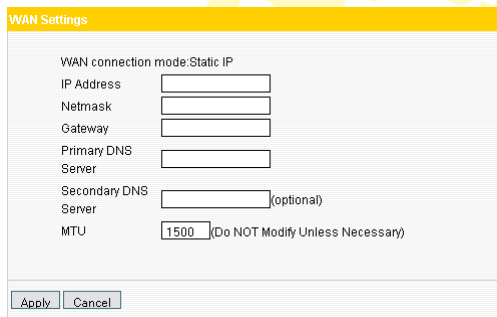
Dynamic IP



The screenshot shows the 'WAN Settings' window with the title bar in yellow. The main area has a light gray background. It displays 'WAN connection mode: Dynamic IP' and 'MTU 1500 (Do NOT Modify Unless Necessary)'. At the bottom, there are 'Apply' and 'Cancel' buttons.

MTU: Maximum Transmission Unit. The default value is **1492**. DO NOT modify it unless necessary. But if some specific websites or web application software can not be open or enabled, you can have a try to change the MTU value as 1450, 1400, etc.

Static IP



The screenshot shows the 'WAN Settings' window with the title bar in yellow. The main area has a light gray background. It displays 'WAN connection mode: Static IP'. Below this, there are input fields for 'IP Address', 'Netmask', 'Gateway', 'Primary DNS Server', 'Secondary DNS Server (optional)', and 'MTU 1500 (Do NOT Modify Unless Necessary)'. At the bottom, there are 'Apply' and 'Cancel' buttons.

If your connection mode is static IP, you can modify the parameters as shown in the above diagram

IP Address: Enter the WAN IP address provided by your ISP. If you are not clear, please inquire your ISP.

Subnet Mask: Enter the WAN Subnet Mask. The default value is **255.255.255.0**.

Gateway: Enter the WAN Gateway provided by your ISP.

Primary DNS Address: Enter the necessary address provided by your ISP.

Secondary DNS Address: Enter the second address if your ISP provides, and it is optional.

ADSL Virtual Dial-up (via PPPoE)

WAN Settings

WAN connection mode: PPPoE

Account:

Password:

MTU:

Service Name: (Do NOT Modify Unless Necessary)

AC Name: (Do NOT Modify Unless Necessary)

Internet Connection Option:

☒ Connect Automatically

☐ Connect Manually

☐ Connect on Demand

Max Idle Time: (60-3600 seconds)

☐ Connect on Fixed Time

IMPORTANT: Please set the time in system Tools, before you select this Internet connection.

Time: From to

Time format, Hours: 0~23; Minute: 0~59

Connection Method: It shows the current connection method.

User name: Enter the user name provided by your ISP

Password: Enter the password provided by your ISP.

L2TP

WAN Settings

WAN connection mode: L2TP

L2TP Server: (IP or Domain name)

User Name:

Password:

MTU:

Address Mode:

IP Address:

Subnet Mask:

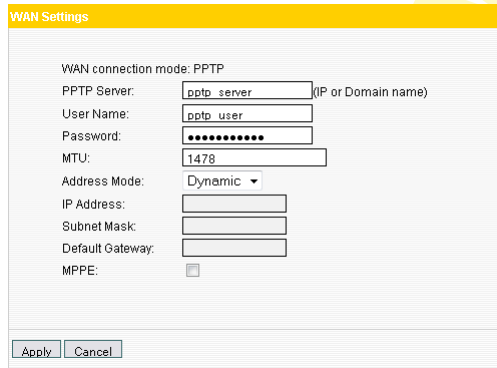
Default Gateway:

L2TP server: The IP address or domain name of the destination server and it is used to specify the destination address which needs for L2TP connection.

User name/Password: Used to validate identity when connecting to the L2TP server.

Address Mode: Set the router's IP address mode, you can select either **Dynamic** or **Static**. If your ISP doesn't provide the IP address, please select **Dynamic**.

All the above parameters are provided by ISP.

PPTP


WAN Settings

WAN connection mode: PPTP

PPTP Server: (IP or Domain name)

User Name:

Password:

MTU:

Address Mode:

IP Address:

Subnet Mask:

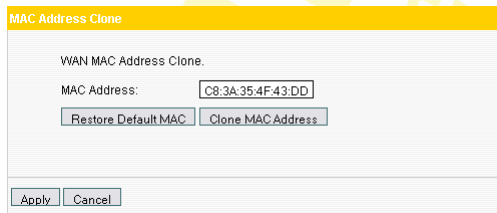
Default Gateway:

MPPE: ☐

For PPTP connection configuration, please refer to the **L2TP** connection method above.

MAC Address Clone [Wireless Router Mode]

This page is for the Router's WAN MAC address configuration.



MAC Address Clone

WAN MAC Address Clone.

MAC Address:

Some ISPs require user's MAC address to access their network. This feature copies the MAC address of your network device to the Router.

MAC Address: It displays the router's WAN MAC address, which can be entered manually.

Clone MAC Address: Copy the computer's MAC address to the router's WAN port as the router's WAN MAC address.

Restore Default MAC Address: Restore the router's WAN port MAC address to the default.

DNS Settings

DNS is short for Domain Name System (or Service). The server that implements domain name service is called DNS server, which is used to respond to the domain name service inquiry.

DNS settings: Tick to enable the DNS server. The router's DNS address connected via WAN will adopt the manually added DNS address. Router's DHCP server will answer the client's requests and distribute DNS address.

Primary DNS Address: Enter the necessary address provided by your ISP.

Secondary DNS Address: Enter the second address if your ISP provides, and it is optional.

NOTE: After the settings are completed, reboot the device to activate the modified settings.

LAN Settings [Wireless AP Mode]

MAC Address: It displays the router's LAN MAC address, which can not be changed.

IP Mode: You can select **Static IP** or **Dynamic IP**. If you select Static IP, you need to input the parameters provided by your ISP. If you choose Dynamic IP, you should set the computer's Internet protocol to obtain an IP address and DNS server address automatically.

IP Address: The device's LAN IP address (not your PC's IP address). The default value is **192.168.1.100**. If you change it, you need to use the new IP to log in to the Web interface.

Subnet Mask: The Router's LAN subnet mask. The default value is **255.255.255.0**.

Default Gateway: Input the Gateway provided by your ISP. If you are not sure, please inquire

your ISP or network administrator.

Primary DNS Address: Enter the necessary address provided by your ISP.

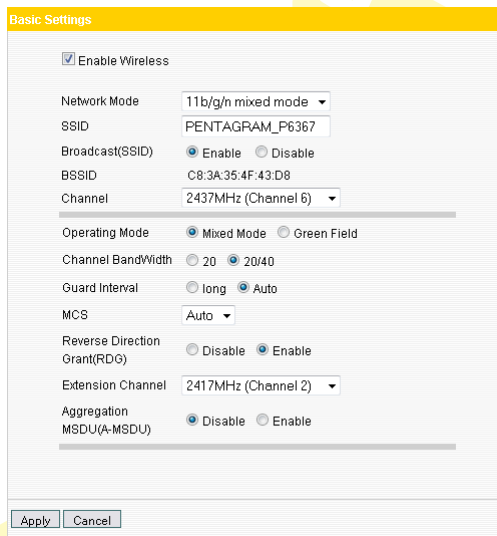
Secondary DNS Address: Enter the second address if your ISP provides, and it is optional.

Host Name: The device's WINS name which you can use to visit the device.

NOTE: Once you changed the IP address of the LAN port, you should use the new IP to enter the WEB management interface.

WLAN Settings

Basic Settings



The screenshot shows the 'Basic Settings' window for WLAN configuration. It includes the following fields and options:

- Enable Wireless:** A checked checkbox.
- Network Mode:** A dropdown menu set to '11b/g/n mixed mode'.
- SSID:** A text field containing 'PENTAGRAM_P6367'.
- Broadcast(SSID):** Radio buttons for 'Enable' (selected) and 'Disable'.
- BSSID:** A text field containing 'C8:3A:35:4F:43:D8'.
- Channel:** A dropdown menu set to '2437MHz (Channel 6)'.
- Operating Mode:** Radio buttons for 'Mixed Mode' (selected) and 'Green Field'.
- Channel BandWidth:** Radio buttons for '20' and '20/40' (selected).
- Guard Interval:** Radio buttons for 'long' and 'Auto' (selected).
- MCS:** A dropdown menu set to 'Auto'.
- Reverse Direction Grant(RDG):** Radio buttons for 'Disable' and 'Enable' (selected).
- Extension Channel:** A dropdown menu set to '2417MHz (Channel 2)'.
- Aggregation MSDU(A-MSDU):** Radio buttons for 'Disable' (selected) and 'Enable'.

At the bottom of the window are 'Apply' and 'Cancel' buttons.

Enable Wireless: Tick to enable the Router's wireless features. If you don't want to use this feature, you can disable it and all functions related with wireless will be disabled.

Network Mode: From this drop-down menu, you can select the wireless standards running on your network. The default is **11b/g/n mode**.

- **11b mode:** Select it if you have only Wireless-B devices.
- **11g mode:** Select it if you have only Wireless-G devices.
- **11b/g mixed mode:** Select it if you have only Wireless-B and Wireless-G devices.
- **11b/g/n mixed mode:** Select it if you have Wireless-B, Wireless-G and Wireless-N devices.

SSID: SSID (Service Set Identifier) is the unique name of the wireless network. Enter this SSID for wireless devices to have access to the router. You can either customize a network name or use the default.

Broadcast (SSID): Select **Enable** to enable the router' SSID to be scanned by wireless devices. The default is **Enabled**. If you disable it, the wireless devices must know the SSID for communication.

PENTAGRAM Cerberus [P 6367]

BSSID: Basic Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.

Channel: The channel used by the current router. You can select other effective channels from the drop-down list. There are channels 1 to 13 for your options. When there are many wireless signals around, you can select a different channel to reduce interference.

Operating mode: works in 11n mode only. Different wireless standards involve different frame formats in physical layer. **Green Field** mode can greatly improve the wireless transmission efficiency. However, if the device that is using 802.11n Greenfield mode does not adopt the same channel width that of 802.11b/g base station, device in 802.11b/g mode can not communicate with the Greenfield connection point. On the contrary, there will be collision, errors and resending in the information transferring process between them. For common usage, we recommend that you use the **Mixed Mode**, which integrates traditional mode and Green Field mode.

Channel bandwidth: Select the best channel bandwidth to enhance the wireless performance. When there are 11b/g and 11n wireless clients, please select the 802.11n mode of 20/40M frequency band; when there are only non-11n wireless clients, you can select 20M frequency band mode; when the wireless network mode is 11n mode, please select 20/40 frequency band to boost its throughput. After you finish the settings, click **Next** to enter the interface for wireless encryption settings.

Guard Interval: Works in 11n mode only. 802.11b/g standards require there's an 800ns interval between the information signs when sending them and this interval is called Guard Interval (GI). Different GIs determine whether there's interference affecting the transmission rate while sending the signal. We recommend that you use the default value.

MCS (Modulation Coding Scheme): Works in 11n mode only. The physical rate relies on several elements such as modulation method, encoding rate, the amount of the three-dimensional flow, 40MHz binding or not, thus, these elements which influence throughput combined will generate multiple physical rates for you choices. MCS can be interpreted as the complete combination of the elements which influence the rate. Each combination is uniquely marked with an integer.

Extension Channel: To figure out the network frequency range in 11n mode.

Aggregation MSDU: Aggregates multi-MSDU to become a bigger load. The MSDU can be considered as an Ethernet Message. Usually when AP or wireless client receives the message (MSDU) from the protocol station, they would mark it with Ethernet Head, which is called A-MSDU Sub-frame. However, it needs to be converted to 802.11 message format before being sent out through RF port. And A-MSDU technology aims to aggregate several A-MSDU Sub-frames and send out by encapsulating them into an 802.11 message. Thus, it reduces the occupied bits of PLCP Preamble, PLCP Header and 802.11MAC which are required to send an 802.11 message. Besides, the amount of response frame is decreased and the message sending rate is improved.

Security Settings

This interface enables you to configure wireless encryption. This device supports WPA-Personal, WPA2-Personal, mixed WPA/WPA2-Personal, Mixed WEP, OPEN, and SHARED etc. It is suggested you encrypt the wireless network to avoid network stealing. Three commonest encryption methods are introduced here (you need to input password to connect to your wireless network adapter when you have encrypted the router).

NOTE:

- To increase security level of a wireless network never use passwords from dictionary or which are very easy to remember.
- Using WEP protocol to secure wireless network is not recommended.
- Protocol 802.11n officially supports only WPA protocol with AES encryption algorithm. Using another security protocol and/or encryption algorithm may cause network to work without full speed or performance.

WPA-Personal

WPA is a standard and interoperable WLAN enhanced security solution which greatly strengthens the existing and future WLAN system data protection and access control ability. WPA originates from IEEE802.11i standard, and is compatible with it. WPA guarantees to protect WLAN users' data and only the authorized network users can have access to WLAN. The encryption Algorithms it adopts is better than WEP.

The screenshot shows the 'Security Settings' window. At the top, the SSID is 'PENTAGRAM_P6367'. The 'Security Mode' is set to 'WPA - Personal'. Under 'WPA Algorithms', 'AES' is selected with a radio button, while 'TKIP' and 'TKIP&AES' are unselected. The 'Pass Phrase' field contains 'PlsChangeMe'. The 'Key Renewal Interval' is set to '3600 second'. A red 'Notice' section states: 'Wireless Security Settings 802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.' At the bottom are 'Apply' and 'Cancel' buttons.

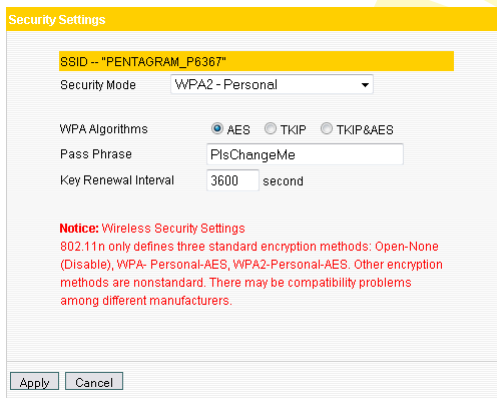
WPA Algorithms: You can choose either **AES** (Advanced Encryption Standard) mode or **TKIP** (Temporal Key Integrity Protocol) mode.

Pass Phrase: Please enter the encryption character string. It consists of 8-63 ASCII characters.

Key Renewal Interval: It refers to the valid period for the key.

WPA2-Personal

WPA2 (Wi-Fi Protected Access version 2) provides better security than Wireless Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) does. It does not only adopt TKIP encryption but also the new encryption mode: AES.



The screenshot shows a 'Security Settings' dialog box. At the top, the title is 'Security Settings'. Below it, the 'SSID' is set to 'PENTAGRAM_P6367'. The 'Security Mode' is set to 'WPA2 - Personal'. Under 'WPA Algorithms', 'AES' is selected with a radio button, while 'TKIP' and 'TKIP&AES' are unselected. The 'Pass Phrase' field contains 'PlsChangeMe'. The 'Key Renewal Interval' is set to '3600' seconds. A red 'Notice' section states: 'Notice: Wireless Security Settings 802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.' At the bottom, there are 'Apply' and 'Cancel' buttons.

WPA Algorithms: Select data encryption type. **AES** (Advanced Encryption Standard), **TKIP** (Temporal Key Integrity Protocol) and **TKIP&AES** are supported.

Pass Phrase: Please enter the encryption characters string. The valid character is ASCII. It consists of 8-63 ASCII characters.

Key Renewal Interval: It refers to the valid period for the key.

Mixed WEP

Wired equivalent protection (WEP) encrypts the data wirelessly transmitted between two devices to avoid unauthorized users' wire tapping or invasion. WEP security, based on RC4 data encryption technology, provides data confidentiality, integrity, and authentication for wireless network communication.

Security Settings

SSID -- "PENTAGRAM_P6367"

Security Mode: Mixed WEP

Default Key: Key 1

WEP Key 1 : Hex

WEP Key 2 : Hex

WEP Key 3 : Hex

WEP Key 4 : Hex

Notice: Wireless Security Settings
802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

Apply Cancel

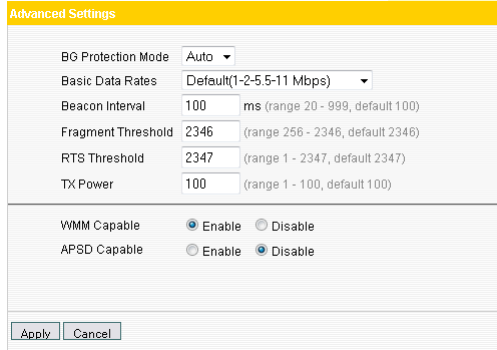
WEP Key: It can be set as **ASCII** and **Hex** formats.

Key description: Select ASCII code (5 or 13 ASCII characters) or valid Hex characters (10 or 26 hex characters).

Default Key: You can select one among the 4 preset keys.

Advanced Settings

This section introduces configuration of wireless advanced functions, which enables you to configure wireless parameters at length, including BG protection mode, basic data rates, Fragmentation threshold, RTS threshold, and WMM etc.



The image shows a screenshot of the 'Advanced Settings' dialog box. It contains several configuration options:

- BG Protection Mode:** A dropdown menu set to 'Auto'.
- Basic Data Rates:** A dropdown menu set to 'Default(1-2-5.5-11 Mbps)'.
- Beacon Interval:** A text input field with '100' and a unit dropdown set to 'ms'. A range hint '(range 20 - 999, default 100)' is shown.
- Fragment Threshold:** A text input field with '2346'. A range hint '(range 256 - 2346, default 2346)' is shown.
- RTS Threshold:** A text input field with '2347'. A range hint '(range 1 - 2347, default 2347)' is shown.
- TX Power:** A text input field with '100'. A range hint '(range 1 - 100, default 100)' is shown.
- WMM Capable:** Two radio buttons, 'Enable' (selected) and 'Disable'.
- APSD Capable:** Two radio buttons, 'Enable' and 'Disable' (selected).

At the bottom of the dialog are 'Apply' and 'Cancel' buttons.

BG protection Mode: **Auto** by default. It is good for relatively slow 11b/g wireless clients to connect 11n wireless network smoothly in a complicated wireless area.

Basic Data Rates: You can select one suitable Basic Data Rate from the drop-down menu according to your need. The default value is **Default(1-2-5.5-11Mbps)**. It is recommended not to modify this value.

Beacon Interval: Set the beacon interval for AP. Generally, the smaller the interval is, the faster wireless clients connect; the bigger it is, the higher efficiency wireless network data transmission will achieve. Default value is 100. It is recommended not to modify this value.

Fragment Threshold: The fragmentation threshold defines the maximum transmission packet size in bytes. The packet will be fragmented if the wireless data packet is bigger than the threshold setting. The default size is **2346** bytes. It is recommended not to modify this value.

RTS Threshold: RTS is short for Request to Send. When the packet size exceeds this threshold, enable CTS/RTS to reduce collision possibility. For the long-distance clients to access in interference involved environment, set a relatively smaller RTS value. It is recommended not to modify the default value in SOHO environment; otherwise it will affect AP performance.

TX Power: Set the output power of wireless radio. The default value is **100**.

WMM Capable: It will enhance the data transfer performance of multimedia data when they're being transferred over wireless network. It is recommended to enable it if you are not familiar with WMM.

APSD Capable: It is used for auto power saving service. The default is **Disable**.

WPS Settings

WPS (Wi-Fi Protected Setting) is an easy and quick way to establish the encrypted connection between the wireless network clients and the device. Users only need to enter PIN code or press WPS button on the side panel to configure it. In the **WLAN Settings** menu, click **WPS settings** to enter the configuration interface.

WPS Config

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Settings: ☐ Disable ☒ Enable

WPS mode: ☐ PBC ☐ PIN

WPS Summary	
WPS Current Status:	Idle
WPS Configured:	No
WPS SSID:	PENTAGRAM_P6367
WPS Auth Mode:	Open
WPS Encrypt Type:	None
WPS Default Key Index:	1
WPS Key(ASCII):	
AP PIN:	51947125

WPS Settings: To enable or disable WPS function.

WPS mode: Provide two simple WPS ways: **PBC** (Push-Button Configuration) and **PIN** code.

- **PBC:** Select the **PBC** and click **Save** or press the **WPS/RESET** button on the side panel of the device for about one second, at the same time enable client's WPS/PBC to establish connection.

Operation process: Press the button for about one second and WPS indicator will be flashing for 2 minutes, which means the WPS is enabled. During the flashing time, you can enable the WPS/PBC of the wireless client for them to negotiate. Two minutes later, the WPS indicator will be off, which means the WPS connection is completed. Repeat the above steps to add more clients. At present, the WPS supports up to 32 clients

- **PIN:** If this option is enabled, you need to enter a PIN code matching with the one in the wireless client.

WPS Summary: It displays the current status of Wi-Fi protected setting, including authentication mode, encryption type, default key and other information.

WPS Current Status: **Idle** means WPS is in idle state. **Start MSC process** means the process has been started and is waiting for being connected. **Configured** means the negotiation between server and clients is successful.

WPS Configured: **Yes** means WPS feature is enabled and goes into effect. **No** means it doesn't takes effect. Usually when the AP-security has been enabled, it displays **No**.

WPS SSID: It displays the main SSID set by WPS. WPS only takes effect in main SSID

WPS Auth. Mode: The authentication mode adopted by WPS, usually it is WPA/WPA2-Personal mode.

WPS Encryption Type: The encryption type used by WPS, generally AES/TKIP.

WPS key: The effective key automatically generated by AP.

AP PIN: The PIN code used by default.

PENTAGRAM Cerberus [P 6367]

Reset OOB: Press this button, the WPS client will be in idle state, and WPS indicator will turn off. AP will not respond to the WPS client's connection requests.

WDS Settings

Wireless AP signal coverage has range limits. WDS is mainly used to repeat wireless signal, and enlarge its coverage. Please keep SSID, channel and encryption type of all AP respectively consistent.

WDS Settings

WDS Mode: Disable

Attention: To configure WDS

1. In the MAC address field, input the connected device's MAC address. If the connected device has configured the WDS encryption method, please enter the same key values.

2. If you need to authorize wireless client's access, please configure the settings in the "Wireless Settings->Security Setting" window. After the configuration is completed, click "Save" and reboot the Router to implement communication between the WDS device.

Apply Cancel

This router supports three WDS modes: **Lazy**, **Bridge**, **Repeater**.

- **Lazy:** In this mode, the connected router must be in **Bridge** or **Repeater** mode and the MAC address of your router must be entered.
- **Bridge:** In this mode, the connected router must be in **Lazy** or **Repeater** mode. Manually add the MAC address of the connected router to **AP MAC** address list or scan to select.
- **Repeater:** In this mode, the connected router can be in **Lazy**, **Bridge** mode or single client. Manually add the MAC address of the connected router to **AP MAC** address list or scan to select.

Access Control

To secure your wireless LAN, the wireless access control is actually based on the MAC address management to allow or block the specific clients to access the wireless network.

Wireless Access Control

MAC Address Filter: Off

Apply Cancel

MAC Address Filter:

- **Allow:** to only allow the clients in the list to access the wireless network.
- **Block:** to only prevent the clients in the list from accessing the wireless network.

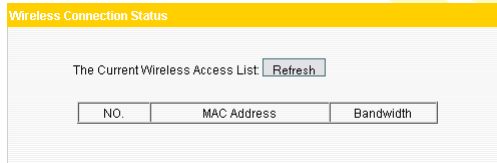
MAC Address Management: Input the MAC addresses of the wireless clients you want to allow or

block and click **Add**.

MAC Address list: Show the added MAC addresses. You can add or delete them.

Connection Status

This page displays wireless client's connection status, including MAC address, rate, etc.



The screenshot shows a web interface titled "Wireless Connection Status". Below the title, it says "The Current Wireless Access List" followed by a "Refresh" button. Below this is a table with three columns: "NO.", "MAC Address", and "Bandwidth". The table is currently empty.

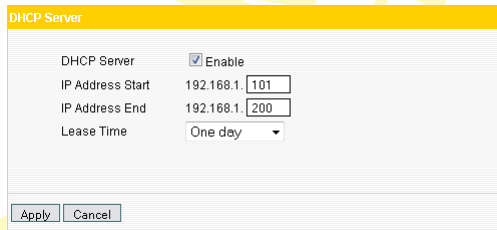
MAC Address: Shows the wireless MAC addresses of the hosts connected to the Router.

Bandwidth: Shows the channel bandwidth current connected host (the wireless client) use.

DHCP Server [3G Router, WISP or Wireless Router Mode]

DHCP Server

DHCP server is to configure TCP/IP parameters for all the computers in LAN. When you enable the router's DHCP server, the DHCP server will automatically configure the TCP/IP protocol for all the computers in LAN (including IP address, subnet mask, gateway, DNS, etc.).



The screenshot shows a web interface titled "DHCP Server". It contains the following configuration options:

- DHCP Server:** A checkbox labeled "Enable" which is checked.
- IP Address Start:** A text input field containing "192.168.1." followed by a small box containing "101".
- IP Address End:** A text input field containing "192.168.1." followed by a small box containing "200".
- Lease Time:** A dropdown menu showing "One day".

At the bottom of the form are two buttons: "Apply" and "Cancel".

DHCP Server: Enable or disable DHCP server to automatically assign IP addresses.

IP Address Start: Starting IP addresses automatically distributed by DHCP server.

IP Address End: Ending IP addresses automatically distributed by DHCP server.

Lease Time: The length of the IP address lease.

DHCP List and Binding

DHCP client list displays computers' IP address, MAC address, host name and other information which are assigned by the DHCP server. You can manually enter the IP and MAC address and convert it to static allocation. According to the connected computer's MAC address, DHCP will assign the appropriate IP address. If you can not find the corresponding static binding entry, assign an IP from the DHCP pool to the computer.

DHCP List&Binding

Static IP

IP Address 192.168.1.

MAC Address

NO.	IP Address	MAC Address	IP-MAC bind	Delete								
<div style="text-align: right; padding-right: 10px;"><input type="button" value="Refresh"/></div> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th style="width: 20%;">Host Name</th> <th style="width: 20%;">IP Address</th> <th style="width: 20%;">MAC Address</th> <th style="width: 20%;">Lease</th> </tr> </thead> <tbody> <tr> <td>PM06</td> <td>192.168.1.101</td> <td>00:1C:C4:C6:0E:5C</td> <td>23:53:16</td> </tr> </tbody> </table>					Host Name	IP Address	MAC Address	Lease	PM06	192.168.1.101	00:1C:C4:C6:0E:5C	23:53:16
Host Name	IP Address	MAC Address	Lease									
PM06	192.168.1.101	00:1C:C4:C6:0E:5C	23:53:16									

IP Address: Enter the IP address which needs static binding.

MAC Address: Enter the MAC address of the computer you want to bind.

Host name: It displays the name of the bound computer.

Lease Time: The left time for the corresponding IP address lease.

Virtual Server [3G Router, WISP or Wireless Router Mode]

Port Range Forwarding

This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

Port Range Forwarding

The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

NO.	Start Port-End Port	To IP Address	Protocol	Enable	Delete
1.	<input type="text"/> - <input type="text"/>	192.168.1. <input type="text"/>	TCP ▾	<input type="checkbox"/>	<input type="checkbox"/>
2.	<input type="text"/> - <input type="text"/>	192.168.1. <input type="text"/>	TCP ▾	<input type="checkbox"/>	<input type="checkbox"/>
3.	<input type="text"/> - <input type="text"/>	192.168.1. <input type="text"/>	TCP ▾	<input type="checkbox"/>	<input type="checkbox"/>
4.	<input type="text"/> - <input type="text"/>	192.168.1. <input type="text"/>	TCP ▾	<input type="checkbox"/>	<input type="checkbox"/>
5.	<input type="text"/> - <input type="text"/>	192.168.1. <input type="text"/>	TCP ▾	<input type="checkbox"/>	<input type="checkbox"/>
6.	<input type="text"/> - <input type="text"/>	192.168.1. <input type="text"/>	TCP ▾	<input type="checkbox"/>	<input type="checkbox"/>
7.	<input type="text"/> - <input type="text"/>	192.168.1. <input type="text"/>	TCP ▾	<input type="checkbox"/>	<input type="checkbox"/>
8.	<input type="text"/> - <input type="text"/>	192.168.1. <input type="text"/>	TCP ▾	<input type="checkbox"/>	<input type="checkbox"/>
9.	<input type="text"/> - <input type="text"/>	192.168.1. <input type="text"/>	TCP ▾	<input type="checkbox"/>	<input type="checkbox"/>
10.	<input type="text"/> - <input type="text"/>	192.168.1. <input type="text"/>	TCP ▾	<input type="checkbox"/>	<input type="checkbox"/>

Well-Known Service Port: ID

Start/End Port: Service port range provided by the mapped host in internal network.

IP Address: the IP address of the computer which is used as a server in LAN.

Protocol: It includes **TCP**, **UDP** and **Both**. Select **Both** when you are not sure about which protocol to use.

Enable: Only after you enable it, can the configured rules go into effect.

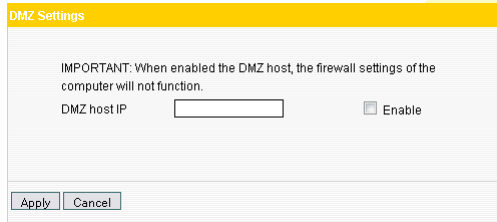
Delete: Click to empty the parameters.

Well-Known Service Port: In **Well-Known Service Port** there are commonly used protocol ports. Select one among them and a serial number for ID then click **Add** to add it to the list. You can also manually add the ports which are not included in the **Well-Known Service Port**.

Add: helps you to add the **Well-Known Service Port** to the item you are configuring.

NOTE: If you set the virtual server of the service port as **80**, you must set the **Remote Web management** port on **Security Settings** menu at any value except **80**, such as **8080**. Otherwise, there will be a conflict to disable the virtual server.

DMZ Settings

A screenshot of the 'DMZ Settings' dialog box. It has a yellow title bar. The main area contains the text: 'IMPORTANT: When enabled the DMZ host, the firewall settings of the computer will not function.' Below this is a label 'DMZ host IP' followed by a text input field. To the right of the input field is a checkbox labeled 'Enable'. At the bottom of the dialog are two buttons: 'Apply' and 'Cancel'.

DMZ Host IP: Please enter the IP address of the LAN computer which you want to set as the DMZ host.

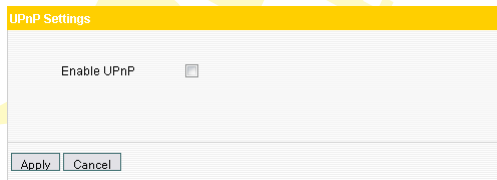
Enable: Click to enable/disable the DMZ host.

For example: Set the LAN computer at the IP address of 192.168.1.10 as a DMZ Host to intercommunicate with another host on the Internet.

NOTE: When the DMZ host is enabled, the computer is completely exposed to extranet, and the firewall settings of the DMZ host will not function.

UPnP Settings

UPnP (Universal Plug and Play), which goes into effect under Windows XP or Windows ME (NOTE: system needs to be integrated with or installed with DirectX 9.0) or would also go into effect if you have installed application software that supports UPnP. With the UPnP function, hosts in LAN can request the router to process some special port switching so as to enable external hosts to visit the resources in the internal hosts.

A screenshot of the 'UPnP Settings' dialog box. It has a yellow title bar. The main area contains the text: 'Enable UPnP' followed by a checkbox. At the bottom of the dialog are two buttons: 'Apply' and 'Cancel'.

Enable UPnP: Click to enable/disable the UPnP.

Traffic Control

Traffic Control

Traffic Control is for communication traffic limit in the LAN and WAN. It can support limitation rules up to 20 entries and simultaneously control maximum of 254 PCs' traffic. In addition, IP address range configuration is supported.

Traffic Control Settings

Traffic Control ☒

Interface **Upload BW** **Download BW**

WAN: 512 2048 (kByte/s)

Protocol	Port	Service
Services: TCP&UDP	0	All
IP: 192.168.1.		
Up/Down: Up		
BW Range:		(kByte/s)
Apply:		

Add

Num	Port	IP	Up/Down	BW Range	Apply	Edit	Del
-----	------	----	---------	----------	-------	------	-----

Apply Cancel

Traffic Control: To enable or disable the internal IP traffic control. The default is disabled.

Interface: Enter the actual uploading and downloading bandwidth in WAN port.

Service: To select the service type for traffic control, such as HTTP service.

IP Address: The range of IP addresses, it can be a single IP or IP range.

UP/Down: To specify the traffic heading way for the selected IP addresses: uploading or downloading.

Bandwidth Range: The Minimum/Maximum Uploading/downloading data traffic (KB/s) which can not exceed the WAN bandwidth limit.

Apply: Check to enable the currently edited rule.

Add: Click **Add to list** button to add the current rule to the rule list.

Apply: Click **Apply** to activate the current rule.

Cancel: Click **Cancel** to drop all settings saved last time.

Traffic Statistics

This function is to calculate the data traffic of the client that connected to this router and the speed of each client.

Traffic Statistic						
<input checked="" type="checkbox"/> Enable						
IP Address	UP Rate(kByte/s)	Down Rate(kByte/s)	Send Packet	Send Byte(MByte)	Receive Packet	Receive Byte(MByte)
<input type="button" value="Apply"/>						

3G WAN Traffic [3G Router Mode]

3G WAN Traffic

In 3G WAN access mode, 3G WAN traffic statistic function is supported. Click **3G WAN traffic** to check the router's Internet traffic, transmission rate, transmission data volume and data traffic for the recent two months, and you will know how much traffic still can be used.

3G WAN Traffic	
The results are only for reference, for the actual traffic please goes to the ISP.	
Upload speed:	0 Kbps
Download speed:	0 Kbps
TX bytes:	0 KB
RX bytes:	0 KB
3G WAN traffic of February:	0 KB
3G WAN traffic of January:	0 KB
Save Traffic data: <input checked="" type="radio"/> Disable <input type="radio"/> Enable	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

You can enable or disable **Save Traffic data** in 3G WAN Traffic. The default is disabled. Enable it and the system will save the 3G traffic data.

NOTE: *The statistics of 3G WAN Traffic are for reference only, the actual statistics is subject to the ISP. (This router can only calculate the time or traffic flow when the 3G modem card access Internet via the device; however, it fails to do so when the 3G modem card is directly plugged into the computer).*

Security Settings [3G Router, WISP or Wireless Router Mode]

Client Filter

To better manage the computers in LAN, you can control LAN computers' access to some ports on Internet by data packet filters function.

Client Filter

Client Filtering Settings ☒

Access Policy: 10

Enable: ☐ Delete the Policy:

Filtering Mode: ☒ Disable ☐ Enable access the Internet

Policy Name:

Start IP: 192.168.1

End IP: 192.168.1

Port:

Type: TCP

Times: 0 ~ 0

Date: ☒ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wen ☐ Thr ☐ Fri ☐ Sat

Client Filtering Setting: Check to enable client filter.

Access Policy: Select one number from the drop-down menu.

Enable: Check to enable the access policy.

Filtering mode: Select **Disable** to forbid the filtered hosts' corresponding ports to access the Internet at a specified time. Select **Enable** to permit the filtered hosts' corresponding ports to access the Internet at a specified time.

Start/End IP: Enter the starting/ending IP address.

Port: Enter the controlled TCP/UDP protocol port; and it can be a port range.

Type: Select the protocol used by the controlled data packets (TCP, UDP or Both).

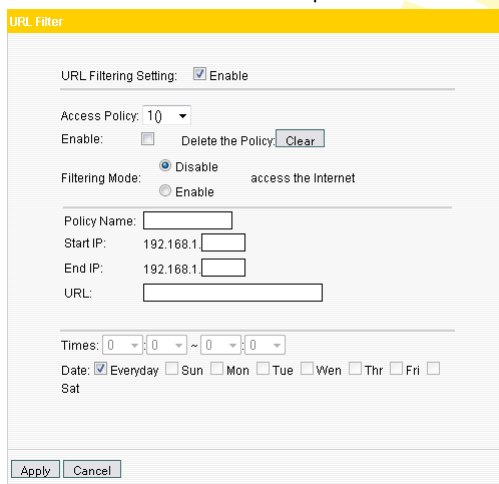
Time: Select the time range of client filter rule.

Date: select according to your needs.

Apply: Select **Apply** to enable the settings.

URL Filter

To better control the LAN computers' access to the websites; you can use URL filtering to permit or forbid their access to certain websites at a specified time.



URL Filter

URL Filtering Setting: ☒ Enable

Access Policy: 10

Enable: ☐ Delete the Policy:

Filtering Mode: ☒ Disable ☐ Enable access the Internet

Policy Name:

Start IP: 192.168.1

End IP: 192.168.1

URL:

Times: 0 ~ 0 ~ 0 ~ 0

Date: ☒ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wen ☐ Thr ☐ Fri ☐ Sat

URL Filtering Setting: Check to enable URL filter.

Access Policy: Select one number from the drop-down menu.

Enable: Check to enable the access policy.

Filtering mode: Select **Disable** to forbid the computer at the filtered IP address to access the Internet at a specified time. Select **Enable** to permit the computer at the filtered IP address to access the Internet at a specified time. Each rule only takes effect on the IP address of its own.

Start/End IP: Enter the starting/ending IP address.

URL: Specify the text strings or keywords needed to be filtered. If any part of the URL contains these strings or words, the web page will not be accessible and displayed.

Time: Select the time range of client filter rule.

Date: select according to your needs.

Apply: Select **Apply** to enable the settings.

MAC Filter

In order to manage the computers in LAN better, you could control the computer's access to Internet by MAC Address Filter.

MAC Filtering Settings: Check to enable MAC address filter.

Access Policy: Select one number from the drop-down menu.

Enable: Check to enable the access policy.

Filtering mode: Select **Disable** to forbid the computer at the filtered MAC address to access the Internet at a specified time. Select **Enable** to permit the computer at the filtered MAC address to access the Internet at a specified time.

Policy Name: Enter a name for the access policy selected.

MAC address: add the computer's MAC address to the MAC address field.

Time: Select the time range of client filter rule.

Date: select according to your needs.

Apply: Select **Apply** to enable the settings.

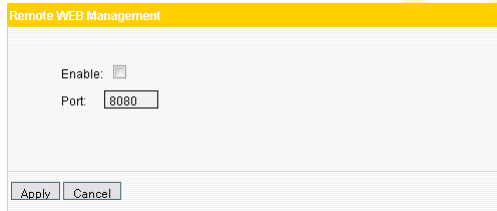
Prevent Network Attack

Check to enable the router's Network Attack Prevention function. Once detecting the device is attacked by some hosts, the router will limit its bandwidth automatically. The attacker's IP address can be found from the **System Log**.

Prevent Network Attack: Check to enable it for attack prevention.

Remote WEB Management

This section is to set the IP address and WEB management port of the computer that can implement remote WEB management.



Enable: Check to enable remote web management.

Port: The management port used by remote WEB management.


WAN IP Address Range: Specify the range of the WAN IP address for remote management.

NOTE:

- If you want to login the device's Web-based interface via port **8080**, you need to use the format of WAN IP address: port (for example **http://123.123.123.123:8080**) to implement remote login.
- If your WAN IP address starts and ends with **0.0.0.0**, it means all hosts in WAN can implement remote Web management. If you change the WAN IP address as **123.123.123.122-123.123.123.124**, then only the computer with its IP address at this IP address range (for example, **123.123.123.122**, **123.123.123.123** and **123.123.123.124**) can implement remote Web management.

WAN Ping

The ping test is to check the status of your Internet connection. When this function is enabled, the router will not respond to Ping request from WAN, but LAN computer can ping pass.



Ignore the Ping from WAN: Check to ignore the ping request and give no reply.

Routing Settings

This page displays the router's main routing table

Routing Table				
Destination IP	Subnet Mask	Gateway	Metric	Interface
239.255.255.250	255.255.255.255	0.0.0.0	0	br0
192.168.1.0	255.255.255.0	0.0.0.0	0	br0

The main duty for a router is to look for a best path for every data packet, and transfer this data packet to a destination. So, it's essential for the router to choose the best path, i.e. routing arithmetic. In order to complete this work, the related data packets of various transfer paths, i.e. routing table, are saved in the router for options.

System Tools

Time Settings

This section is to set the router's system time; you can either set the time by yourself or obtain the GMT time from the Internet.

Time Settings	
Time Zone:	(GMT+08:00) Beijing, Chongqing, Hong Kong SAR, Urumqi
(Notice: GMT time can be obtained only after accessing to the Internet.)	
Customized time:	<input checked="" type="checkbox"/>
	2009 Y 08 M 01 D 00 H 34 M 46 S
<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>

Time Zone: Select your time zone from the drop-down menu.

Customized time: Enter the time you customize.

NOTE: When the Router is powered off, the time settings will be lost. When you next time access to the Internet, the Router will obtain GMT time automatically. And only when you have access to the Internet and obtain the GMT time, or set the time on this page first, the time in other features (e.g. security settings) can be activated.

DDNS [3G Router, WISP or Wireless Router Mode]

DDNS is short for Dynamic Domain Name Server, and it takes effect in 3G router, WISP and wireless router modes. It is to assign a fixed host and domain name to a dynamic Internet IP address, which is used to monitor hosting website, FTP server and so on behind the Router. If you want to activate this function, please select **Enable** and a DDNS service provider to sign up. Owing to ISP most times provides dynamic IP address, DDNS is used to capture the changeable IP address and match the fixed domain. Then users can have access to the Internet to communicate with others. DDNS can help you establish virtual host in your home and company.

Service Provider: Select one from the drop-down menu and click **Sign up** for registration.

User Name: Enter the user name the same as the registration name.

Password: Enter the password the same as the registration password.

Domain Name: Enter the effective domain name which is optional.

Backup/Restore Settings

Backup Settings

1. Click **Backup** button to export the configuration files and select the path to save it.
2. Click **Save** to save the configuration files.

Restore Settings

1. Click **Browse** button to select the backup files.
2. Click **Restore** button to restore the previous settings.

Restore to Factory Default Settings

This button is to restore all settings to the default values.

NOTE: Click **Restore to Factory Default Settings**, and the router will reboot automatically.

Firmware Upgrade

By upgrading the router's firmware, you'll get more stable firmware version and appreciated routing function. For upgrading files, you can download from www.pentagram.eu.

Browse: click this button to select the upgrade file.

Upgrade: click this button to start the upgrading process. After the upgrade is completed, the Router will reboot automatically.

NOTE: Do not disconnect the device during the upgrading process.

Reboot the Router

Rebooting the Router makes the settings configured go into effect or to set the Router again if setting failure happens.

Reboot the router: Click this button to reboot the device.

Change Password

This section is to change the default user name and password.

Change Password

Note: User Name and Password makeup only by number or/and letter.

User Name

Old Password

New Password

Re-enter to Confirm

User Name: Enter a new user name for the device.

Old Password: Enter the old password.

New Password: Enter a new password.

Re-enter to Confirm: Re-enter to confirm the new password.

NOTE: *It is highly recommended to change the password to secure your network and the Router.*

System Log

The section is to view the system log.

System Log

Page 1 content

1	2009-08-01 00:37:59	System	No USB modem found.
---	---------------------	--------	---------------------

[1]

Refresh: Click this button to update the log.

Clear: Click this button to clear the log record.

Logout

After you have finished the settings completely, in logout page click **Yes** to logout the web management page.

Compatible 3G modems

Brand	Model
AT&T	USBConnect mercury
AT&T	GI0322
BeiFang Qingniao	EC805U
CCU	680
CCU	650
ChangHe	868
ChangHong	CH600
Cricket	UM185C
Cricket	A600
D-LINK	DWM_162U5
D-LINK	DWM_162
Datang	AirCard 901
DCWL	390
DeUnite	DU360
DeUnite	DU456
DeUnite	DU458
DTM	5731E
GXZG	GX100C
HiNet	E220
HUAWEI	EC169
HUAWEI	EC169 New
HUAWEI	EC1260 China
HUAWEI	EC1260 New
HUAWEI	EC1260 India
HUAWEI	EC1261
HUAWEI	ET128
HUAWEI	E1750
HUAWEI	EC226
HUAWEI	E1630 TMobile
HUAWEI	E176G
HUAWEI	E176 Chile
HUAWEI	E180
HUAWEI	EC170 BT
HUAWEI	EC168C_Reliance
HUAWEI	EC168C_Tata
HUAWEI	MD-@ HSUPA
HUAWEI	E160E
HUAWEI	E1550
HUAWEI	E2220 3G UK
HUAWEI	BASE e.plus E169
Intertel leader	C810
JinXunChi	EV169
MACAO	CTM H21
Ruijie	EV2000

Brand	Model
Sierra	USB306
Sprint	USB 598
Sprint	U150
Sprint	U760
T-Linking	T-Linking
T-Mobile	UMG181
Tenda	3G189C
TIMESPOWER	WM2080A-110
Ttec	WS220
Ttec	WS 119
TURKCELL	E176G
Verizon	UMW190VW
Verizon	UMW190
Verizon	UMW175VW
Verizon	USB760
Vodafone	E220
Vodafone	K3520
Vtton	E1916
WEWINS	U602D
ZTE	MU351
ZTE	AC580
ZTE	AC581
ZTE	AC581 New1
ZTE	AC581 New2
ZTE	AC560
ZTE	AC560-New
ZTE	MF626 Chile
ZTE	MF626 TMobile
ZTE	AC2736
ZTE	AC2746
ZTE	AC8710
ZTE	MF637U
ZTE	MU350
ZTE	MF622
ZTE	MF627
ZTE	AC2726
ZTE	AC2726 Reliance
ZTE	AC8700 BSNL
ZTE	AC8710 TATA
	CM810EV
	MC727
	LKT 828
	Modem LC625

