200 Mbps High-speed

Powerline Router

User’s Manual

(DN-15017)

Index

FCC Part 68 3
FCC Part 15 4
Chapter 1 Introduction 5
1.1 Overview 5
1.2 Features 5
1.3 System Requirements 6
Chapter 2 Installation 7
2.1 Checklist 7
2.2 The Front LEDs 8
2.3 The Rear Ports 8
2.4 The Bottom Port 9
Chapter 3 Configuration 9
3.1 Determine your connection settings 9
3.2 Connecting the Wireless 11n Router to your network 9
3.3 Configuring with Web Browser 9
3.3.1 WAN Setting 11
3.3.2 LAN Setting 13
3.3.3 DHCP Setting 14
3.3.4 Static Route Setting 15
3.3.5 NAT Setting 16
3.3.6 Packet Filter Setting 18
3.3.7 URL Filter Setting 20
3.3.8 Security Setting 21
3.3.9 UPNP Setting 22
3.3.10 DDNS Setting 23
3.3.11 QOS Setting 24
3.4.1 System Information 25
3.4.2 Routing Table 26
3.4.3 Packet Statistics 27
3.4.4 System Log 28
3.5.1 Admin Account 29
3.5.2 System Log Setting 30
3.5.3 Data / Time 31
3.5.4 Ping Test 32
3.5.5 Config Setting 33
3.5.6 Firmware Update 34

3.6.1 Logout 35
3.6.2 Reboot 36
3.7.1 TCP/IP Settings for Windows Operating System 37
Chapter 4. Powerline Networking Utility 44
4.1 Configuration Utility Setup 44
4.1.1 Installation of the Utility 44
4.2 Windows Configuration Utility 46
4.3 User Interface 47
4.3.1 Main Screen 47
4.3.2 Privacy Screen 51
4.4 Diagnostics Screen 53
4.4.1 About Screen 55
4.4.2 Preferences 55
5. Push Button Setting 56
6. Trouble Shooting 59
Appendix A Glossary 60
Appendix B Cabling / Connection 67

FCC Part 68

This equipment complies with Part 68 of the FCC Rules. On the bottom of this equipment is a label that contains the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. You must provide this information to the telephone company upon request.

The REN is useful to determine the quantity of devices you may connect to the telephone line and still have those entire devices ring when your number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If the modem causes harm to the telephone network, the telephone company may discontinue your service temporarily.
If possible, they will notify you in advance. But if advance notice isn't practical, you will be notified as soon as possible.
You will be advised of your right to file a complaint with the FCC.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this modem, please contact your dealer for repair/warranty information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected or you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

FCC Part 15

The modem generates and uses radio frequency energy. If it is not installed and used properly in strict accordance with the user's manual, it may cause interference with radio and television reception. The modem has been tested and found to comply with the limits for Class B computing devices in accordance with the specifications in Subpart B, Part 15 of the FCC regulations. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. FCC regulations require that shielded interface cables be used with your modem.

If interference does occur, we suggest the following measures be taken to rectify the problem:

1) Move the receiving antenna.

2) Move the modem away from the radio or TV.

3) Plug the modem into a different electrical outlet.

4) Discuss the problem with a qualified radio / TV technician.

CAUTION:

Changes or modifications not expressly approved by the party responsible for compliance to the FCC Rules could void the user's authority to operate this equipment.

Cable connections:

All equipment connected to this modem must use shielded cable as the interconnection means.

Notes:

Operation is subject to the following two conditions:

1) This device may not cause harmful interference, and

2) This device must accept any interference received including interference that may cause undesired operation.

Chapter 1 Introduction

Congratulations on your purchase of an Instant Powerline 200M Router with 3-port Fast Ethernet Switch and Homeplug for cable and DSL application. The Powerline Router is the perfect option to connect a small group of PCs to a high-speed Broadband Internet connection or to an Ethernet backbone. Configurable as a DHCP server, the Broadband Router acts as the only externally recognized Internet device on your local area network (LAN). The Router serves as an Internet firewall, protecting your network from being accessed by outside users.

1.1 Overview

Unlike a simple hub or switch, the setup of the Cable/DSL Router consists of more than simply plugging everything together. Because the Router acts as a DHCP server, you will have to set some values within the Router, and also configure your networked PCs to accept the IP Addresses the Router chooses to assign them. And generally there are three different operating modes for your applications. And you can know which mode is necessary for your system from ISP. These three modes are PPPoE, DHCP client and Static IP. Actually all these are for IP address of WAN.

1.2 Features

- Router Mode
  - PPP over Ethernet (RFC-2516)
  - DHCP Server and Client
  - NAPT (Network Address and Port Translation)
  - NAT (Network Address Translation
- Internet Access
  - TCP/IP, UDP, ICMP, ARP, RARP, PPPoE, NAT, DHCP (client/server), Static IP assignment
- Security Features
  - Password protected configuration access
  - User authentication (PAP/CHAP) for PPP connection
- Powerline Features
  - Up to 200M data rates for Powerline network
  - Support 128-Bit AES link encryption for Powerline security
  - Support co-exist with Powerline 85/14M .
- Security
  - Support packet inspection and filtering
  - Intrusion detection and protection
  - Password protected system management

- Ethernet Interface
  - Compliant with IEEE 802.3 and 802.3u 10/100 Mbps
- HTTP Web-Based Management
  - Firmware upgrade by UI
  - WAN and LAN side connection statistics
  - Advanced QoS
  - Password protected access
  - System log

1.3 System Requirements

1) Personal computer (PC)
2) Pentium II 233 MHz processor minimum
3) 32 MB RAM minimum
4) 20 MB of free disk space minimum
5) Ethernet Network Interface Controller (NIC) RJ45 Port
6) Internet Browser

Chapter 2 Installation

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

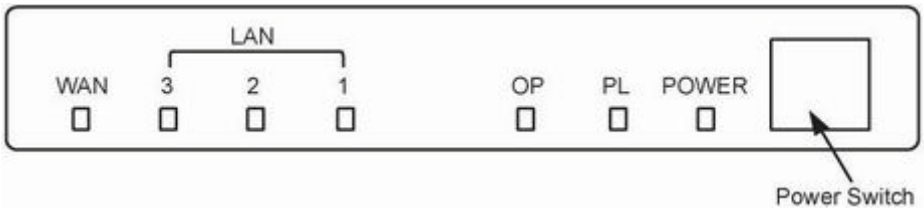
2.1 Checklist

Check the shipping box carefully to ensure that the contents include the items you ordered. If any of the items are missing or damaged, contact your local distributor. The contents of your carton may vary depending on your service provider.

Contents description

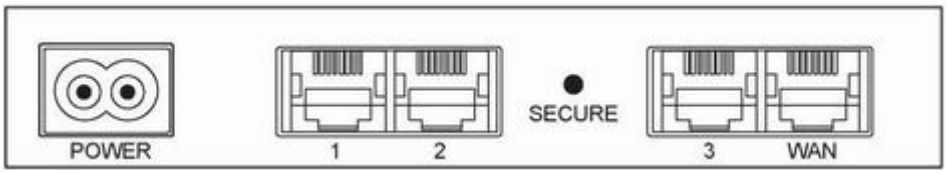
1) Powerline 200M Router for home/office use
2) Powerline 200M Router Installation and Operation Guide (this publication)
3) Power cord
4) Ethernet cable Ethernet category 5 twisted pair cable (6 ft)

2.2 The Front LEDs



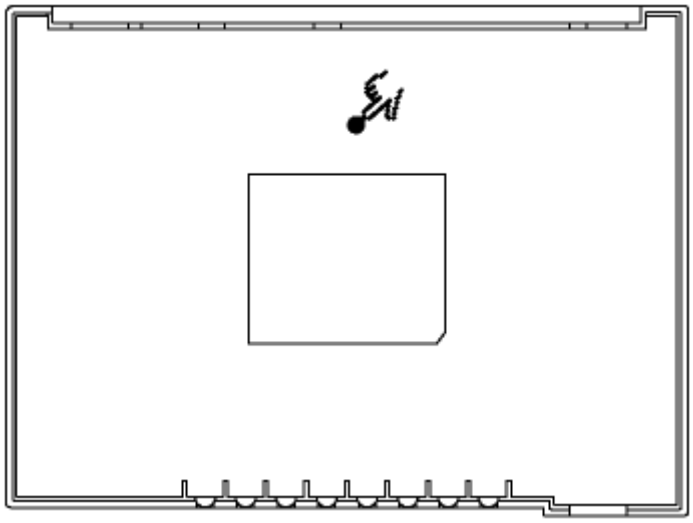
LED	State	Description
POWER	ON	Press the button to power one the router.
WAN	ON	"Showtime"-successful connection between ADSL modem and telephone company's network.
	Flashing	"Handshaking"-modem is trying to establish a connection to telco's network Modem is powered OFF ADSL Carrier Detect if LED is flash.
	OFF	No link.
PL	Flashing	When the router detect other Powerline devices
OP	Flashing	The router running well.
LAN 1-3	ON	Link
	Flashing	TX or RX activity
	OFF	No Link These three LAN (Local Area Network) ports are where you will connect networked devices, such as PCs, print servers remote hard drives, and anything else you want to put on your network.

2.3 The Rear Ports



Connector	Description
POWER	Power connector with power cord.
LAN (1-3)	Router is successfully connected to a device through the corresponding port (1, 2 or 3). If the LED is flashing, the Router is actively sending or receiving data over that port.
Secure	Button can auto secure and group the Powerline devices.
WAN	The WAN (Wide Area Network) Port is where you will connect your cable, DSL modem or Ethernet backbone.

2.4 The Bottom Port



Connector	Description
Reset Switch	Press 10 sec to reboot the router and restore default settings.

Chapter 3 Configuration

3.1 Determine your connection settings

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

3.2 Connecting the Wireless 11n Router to your network

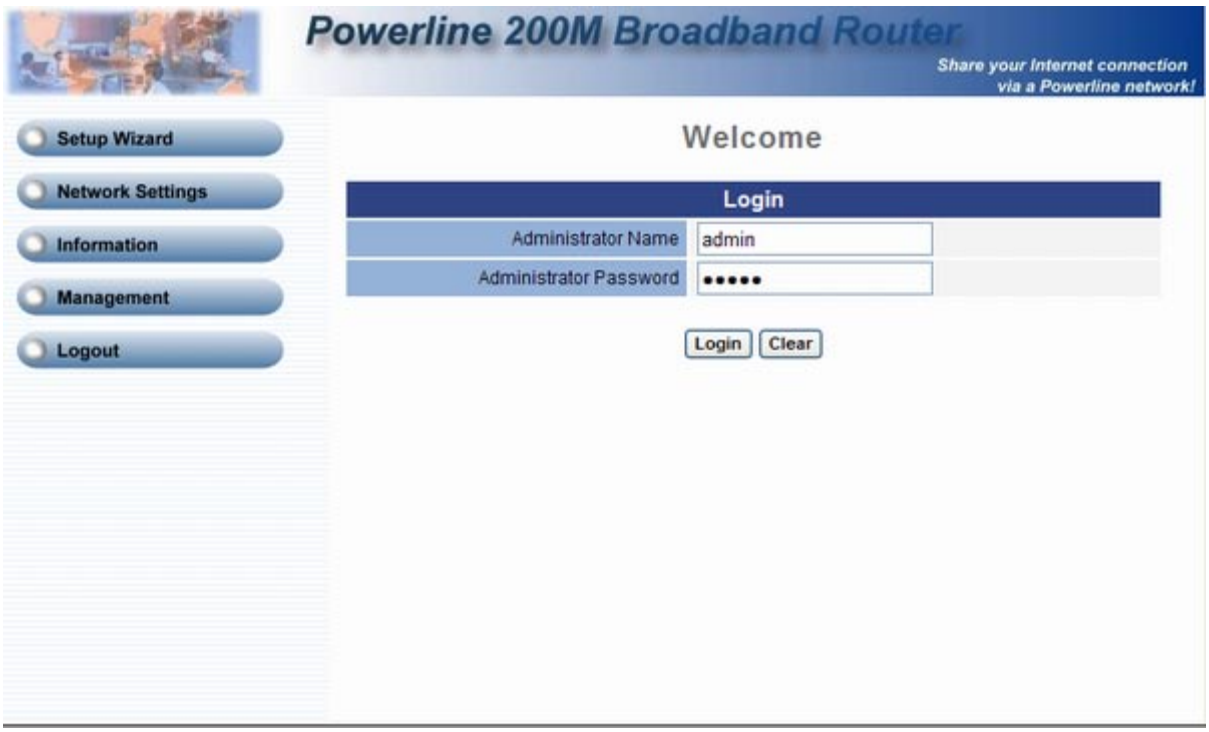
Unlike a simple hub or switch, the setup of the Powerline Router consists of more than simply plugging everything together.

Because the Router acts as a DHCP server, you will have to set some values within the Router, and also configure your networked PCs to accept the IP Addresses the Router chooses to assign them. Generally there are several different operating modes for your applications. And you can know which mode is necessary for your system from ISP. These modes are router, bridge, PPPoE+NAT.

3.3 Configuring with Web Browser

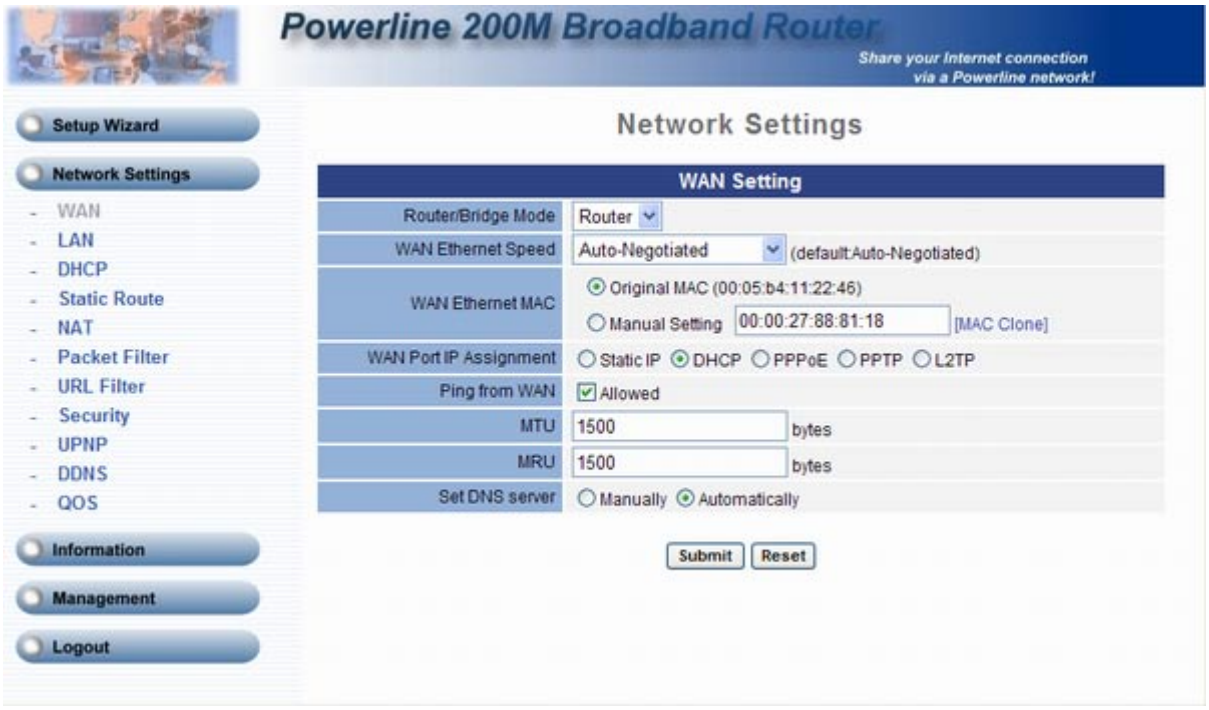
It is advisable to change the administrator password to safeguard the security of your network.

To configure the router, open your browser, type '**http://192.168.6.1**' into the address bar and click 'Go' to get to the login page. Save this address in your Favorites for future reference.



At the Password prompt, the User name is '**admin**' and the password is '**admin**'. You can change these later if you wish. Click **'Login**' to login.

3.3.1 WAN Setting



WAN Settings are settings that are used to connect to your ISP (Internet Service Provider). The WAN settings are provided to you by your ISP and often times referred to as "public settings". Please select the appropriate option for your specific ISP.

For most users, Internet access is the primary application. The router supports the WAN interface for internet access and remote access. The following sections will explain more details of WAN Port Internet access and broadband access setup. When you click “WAN Setting”, the following setup page will be shown. Three methods are available for Internet Access.

Static IP

If you are a leased line user with a fixed IP address, enter in the IP address, subnet mask, gateway address, and DNS (domain name server) address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

Example: 168.95.1.2

IP Address: Check with your ISP provider.

Subnet Mask: Check with your ISP provider.

Default Gateway: Check with your ISP provider.

DHCP

Dynamic Host Configuration Protocol (DHCP), Dynamic IP (Get WAN IP Address automatically). If you are connected to the Internet through a Cable modem line, then a dynamic IP will be assigned.

Note: WAN port gets the IP Address, Subnet Mask and default gateway IP address automatically, if DHCP client is successful.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE). Some ISPs provide DSL-based services and use PPPoE to establish communication link with end-users. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you need to make sure the following items,

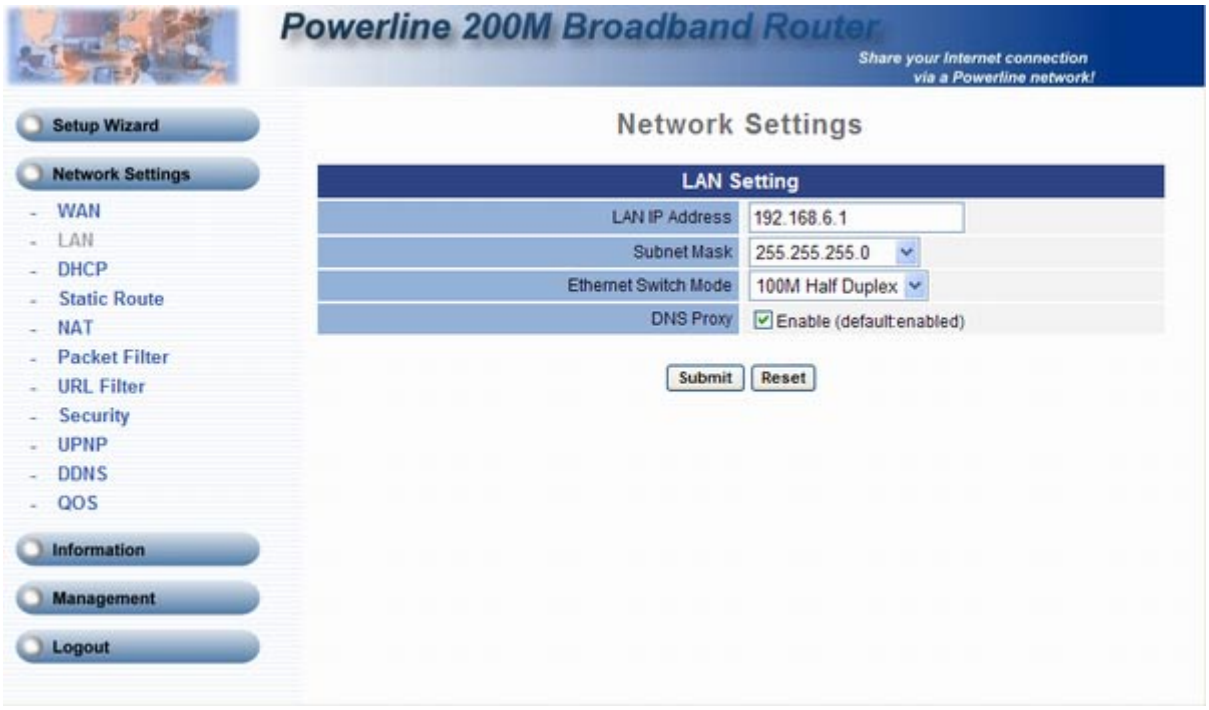
PPPoE User name: Enter username provided by your ISP.

PPPoE Password: Enter password provided by your ISP.

WAN Ethernet MAC

The MAC (Media Access Control) Address field is required by some Internet Service Providers (ISP). The default MAC address is set to the MAC address of the WAN interface in the device. It is only necessary to fill the field if required by your ISP.

3.3.2 LAN Setting



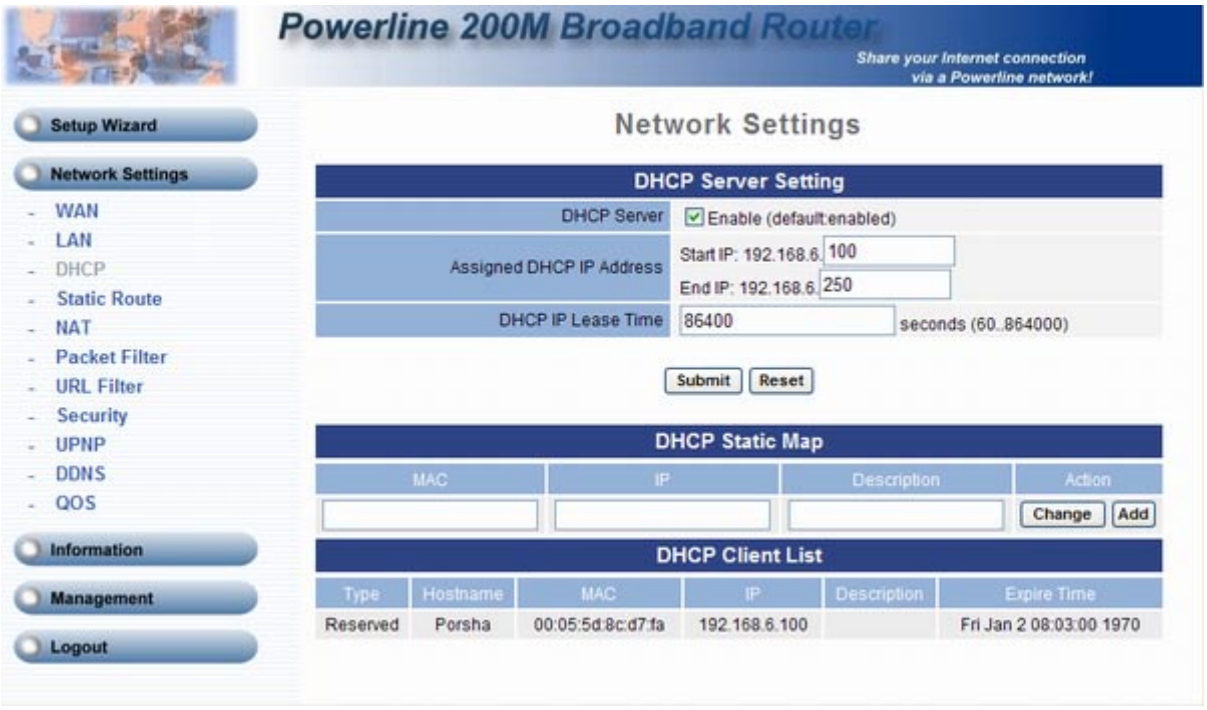
These are the IP settings of the LAN (Local Area Network) interface for the device. These settings may be referred to as "private settings". You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet. The default IP address is 192.168.6.1 with a subnet mask of 255.255.255.0

LAN is a network of computers or other devices that are in relatively close range of each other. For example, devices in a home or office building would be considered part of a local area network.

LAN IP Address: Assign the IP address of LAN server, default is 192.168.6.1

Subnet Mask: Select a subnet mask from the pull-down menu, default is 255.255.255.0

3.3.3 DHCP Setting

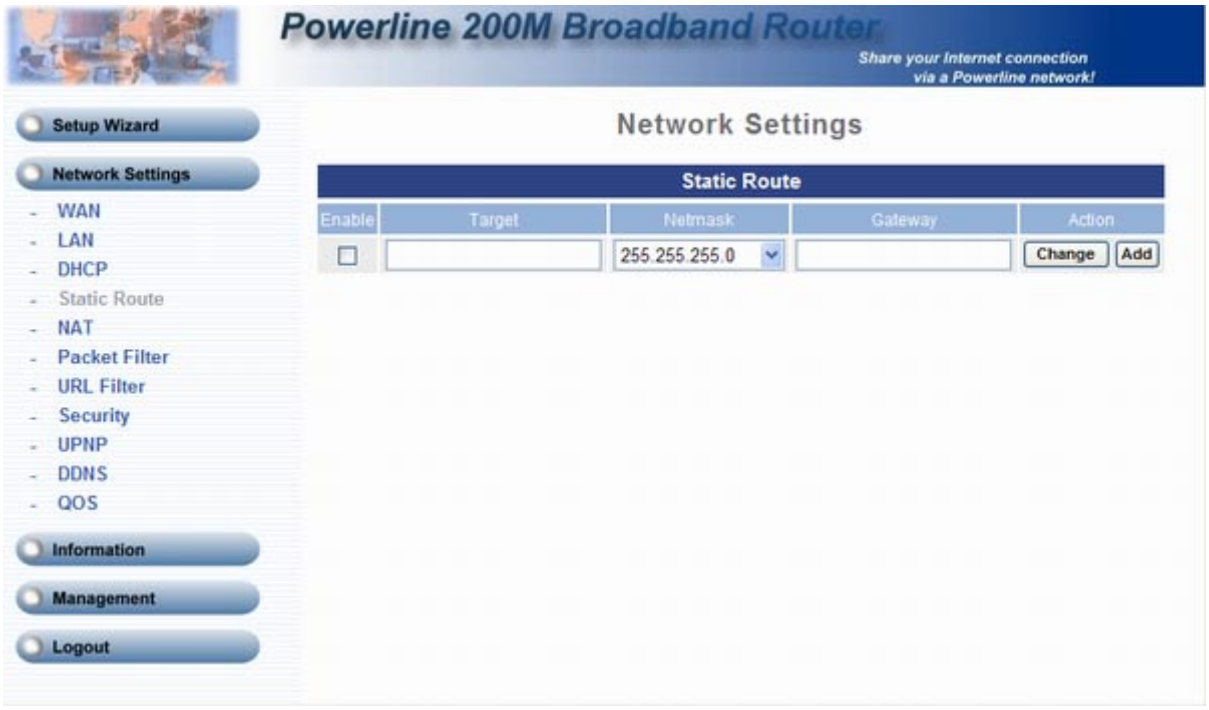


When you enable the DHCP server,

Assigned DHCP IP Address: Enter the starting IP address for the DHCP server's IP assignment and the ending IP address for the DHCP server's IP assignment.

DHCP IP Lease Time: Assign the length of time for the IP lease, default setting is 86400 seconds.

3.3.4 Static Route Setting



Static routes are special routes that the network administrator manually enters into the router configuration. You could build an entire network based on static routes. The problem with doing this is that when a network failure occurs, the static route will not change without you performing the change. This isn't a good thing if the failure occurs during the middle of the night, or while you are on vacation.

The route table allows the user to configure and define all the static routes supported by the router.

Enable: Enable/Disable the static route.

Type: Indicates the type of route as follows, Host for local connection and Net for network connection.

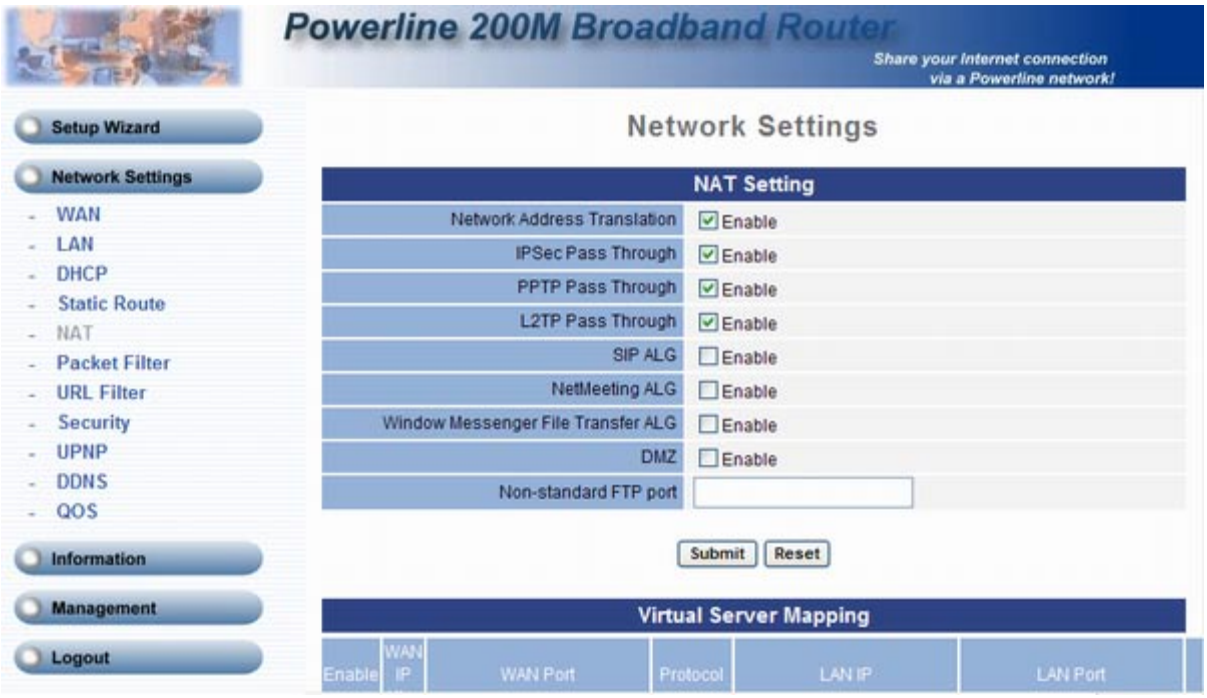
Target: Defines the base IP address (Network Number) that will be compared with the destination IP address (after an AND with NetMask) to see if this is the target route.

NetMask: The subnet mask that will be AND'd with the destination IP address and then compared with the Target to see if this is the target route.

Gateway: The IP address of the next hop router that will be used to route traffic for this route. If this route is local (defines the locally connected hosts and Type = Host) then this IP address MUST be the IP address of the router

Action: Add a new Static Route entry or update a specified entry.

3.3.5 NAT Setting



Network Address Translation: Enable/Disable NAT.

IPSec Pass Through: IPsec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication. Enable/Disable this framework verification.

PPTP Pass Through: PPTP (Point-to-Point Tunneling Protocol) is a protocol that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Enable/Disable this protocol verification.

L2TP Pass Through: L2TP (The Layer 2 Tunnel Protocol) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. Enable/Disable this function.

SIP ALG: SIP, the Session Initiation Protocol, is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. Enable/Disable this protocol verification.

NetMeeting ALG: Enable/Disable this protocol verification.

Window Messenger File Transfer ALG: Enable/Disable this protocol verification.

DMZ: In computer networks, a DMZ (Demilitarized Zone) is a computer host or small network added as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

Think of DMZ as the front yard of your house. It belongs to you and you may put some things there, but you would

put anything valuable inside the house where it can be properly secured.

Virtual Server Mapping

A Virtual Server is defined as a service port, and all requests to this port will be redirected to the computer specified by the server IP.

Enable: Enable/Disable the virtual server mapping, default setting is Disable.

WAN Port: The port number on the WAN side that will be used to access the virtual service. Enter the WAN Port number, e.g. enter 80 to represent the Web (http server), or enter 25 to represent SMTP (email server). Note: You can specify maximum 32 WAN Ports.

Protocol: The protocol used for the virtual service. Select a protocol type is TCP or UDP.

LAN IP: The server computer in the LAN network that will be providing the virtual services. Enter the IP address of LAN.

LAN Port: The port number of the service used by the Private IP computer. Enter the LAN port number.

Action: Add a new WAN port or update a specified WAN port.

Port Trigger

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol), then enter the public ports associated with the trigger port to open them for inbound traffic.

Enable: Enable/Disable the port trigger, default setting is Disable.

Trigger Port: This is the port used to trigger the application. It can be either a single port or a range of ports.

Trigger Type: This is the protocol used to trigger the special application.

Public Port: This is the port number on the WAN side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

Public Type: This is the protocol used for the special application.

Action: Add a new Port Trigger or update a specified Port Trigger.

Port Forward

Enable: Enable/Disable the port forward, default setting is Disable.

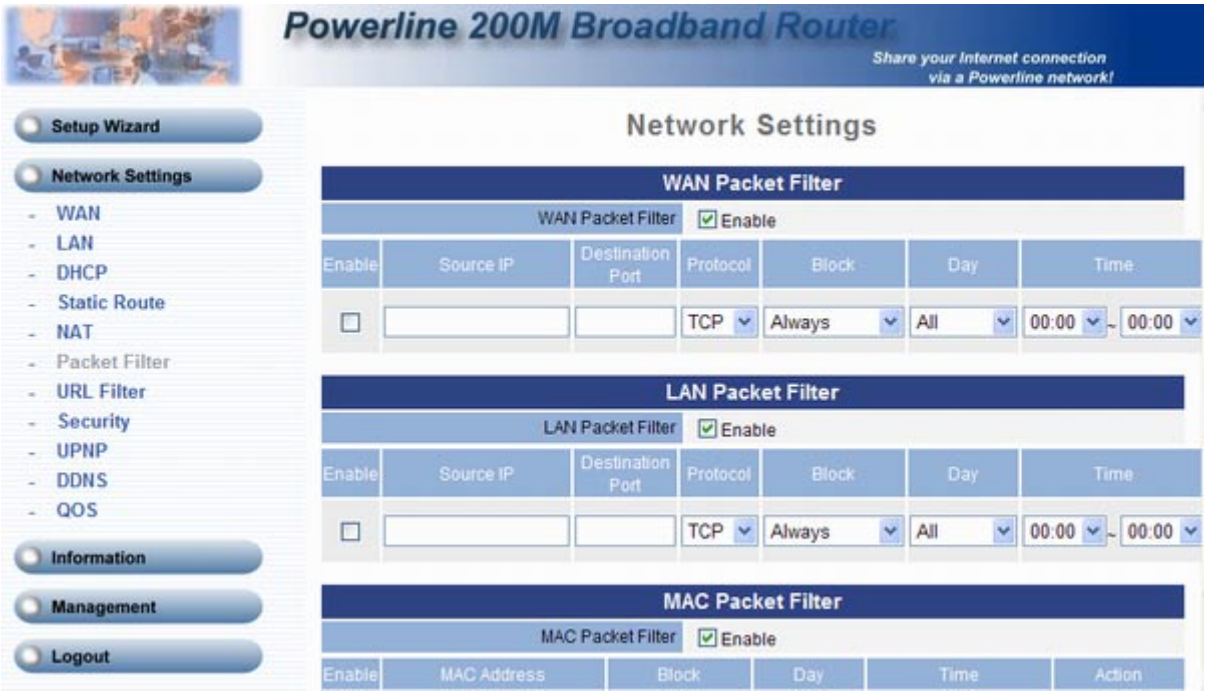
Forward Port: This is the port used to forward the application. It can be either a single port or a range of ports.

Forward Type: This is the protocol used to forward the special application.

Forward IP: This is the IP address you want to forward.

Action: Add a new Port forward or update a specified Port Forward.

3.3.6 Packet Filter Setting



WAN – Packet Filter

Use IP Filters to deny particular WAN IP addresses from the Internet. You can deny special port number or all ports for a specific IP address. You will only need to input the WAN IP address(es) of the computer(s) that will be denied.

Enable: Enable/Disable the WAN packet filter, default setting is Disable.

Source IP: The IP address of the WAN computer that will be denied access to the Internet. You can also add a range of IP addresses.

Destination Port: The single port or port range that will be denied to access. If no port is specified, all ports will be denied access.

Protocol: This is the protocol type that will be used with the Port that will be blocked.

Block: You can block the IP address of the WAN computer always or by schedule.

Day: If Block set to “by schedule”, you need to determine which day(s) will be performed.

Time: If Block set to “by schedule”, you need to determine which time will be performed.

Action: Add a new WAN packet filter or update a specified WAN packet filter.

LAN – Packet Filter

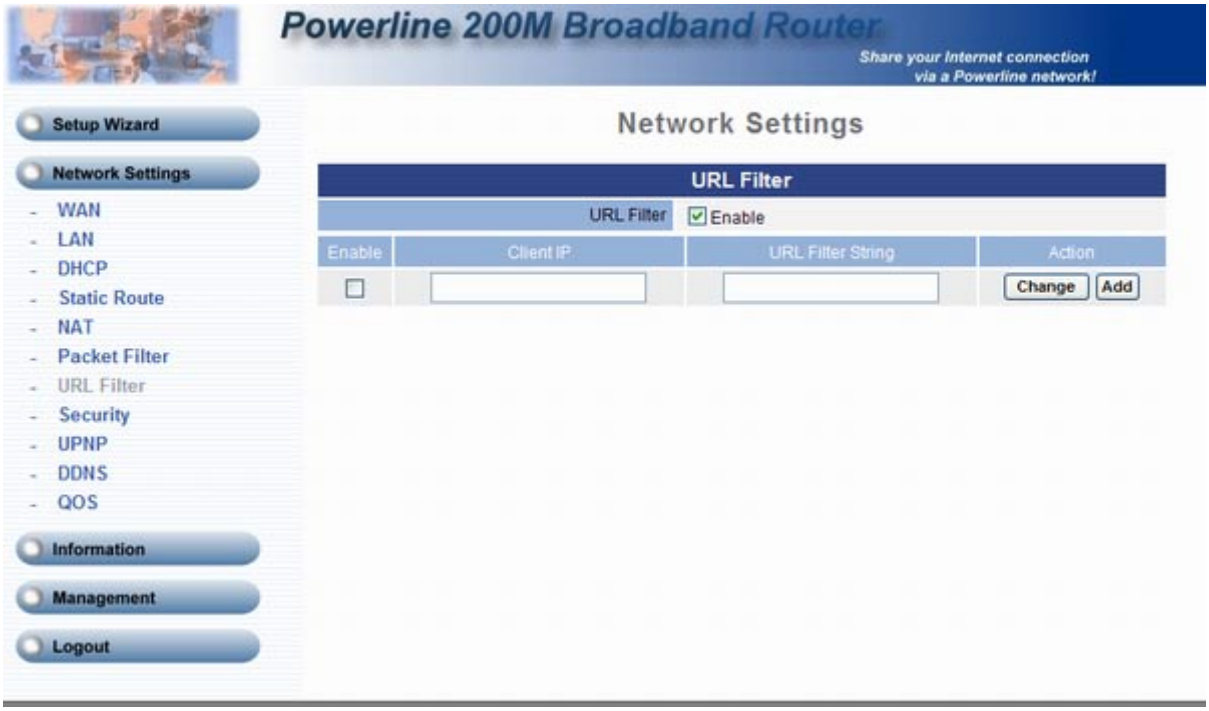
Use IP Filters to deny particular LAN IP addresses from accessing the Internet. You can deny special port number or all ports for a specific IP address. You will only need to input the LAN IP address(es) of the computer(s) that will be denied Internet access.

Enable: Enable/Disable the LAN packet filter, default setting is Disable.
Source IP: The IP address of the LAN computer that will be denied access to the Internet. You can also add a range of IP addresses.
Destination Port: The single port or port range that will be denied access to the Internet. If no port is specified, all ports will be denied access.
Protocol: This is the protocol type that will be used with the Port that will be blocked.
Block: You can block the IP address of the WAN computer always or by schedule.
Day: If Block set to “by schedule”, you need to determine which day(s) will be performed.
Time: If Block set to “by schedule”, you need to determine which time will be performed.
Action: Add a new LAN packet filter or update a specified LAN packet filter.

MAC – Packet Filter
Use MAC Filters to deny computers within the local area network from accessing the Internet. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the unit.

Enable: Enable/Disable the MAC packet filter, default setting is Disable.
MAC Address: The MAC address of the computer in the LAN (Local Area Network) to be used in the MAC filter table. Enter the MAC address of LAN port, e.g. 00:00:27:88:81:18.
Block: You can block the MAC address of the LAN computer always or by schedule.
Day: If Block set to “by schedule”, you need to determine which day(s) will be performed.
Time: If Block set to “by schedule”, you need to determine which time will be performed.
Action: Add a new MAC packet filter or update a specified MAC packet filter.

3.3.7 URL Filter Setting



With security reason, the URL Filter provides the enterprise to manage and restrict employee access to non-business or undesirable content on the Internet. URL Filter is a web solution that blocks web-sites access according the URL Filter String no matter the URL string is found full or partial matched with a keyword.
For example, if you add URL Filter String with keyword “sex”, the ATA device will limit local hosts to access the web site or web pages such as “www.sex.com” or “www.fronthost.com/sex/index.html”.

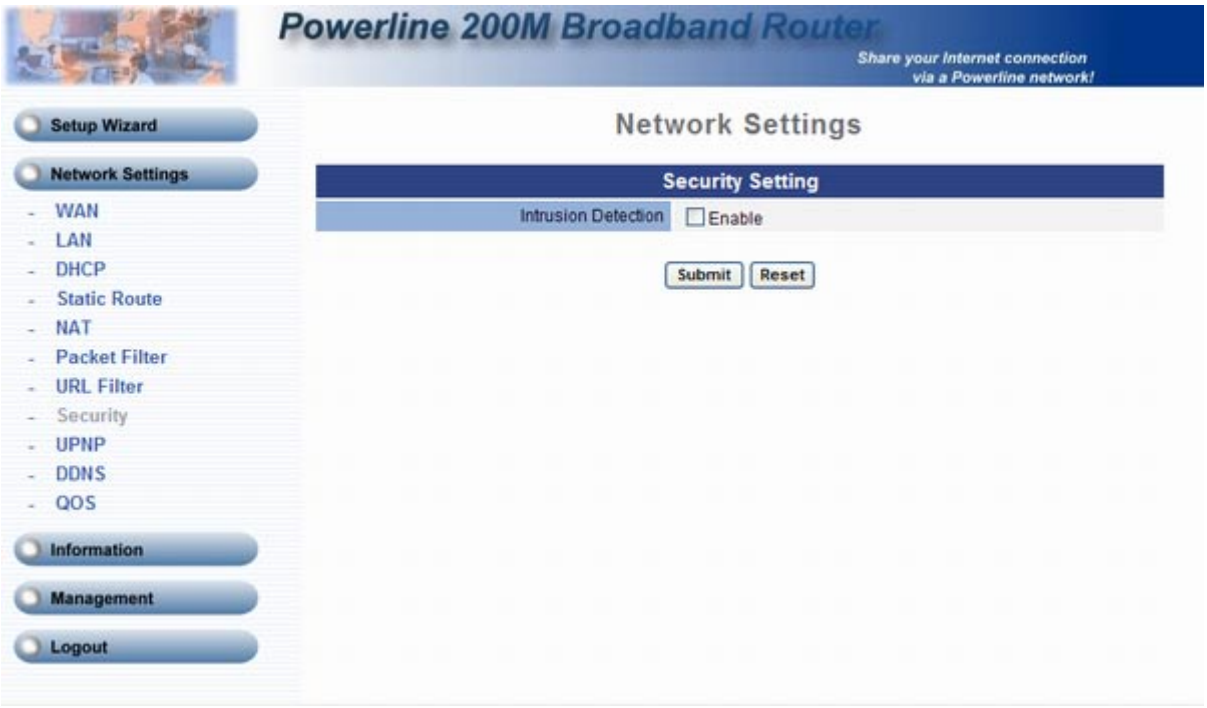
Enable: Enable/Disable the URL Filter, default setting is Disable.

Client IP: The host computer which will be blocked to access the Internet.

URL Filter String: The pattern which will be blocked. For example, “yahoo.com” or keyword “sex”.

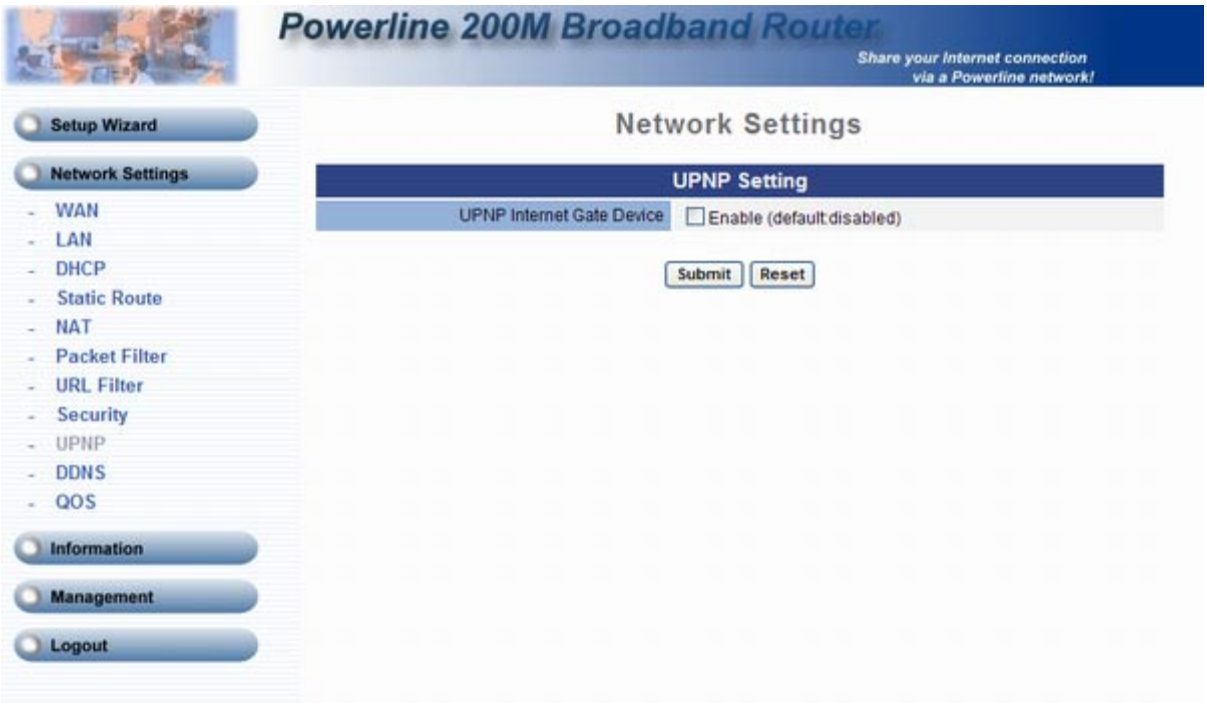
Action: Add a new URL Filter or update a specified URL Filter.

3.3.8 Security Setting



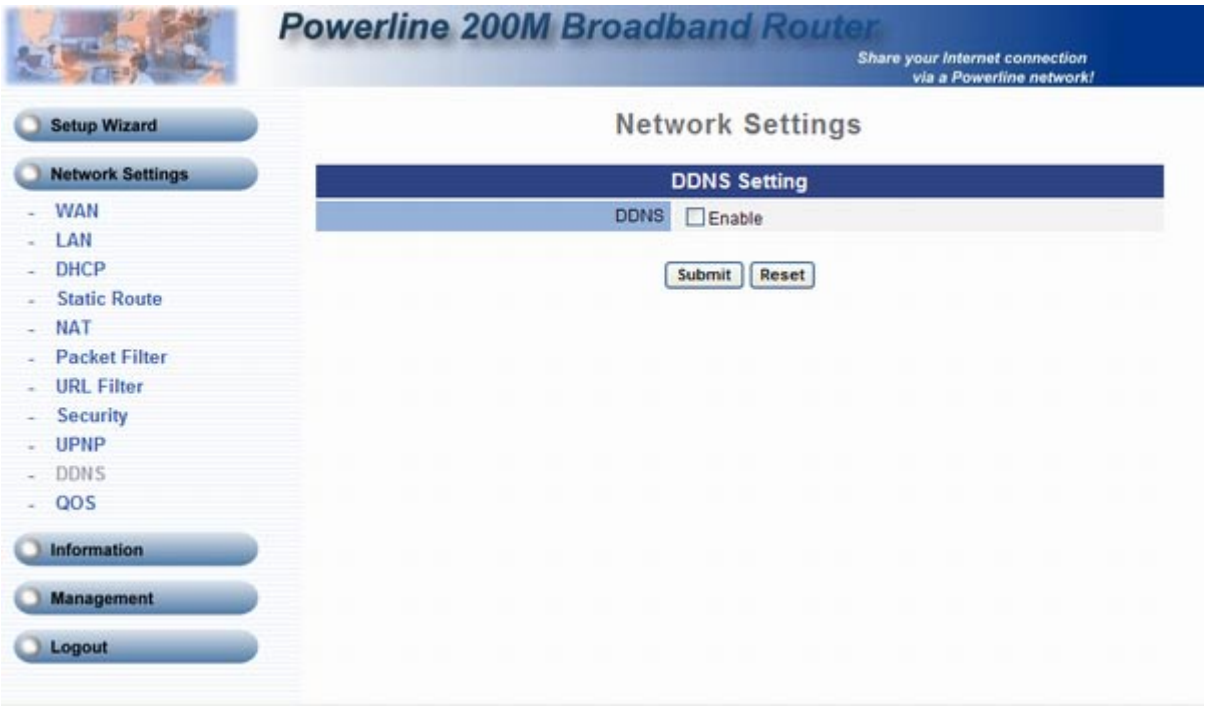
Intrusion Detection: Enable/Disable the intrusion detection.

3.3.9 UPNP Setting



UPnP (Universal Plug-and-Play). Network architecture based on TCP/IP and intended to allow terminals to be networked without the need for configuration. In the Barricade router, for example, the correct ports are automatically opened for applications like Net meeting, online games, etc. You can choose to enable or disable the UPnP Service.

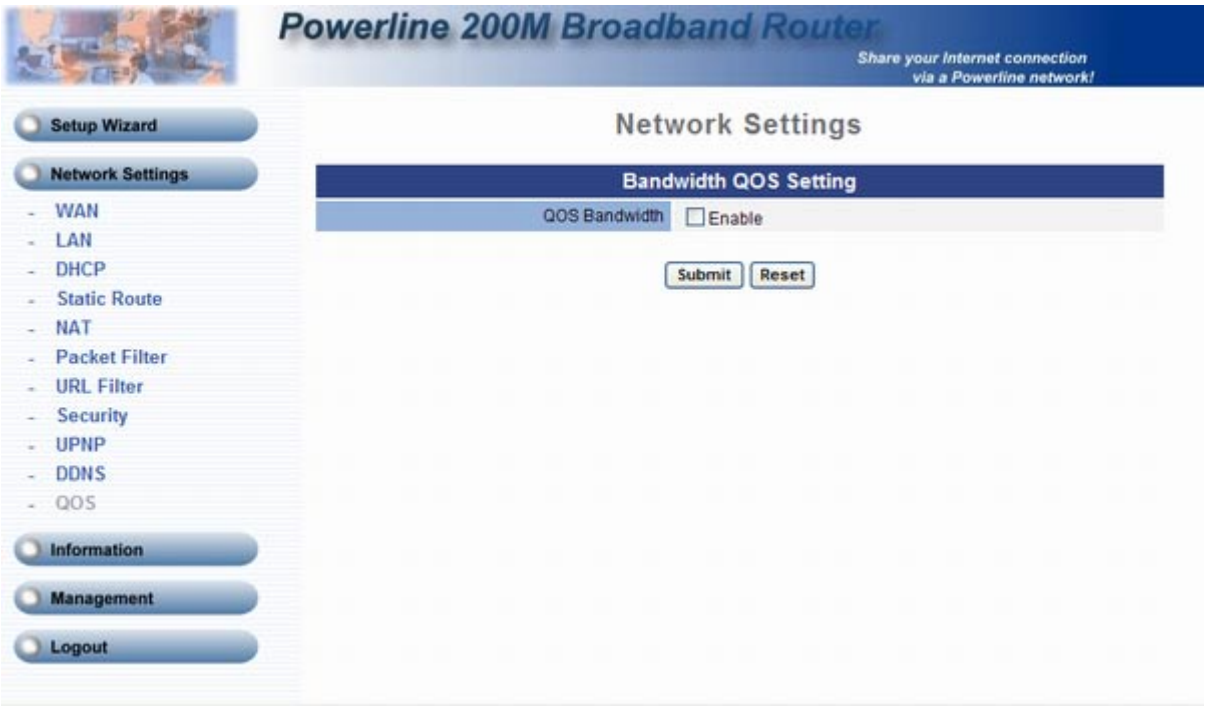
3.3.10 DDNS Setting



DDNS is a method of keeping a domain name linked to a changing (dynamic) IP address. With most Cable and DSL connections, you are assigned a dynamic IP address and that address is used only for the duration of that specific connection. User can setup your DDNS service and the device will automatically update your DDNS server every time it receives a different IP address.

Enable: Enable/Disable the DDNS service, default setting is Disable.
DDNS Server Type: The device support two types of DDNS, DynDns.org or No-IP.com
DDNS Username: The username which you register in DynDns.org or No-IP.com website.
DDNS Password: The password which you register in DynDns.org or No-IP.com website.
Confirmed Password: Confirm the password which you typing.
Hostname to register: The hostname which you register in DynDns.org or No-IP.com website.

3.3.11 QOS Setting



The QOS (Quality Of Service) is to guarantee that the Voice and Data should be transmitting at the same time and Data couldn't influence the Voice quality. When TOS bits is enabled, it will guarantee the Voice have the first priority pass through the TOS enable devices.

QOS: Enable/Disable the QOS Service. Default setting is disable.

Voice VLAN Priority: The priority value for voice packet. Default is 1.

Voice VLAN ID: The voice VLAN ID. Default is 3.

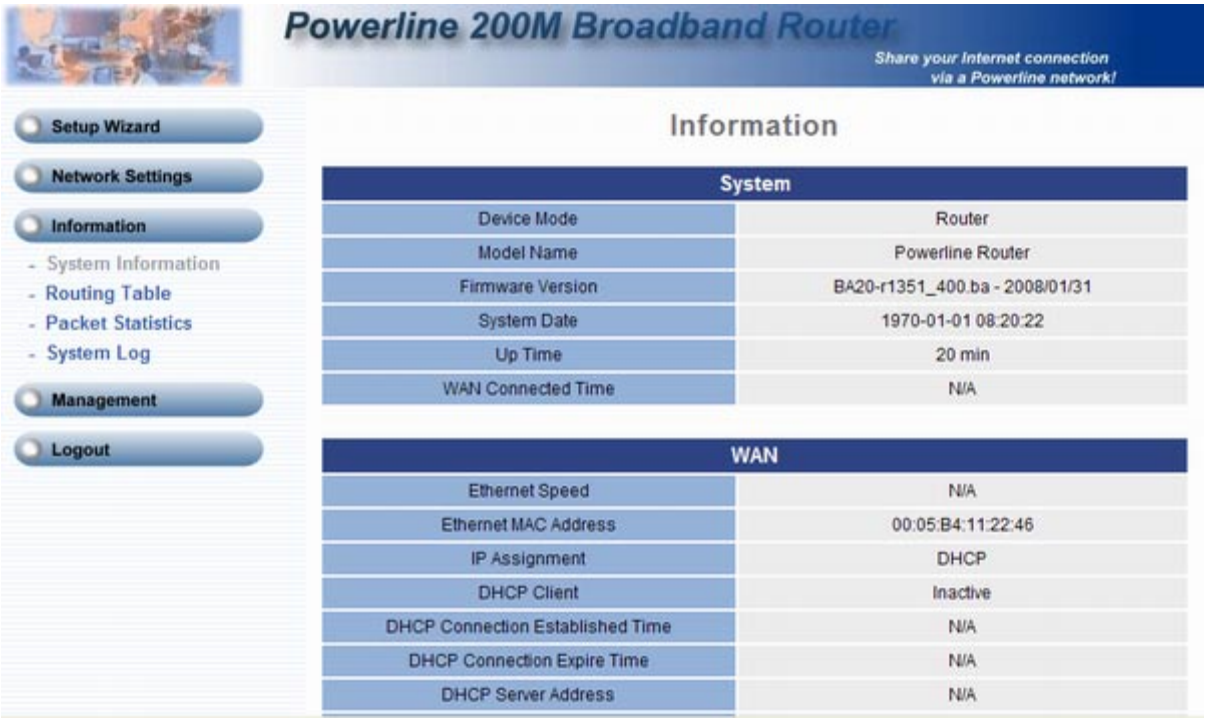
Data VLAN Priority: The priority value for data packet. Default is 0.

Data VLAN ID: The data VLAN ID. Default is 4.

SIP TOS/DiffServ: This option enables the phone to support QOS for SIP traffic in a network. This makes sense only if all parts of the involved network also support QOS. Assign the priority value from 0 to 255. Default is 0.

RTP TOS/Diffserv: This option enables the phone to support QOS for RTP traffic in a network. This makes sense only if all parts of the involved network also support QOS. Assign the priority value from 0 to 255. Default is 0.

3.4.1 System Information

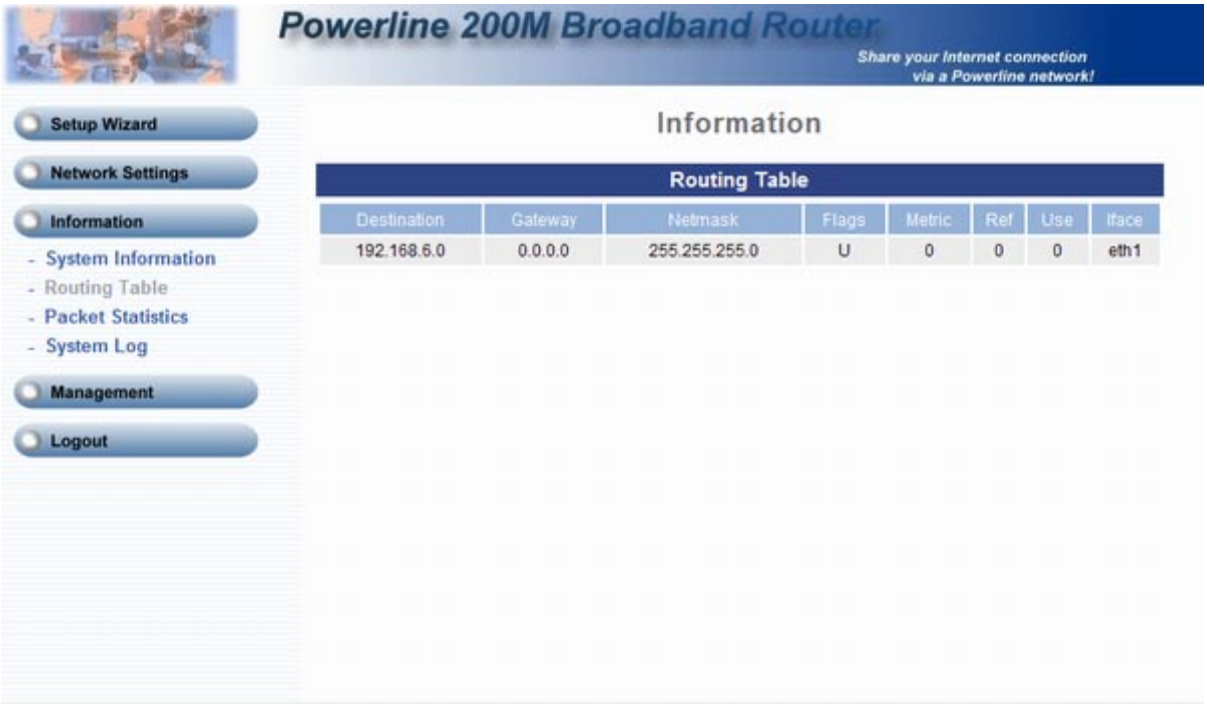


This page displays the current information for the device. It will display the LAN, WAN, and system firmware information. This page will display different information for you, according your WAN setting (Static IP, DHCP, or PPPoE).

If your WAN connection is set up for Dynamic IP address, there will be a Release button and Renew button. Use Release to disconnect from your ISP and use Renew to connect to your ISP.

If your WAN connection is set up for PPPoE, there will be a Connect button and Disconnect button. Use "Disconnect" to drop the PPPoE connection and use "Connect" to establish the PPPoE connection.

3.4.2 Routing Table



A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network.

Destination: The IP address of the packet's final destination. The destination can be an IP address or a class-based, subnetted, or supernetted network ID.

Gateway: The IP address to which the packet is forwarded.

Netmask: Includes directly-attached subnets, indirect subnets that are not attached to the device but can be accessed through one or more hops, and default routes to use for certain types of traffic or when information is lacking.

Flags: Possible flags include: **U**: route is up, **H**: target is a host, **G**: use gateway, **C**: cache entry, **!**: Reject route.

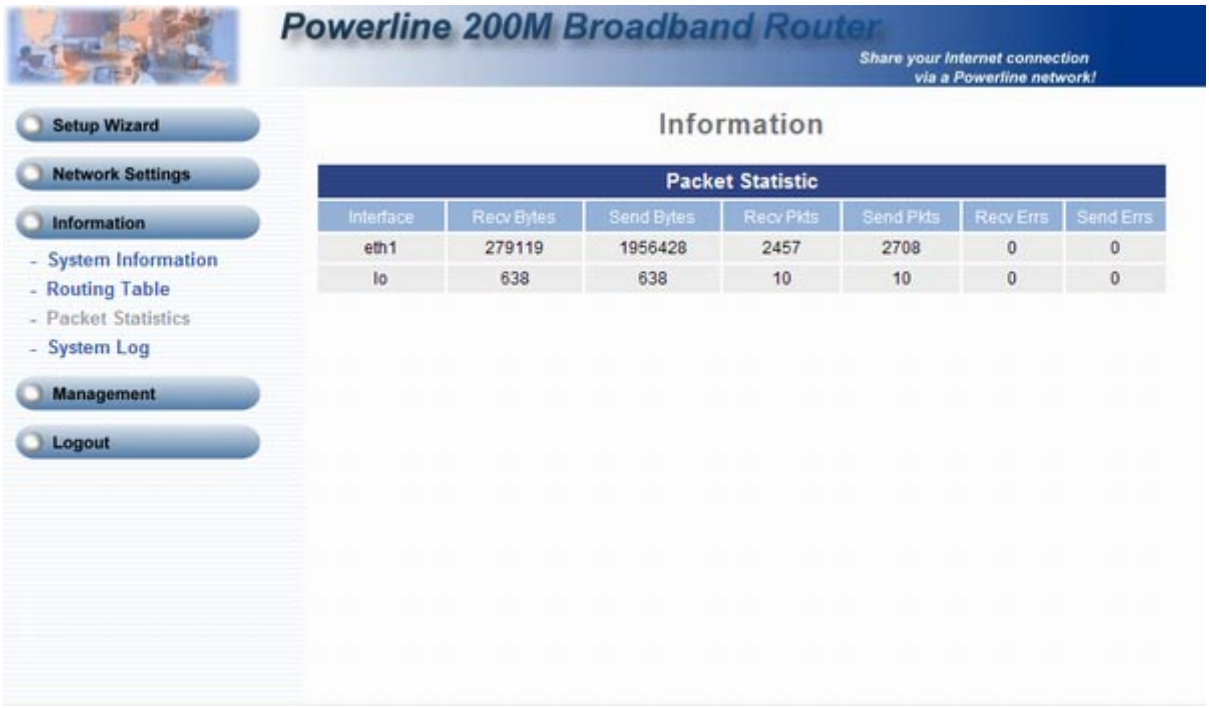
Metric: A number used to indicate the cost of the route so that the best route, among potentially multiple routes to the same destination, can be selected.

Ref: Number of references to this route.

Use: Count of lookups for the route.

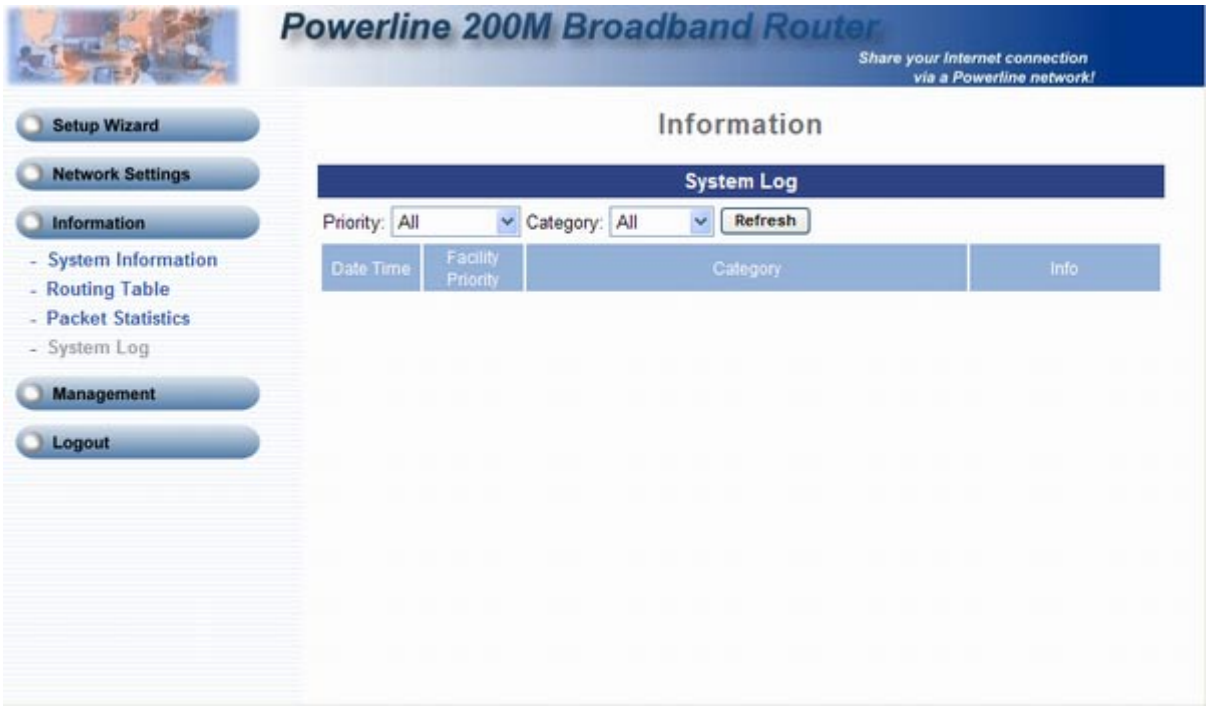
Iface: Interface to which packets for this route will be sent.

3.4.3 Packet Statistics



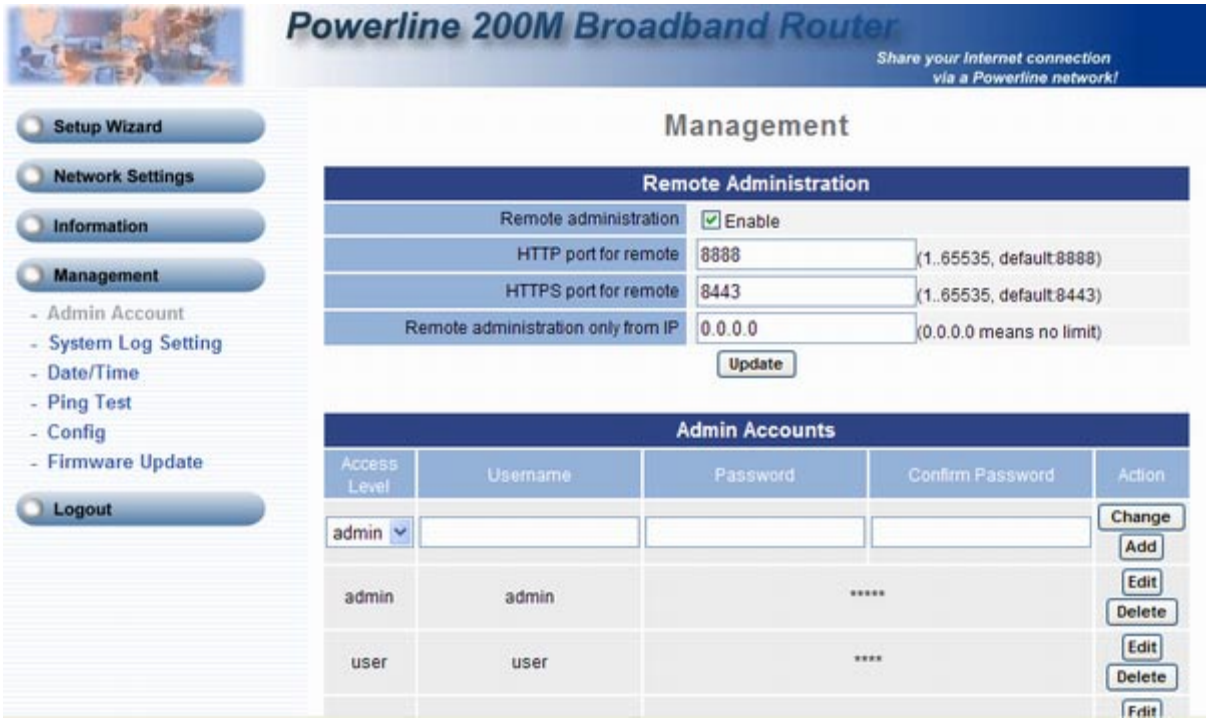
The device keeps statistic of the data traffic that it handles. You are able to view the amount of Receive and Sent packets that passes through the device on both the WAN port and the LAN ports. The traffic counter will reset when the device is rebooted.

3.4.4 System Log



The log file keeps a running log of events and activities occurring on the device. The log always displays recent logs. When the device is rebooted, the logs would not be cleared.

3.5.1 Admin Account



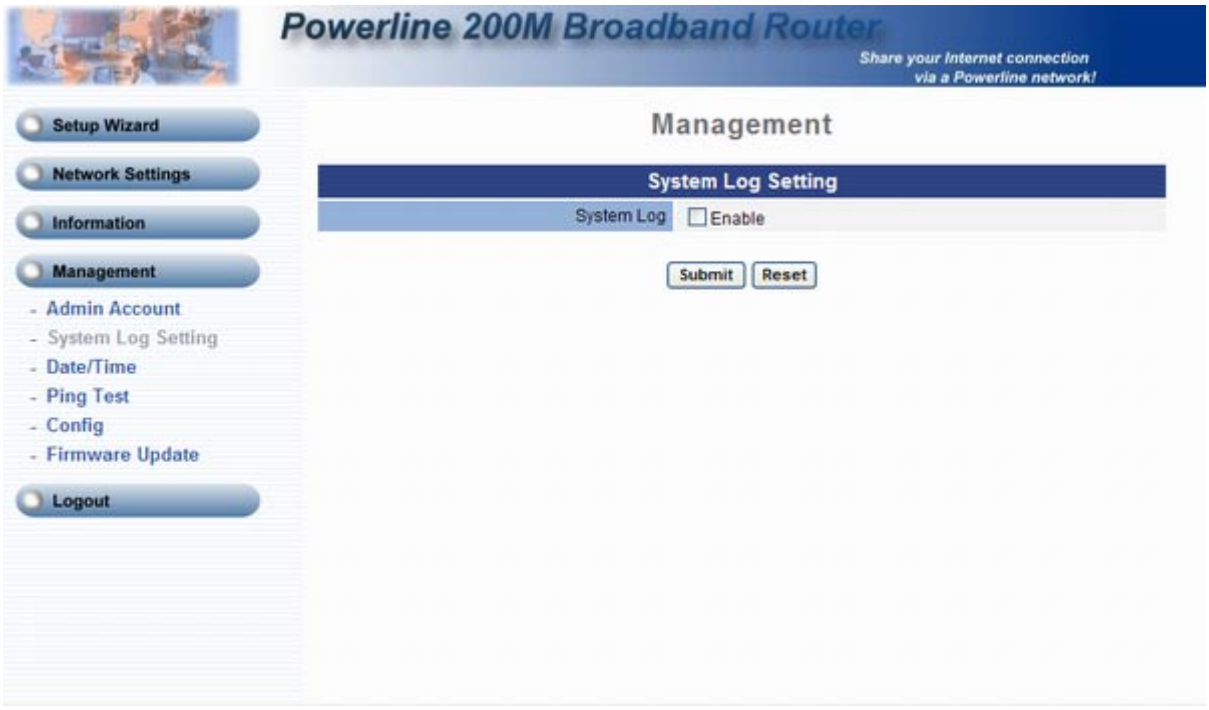
The administrator account can access the management interface through the web browser. Only the administrator account has the ability to change account password.

Administrator Name: Assign a name to represent the administrator account. Maximum 16 characters. Legal characters can be the upper letter “A” to “Z”, lower letter “a” to “z”, digit number “0” to “9” and an underscore sign” _” . The administrator name is case-sensitive. Note: the “blank” character is an illegal character

Administrator Password: Assign the administrator password, the Maximum 16 characters and minimum 6 characters. Mix the characters with the digits. Legal characters can be the upper letter “A” to “Z”, lower letter “a” to “z”, digit number “0” to “9” and an underscore sign”_”. The password is case-sensitive. Note: the “blank” character is an illegal character.

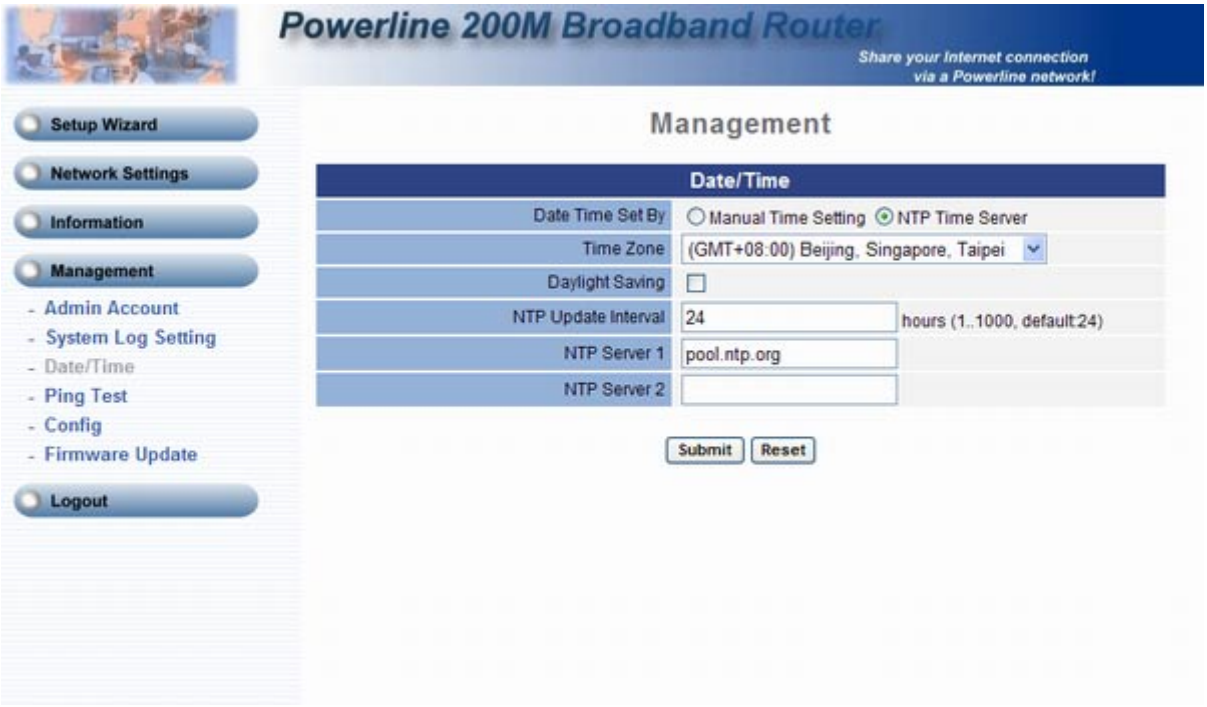
Confirm Password: Enter the administrator password again.

3.5.2 System Log Setting



The log file keeps a running log of events and activities occurring on the device. The log always displays recent logs. When the device is rebooted, the logs would not be cleared.

3.5.3 Data / Time



Date Time Set By: Manual Time Setting or NTP Time Server.

Manual Time Setting: If you choose this item, then go to the fields of Date Value Setting and Time Value Setting for setting time.

NTP Time Server: If you choose this item, then go to the filed of NTP Server Address to assign the domain name for NTP Server.

Time Zone: GMT (Greenwich Mean Time) is World Time and the basis of every world time zone which sets the time of day and is at the centre of the time zone map. GMT sets current time or official time around the globe. According to the location, select a time zone from the pull-down menu.

Daylight Saving: Daylight Saving Time begins for most of the United States at 2:00 a.m. on the first Sunday of April. Time reverts to standard time at 2:00 a.m. on the last Sunday of October. In the U.S., each time zone switches at a different time. In the European Union, Summer Time begins and ends at 1:00 a.m. GMT. It begins the last Sunday in March and ends the last Sunday in October. In the EU, all time zones change at the same moment.

Day Value Setting: Assign the day value from the pull-down menus.

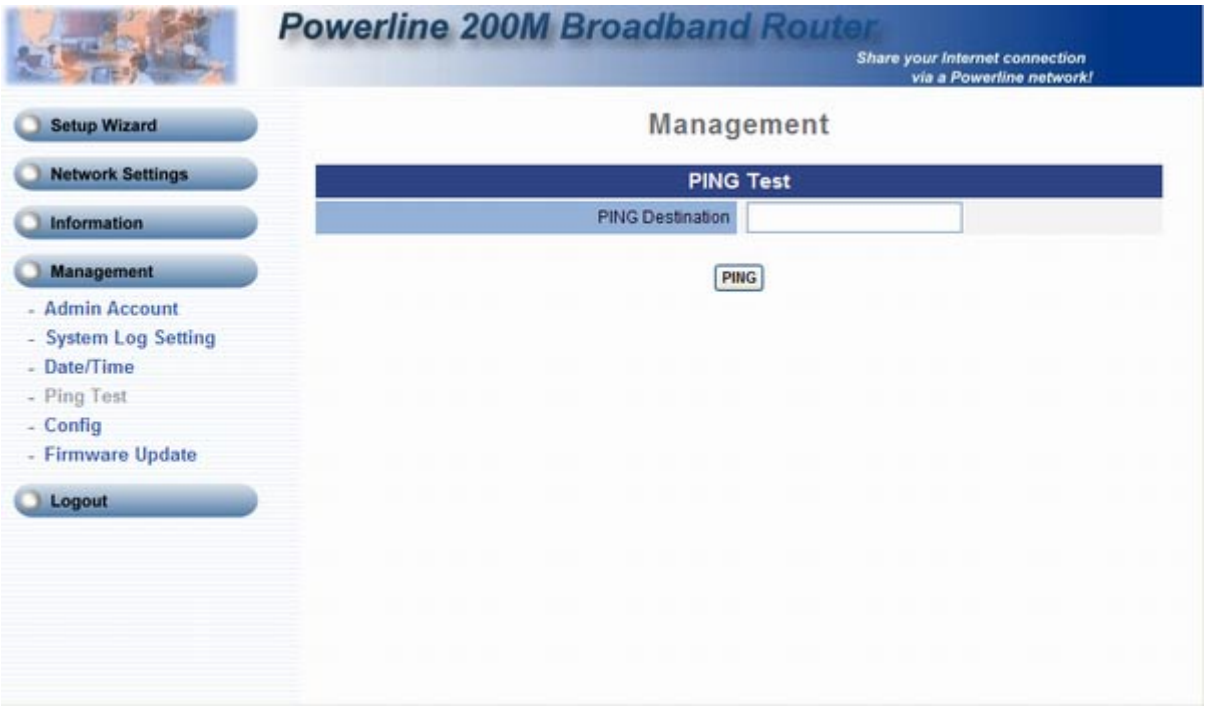
Time Value Setting: Assign the time value from the pull-down menus.

NTP Update Interval: Configure how often to updates its system clock. This setting is based on hour inside the registry. Default is 24 hours.

NTP Server 1: Assign the domain name of the NTP Server 1.

NTP Server 2: Assign the domain name of the NTP Server 2.

3.5.4 Ping Test



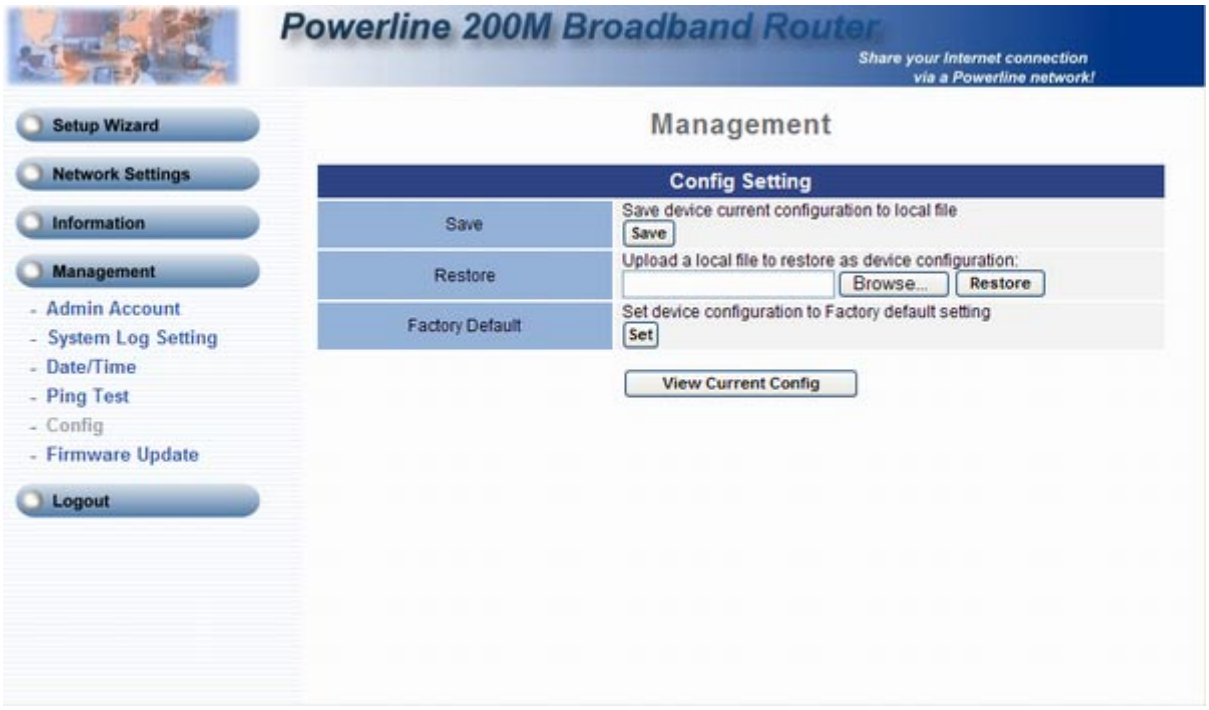
This useful diagnostic utility can be used to check if a computer is on the Internet. It sends ping packets and listens for replies from the specific host. Enter in a host name or the IP address that you want to ping (Packet Internet Groper) and click Ping.

Example:

yahoo.com or 216.115.108.245

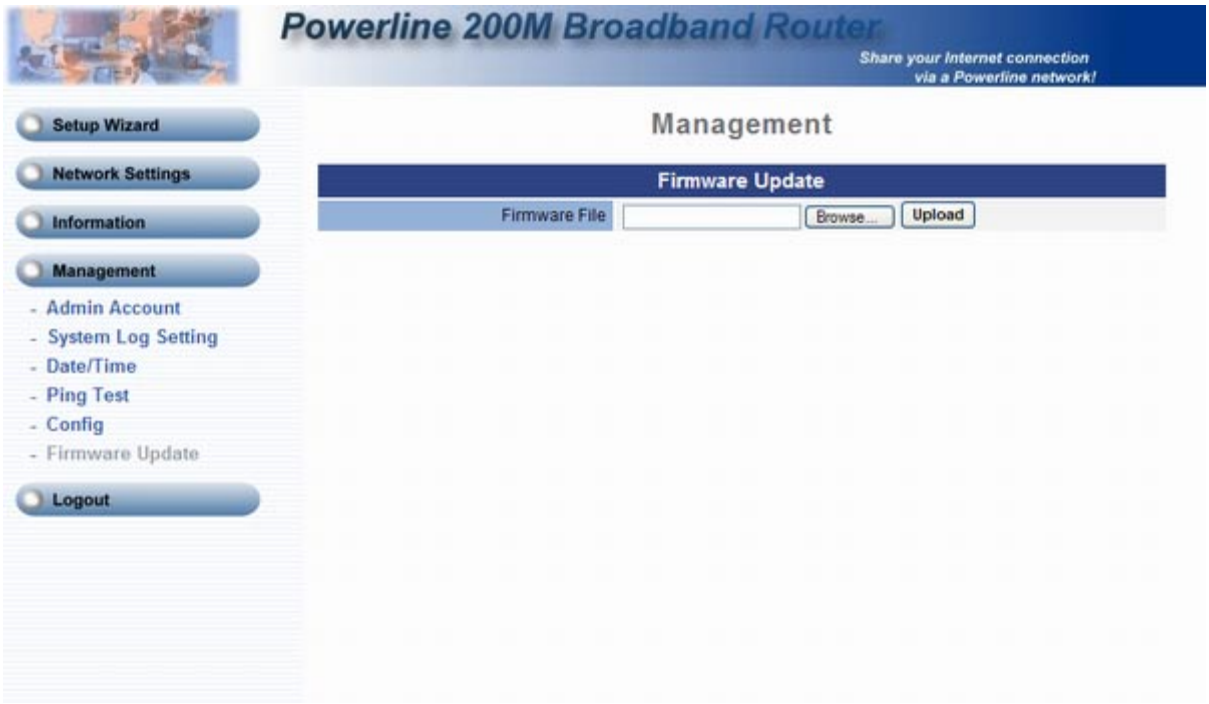
Ping Destination: Assign a legal IP address.

3.5.5 Config Setting



Save the current setting or restore a backup setting here. User can also reset the device to factory default here.

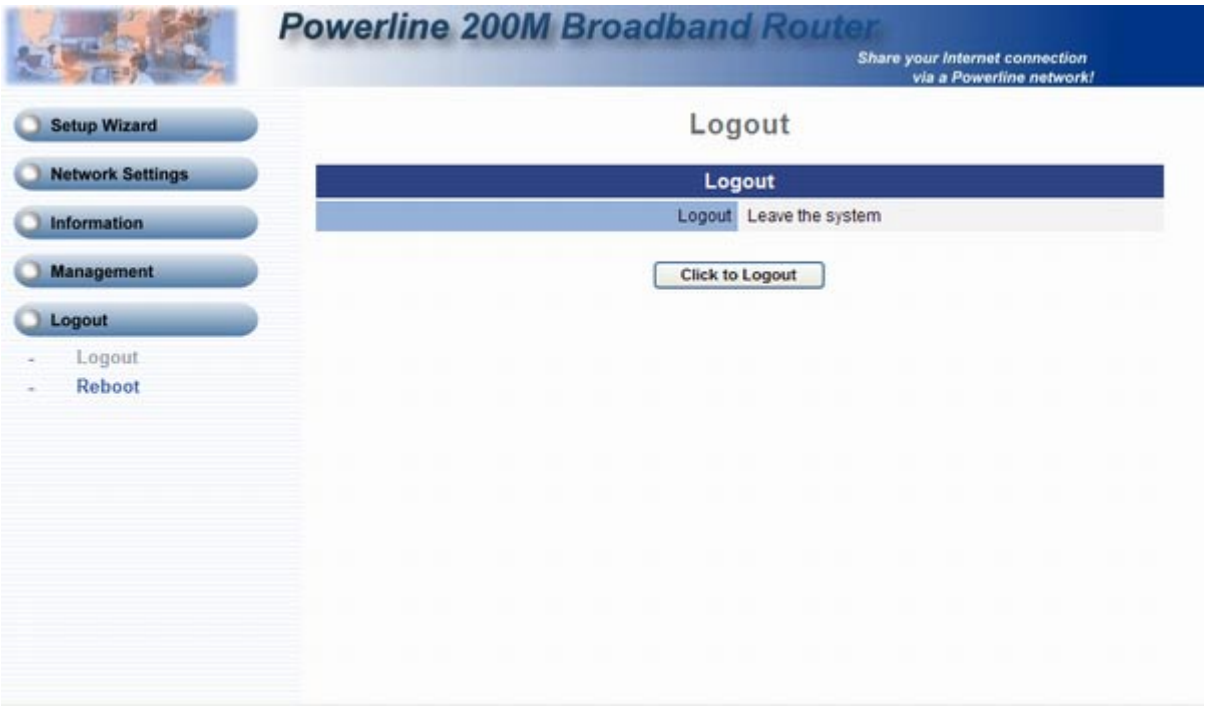
3.5.6 Firmware Update



You can upgrade the firmware of the device using this tool. Make sure that the firmware you want to use is saved on the local hard drive of the computer. Click on Browse to search the local hard drive for the firmware to be used for the update. Upgrading the firmware will not change any of your system settings but it is recommended that you save your system settings before doing a firmware upgrade.

There are two ways to update firmware.
Upload the firmware to system manually. However, for the user may not familiar with the product, recommend to enable Auto-provisioning.
Auto-provisioning mechanism is a way which can automatically check for latest firmware and then upgrade it. It enables a system to always run with a newest or stable firmware.

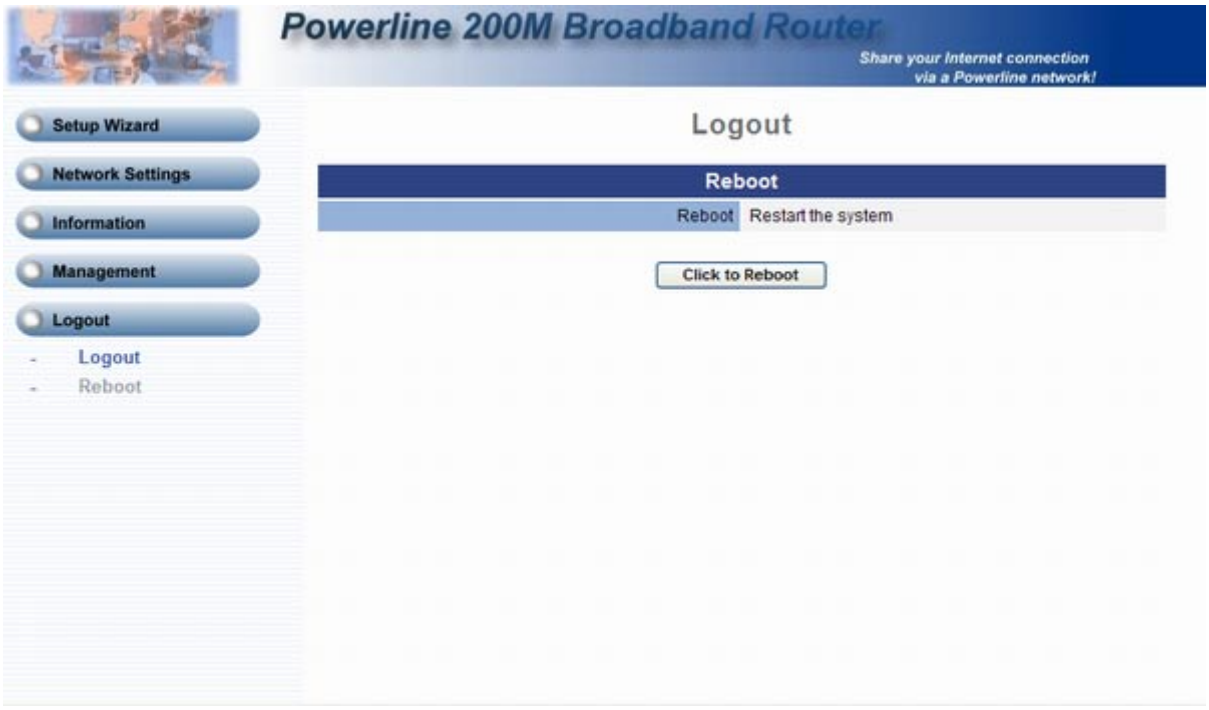
3.6.1 Logout



If you need to logout administrator right for web-access, please click the Logout link.

The web system management interface will auto–logout with 1800 sec default value.

3.6.2 Reboot

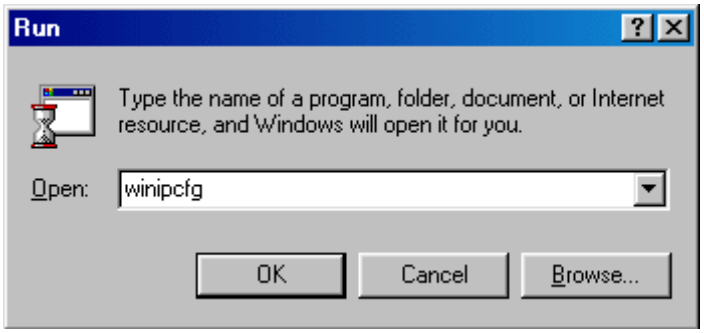


If for any reason the device is not responding correctly, you may want to reboot the system.

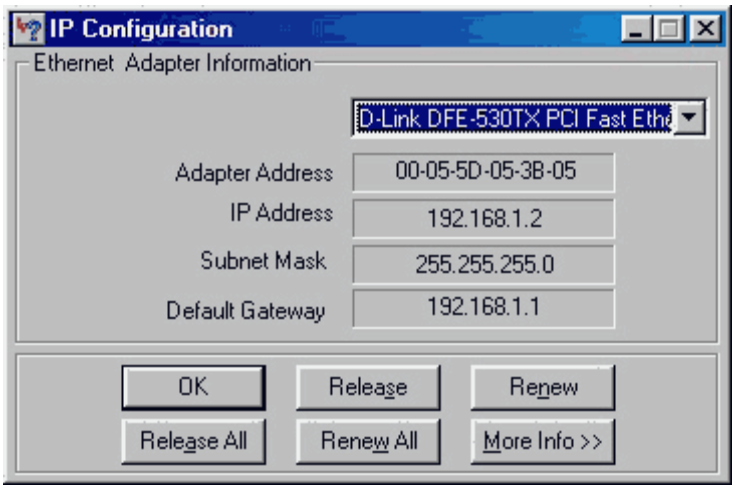
3.7.1 TCP/IP Settings for Windows Operating System

1. How can I find my IP Address in Windows 95, 98, or Me?

- Click on **Start**, then click on **Run**.
- The Run Dialogue Box will appear. Type **winipcfg** in the window as shown then click OK



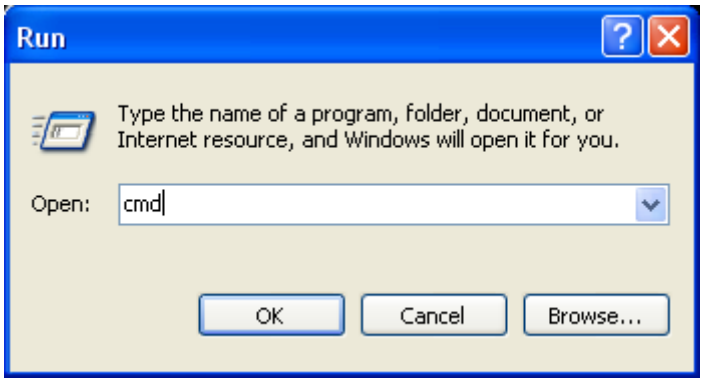
- The **IP Configuration** window will appear, displaying your **Ethernet Adapter Information**.
- Select your adapter from the drop down menu.
- If you do not see your adapter in the drop down menu, your adapter is not properly installed.



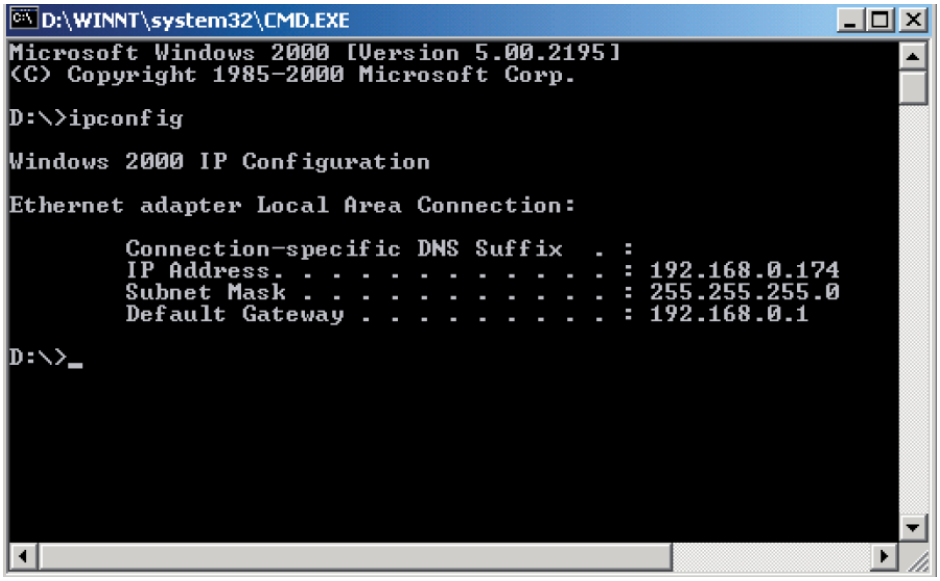
- After selecting your adapter, it will display your IP Address, subnet mask, and default router.
- Click **OK** to close the IP Configuration window.

2. How can I find my IP Address in Windows 2000/XP?

- Click on **Start** and select **Run**.
- Type **cmd** then click **OK**.



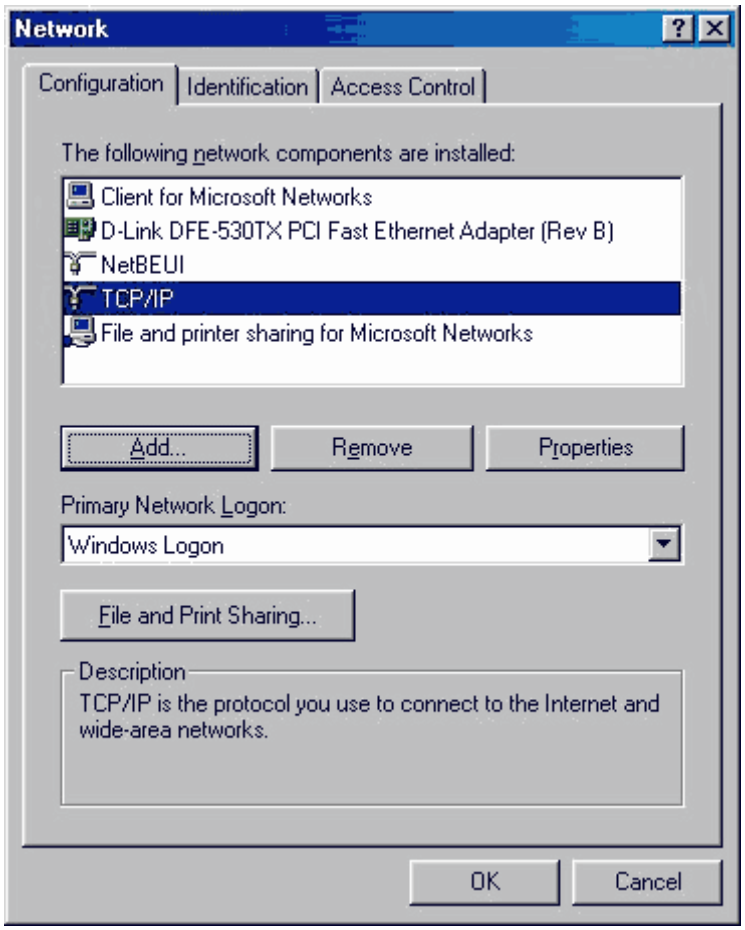
- From the Command Prompt, enter **ipconfig**. It will return your IP Address, subnet mask, and default router.



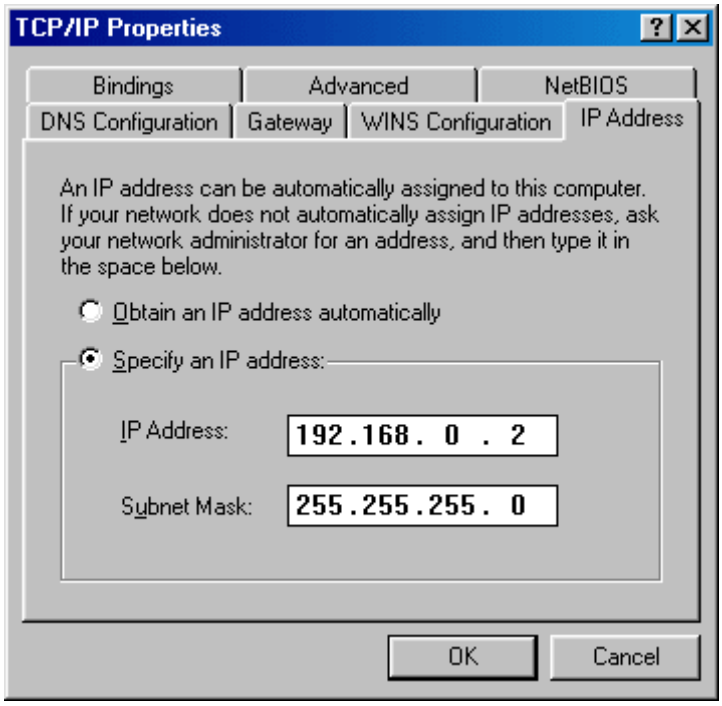
- Type exit to close the command prompt.
- Make sure you take note of your computer´s Default Router IP Address. The Default Router is the IP Address of the router. By default, it should be 192.168.0.1

3. How can I assign a Static IP Address in Windows 98/Me?

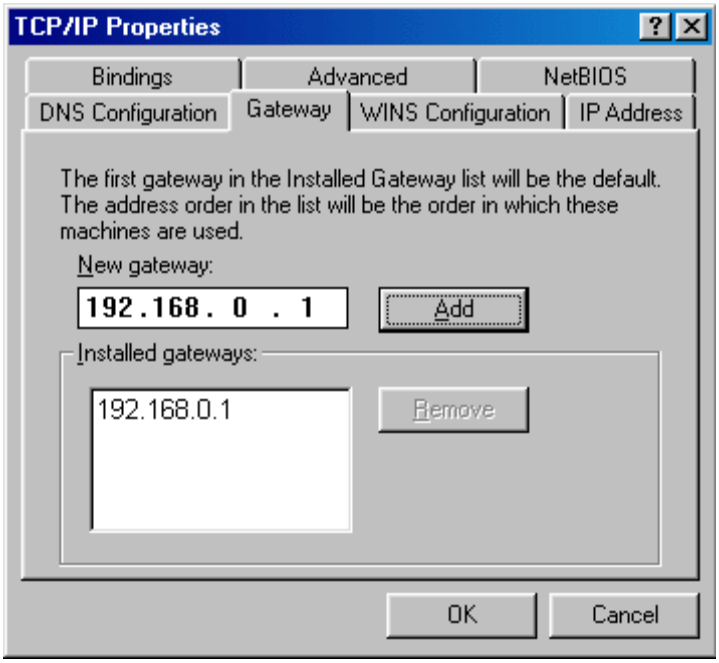
- From the desktop, right-click on the **Network Neighborhood** icon (Win ME - My Network Places) and select **Properties**.
- Highlight **TCP/IP** and click the **Properties** button. If you have more than 1 adapter, then there will be a TCP/IP "Binding" for each adapter. Highlight **TCP/IP > (your network adapter)** and then click **Properties**.



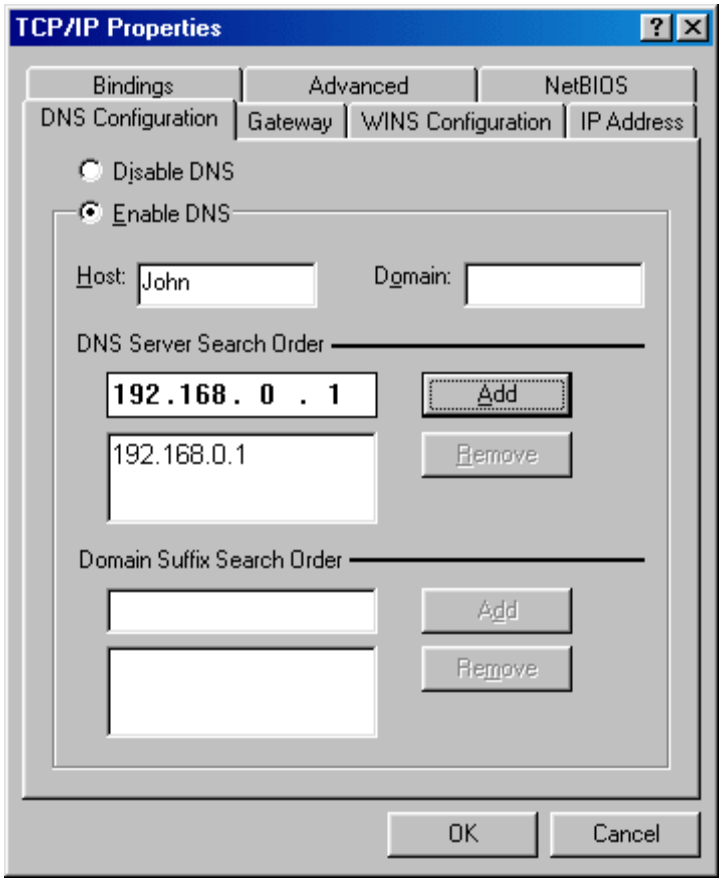
- Click **Specify an IP Address**.
- Enter in an IP Address that is on the same subnet as the LAN IP Address on your router. Example: If the router´s LAN IP Address is 192.168.0.1, make your IP Address 192.168.0.X where X is between 2-99. Make sure that the number you choose is not in use on the network.



- Click on the **Router** tab.
- Enter the LAN IP Address of your router here (192.168.0.1).
- Click **Add** when finished.



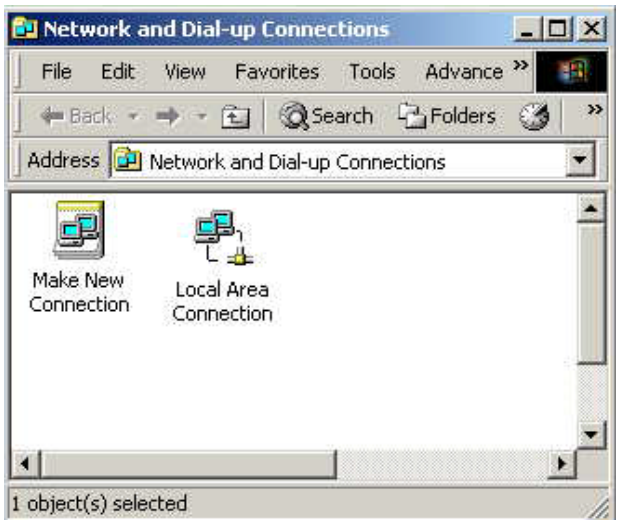
- Click on the **DNS Configuration** tab.
- Click **Enable DNS**. Type in a **Host** (can be any word). Under DNS server search order, enter the LAN IP Address of your router (192.168.0.1). Click **Add**.



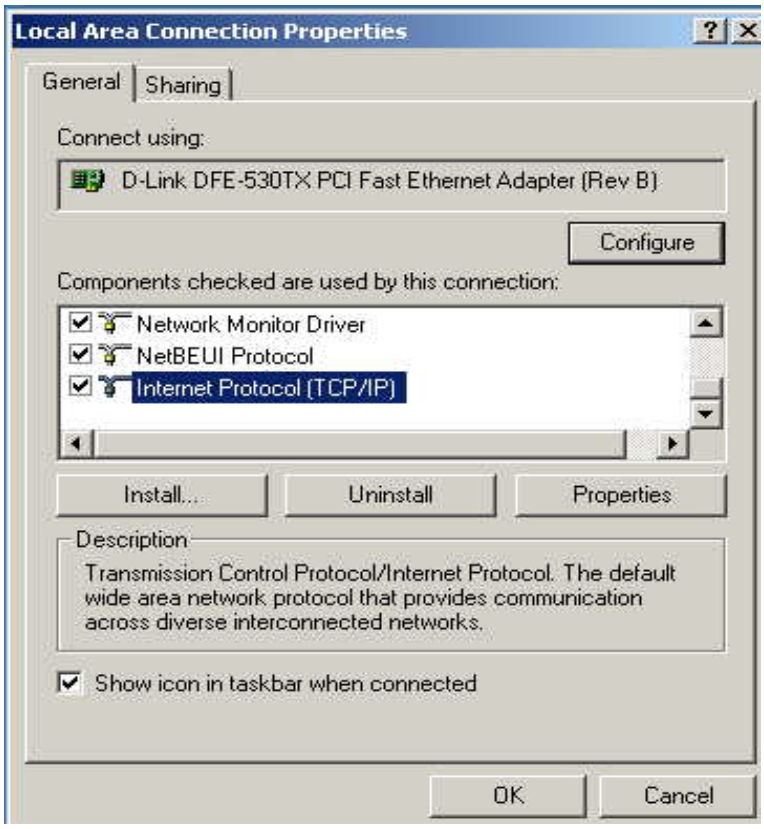
- Click **OK** twice.
- When prompted to reboot your computer, click **Yes**. After you reboot, the computer will now have a static, private IP Address.

4. How can I assign a Static IP Address in Windows 2000?

- Right-click on **My Network Places** and select **Properties**.
- Right-click on the **Local Area Connection** which represents your network card and select **Properties**.



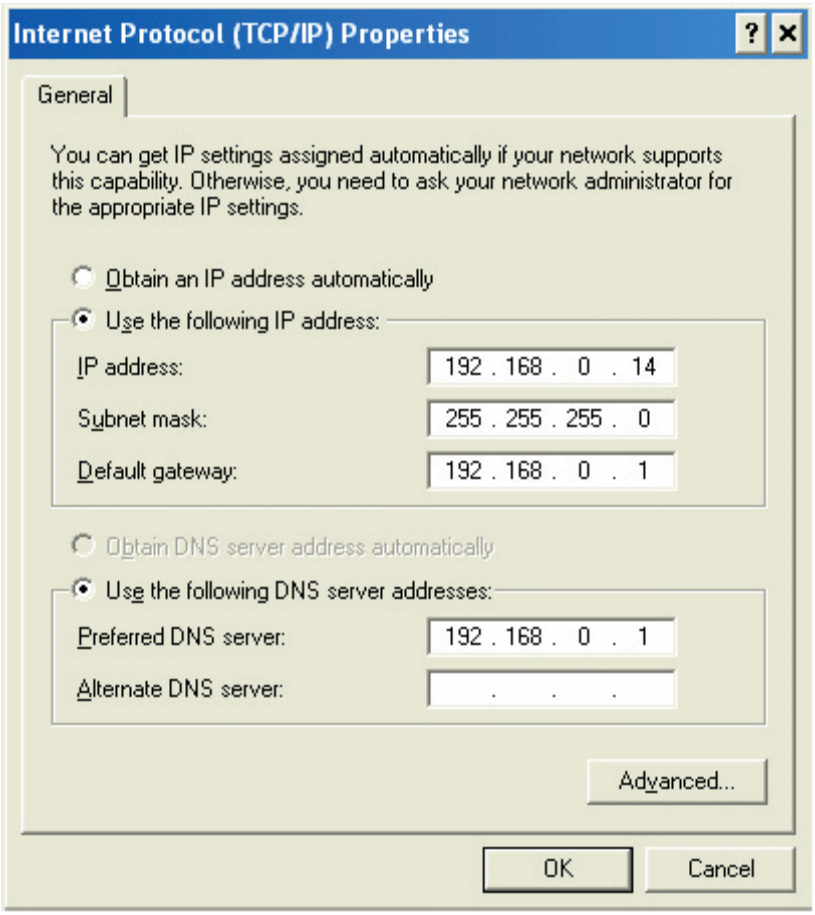
- Highlight **Internet Protocol (TCP/IP)** and click **Properties**.



- Click **Use the following IP Address** and enter an IP Address that is on the same subnet as the LAN IP Address on your router. Example: If the router´s LAN IP Address is 192.168.0.1, make your IP Address 192.168.0.X where X = 2-99. Make sure that the number you choose is not in use on the network.
- Set the **Default Router** to be the same as the LAN IP Address of your router (192.168.0.1).
- Set the **Primary DNS** to be the same as the LAN IP address of your router (192.168.0.1).
- **The Secondary DNS** is not needed or enter a DNS server from your ISP.
- Click **OK** twice. You may be asked if you want to reboot your computer. Click **Yes**.

5. How can I assign a Static IP Address in Windows XP?

- Click on **Start > Control Panel > Network and Internet Connections > Network connections**.
- See the steps for assigning a static IP address in Windows 2000 and continue from there.



- Access the Web management. Open your Web browser and enter the IP Address of your router device in the address bar. This should open the login page for the Web management. Follow instructions to login and complete the configuration.

Chapter 4. Powerline Networking Utility

Note. The Powerline Device can auto detect the other powerline bridges which plug in the same power circuit, you don't need to use this powerline utility except you want to encryption all the powerline devices as the same group or you can not access the other computers.

Introduction of Configuration Utility

The Configuration Utility for Windows OS enables the user to find Powerline Ethernet devices on the Powerline network; measures data rate performance, ensures privacy, performs diagnostics and secures Powerline networks.

Before install the utility, please check the windows edition of your computer. For vista 64, it need to install the vista 64 utility, you can easy to see it in the CD auto run screen. Please use the correct utility to install; otherwise it can not work properly.

4.1 Configuration Utility Setup

4.1.1 Installation of the Utility

Please verify that no other Powerline Management Utilities are installed before installing this product. If other utilities are installed, uninstall them and restart before installing this software.

To install, insert the Windows OS Configuration Utility Setup utility CD-ROM into the computer's CD-ROM drive. The Setup utility shall run automatically. Choose the correct one utility to install or user can manually install by double clicking the setup.exe file when browse the folder. The CD will launch an installation utility similar to the one shown in *Figure 1*.

This Utility is designed for Powerline 85M/200M Ethernet bridges. Click the **Next** button to continue.

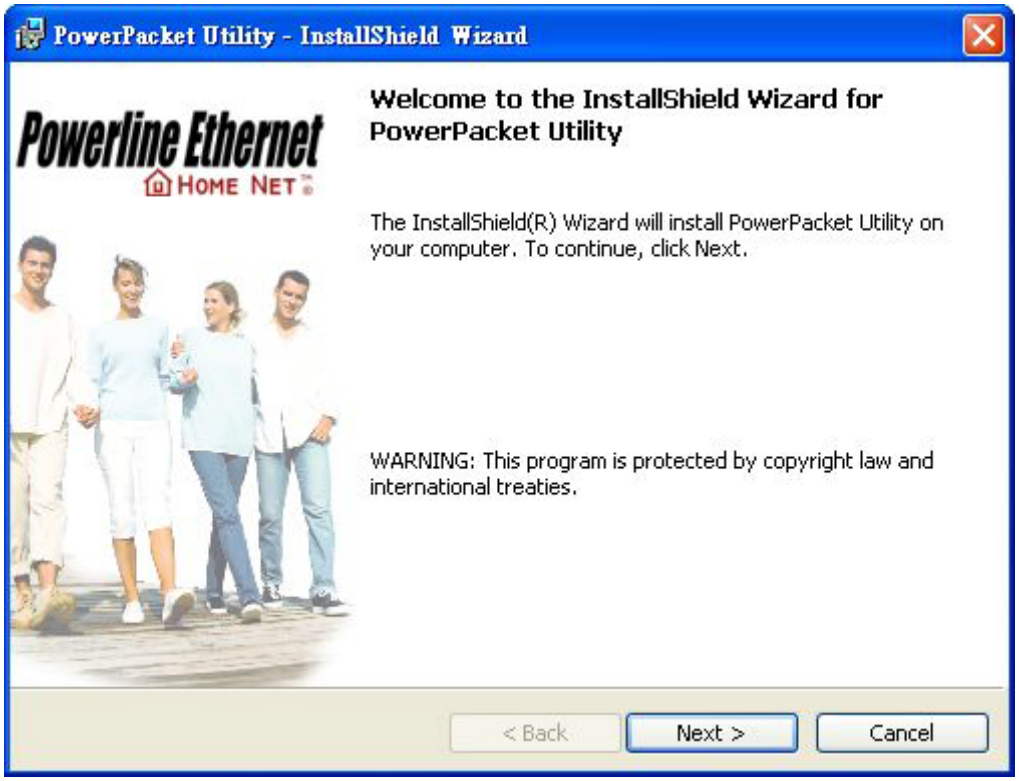


Figure 1: Install Shield Screen

4.2 Windows Configuration Utility

In order to run the utility, double-click the utility icon. *Figure 2* shows the main screen of the configuration utility. This screen shot shows a Powerline Ethernet device connected as a local device and other Powerline Ethernet devices as remote devices.

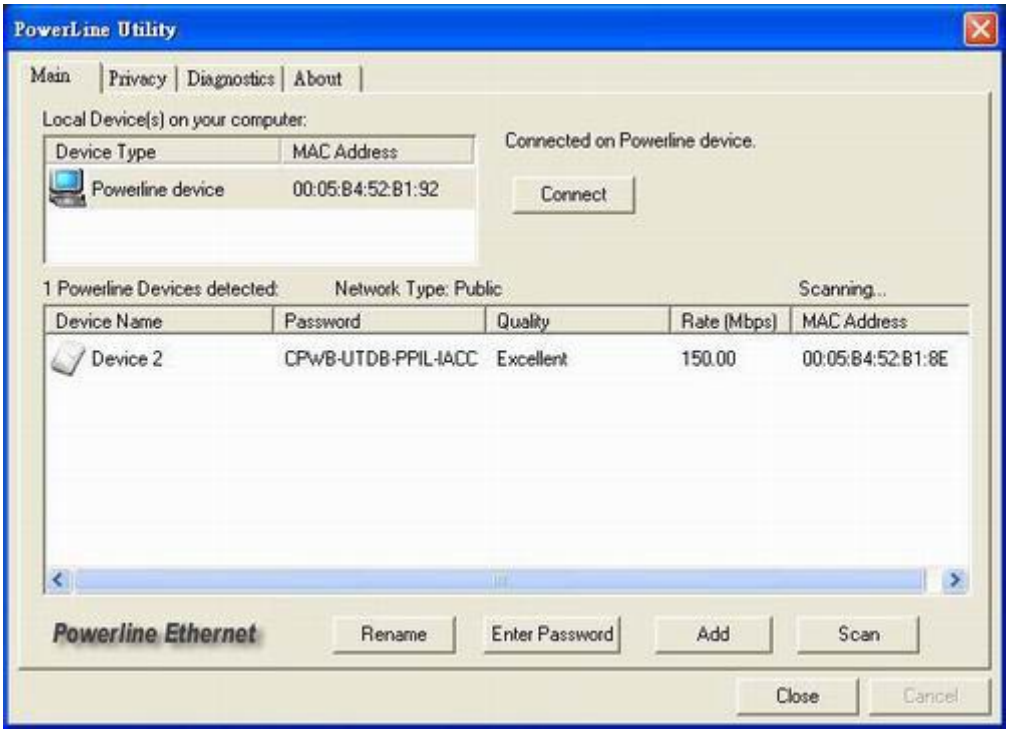


Figure 2: Main Screen with High-Speed Powerline Ethernet device Local

4.3 User Interface

4.3.1 Main Screen

The **Main** screen essentially provides a list of all Powerline Ethernet devices logically connected to the computer where the utility is running.

The top panel shows all local Powerline Ethernet devices found connected to the computer's NIC (Network Interface Card). In most cases, only one device will be seen. In situations where there are more than one device connected, such as a USB and also an Ethernet device, the user may click to select the one to manage through and then click the **Connect** button to its right. The status area above the button indicates that your PC is connected to that same device. Once connected to the chosen local device, the utility will automatically scan the powerline periodically for any other Powerline Ethernet devices. If no local Powerline Ethernet devices are discovered, the status area above the connect button will indicate that accordingly.

Figure 3 illustrates the presence of two local devices in the computer.

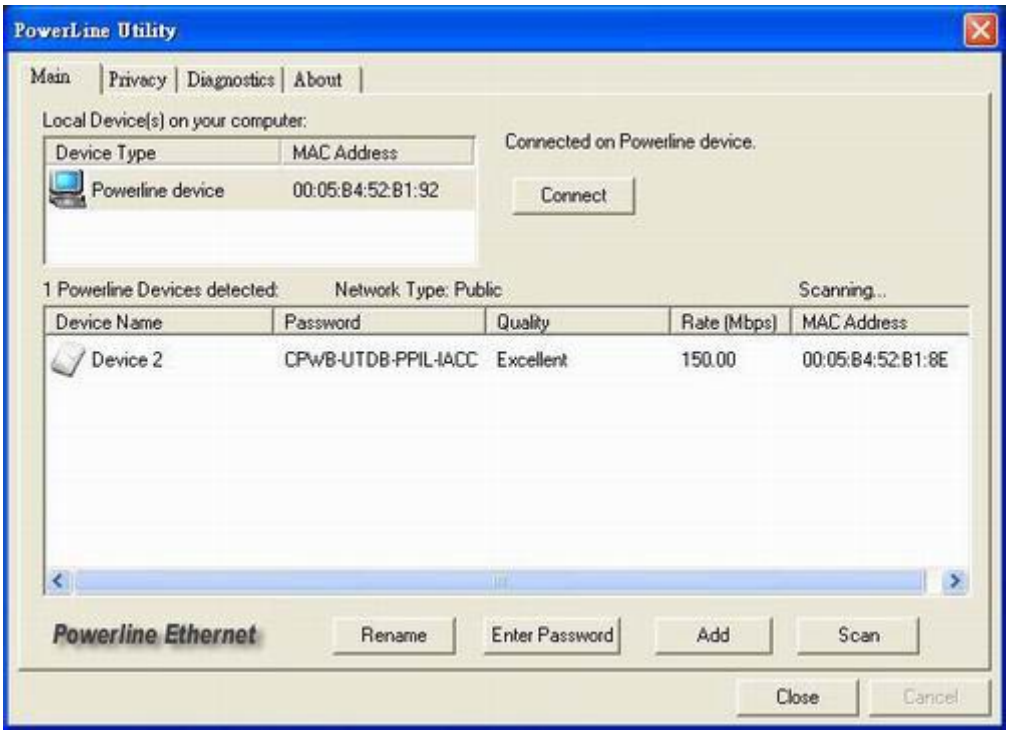


Figure 3: Multiple Local Device Connection

The **lower panel** displays all the Powerline Ethernet devices, discovered on the current logical network (remote devices). Displayed immediately above this panel is the number of remote devices found, the type of logical network (Public or Private), and a message area that reports connectivity
and scan status. The following information is displayed for each of the devices discovered that appear in the lower panel:

Device Name column shows the default device name, which may be user re-defined. A user may change the name by clicking on the name and editing in-place, or by using the rename button. An icon is optionally shown with the name. A distinction in icons is made between low-speed and high-speed devices . By default, the icon is displayed with the name.

MAC Address column shows the device's MAC address.

Password column shows the user-supplied device password (initially left blank).
A user may enter the password by using the Enter Password button.
To set the **Password** of the device (required when creating a private network), first select the device by clicking on its name in the lower panel and then click on the Enter Password button.
A dialog box will appear as shown in Figure 4 to type the password. The selected device name is shown above the field for entering the password. Hit OK after entering the new password. A confirmation box will appear if the password was entered correctly.
If a device is not found, the user will be notified and suggestions to resolve common problems will be presented.

Figure 4: Set Device Password

The **Add** button is used to add a remote device to your network that is not on the displayed list in the lower panel, for example, a device currently on another logical network. Users are advised to locate the passwords for all devices they wish to manage and add them to the local logical network by clicking on the Add button.

A dialog box will appear as seen below. The dialog box allows the user to enter both a device name and the password.

A confirmation box will appear if the password was entered correctly and if the device was found.

If a device is not found, the user will be notified and suggestions to resolve common problems will be presented.

Figure 5: Add Remote Device

Note: The device must be present on the power line (plugged in) in order for the password to be confirmed and added to the network. If the device could not be located, a warning message will be shown.

The **Scan** button is used to perform an immediate search of the Powerline Ethernet devices connected to the computer.

By default the utility automatically scans every few seconds and updates the display.

A typical screen after naming and supplying passwords might appear as in *Figure 6*.

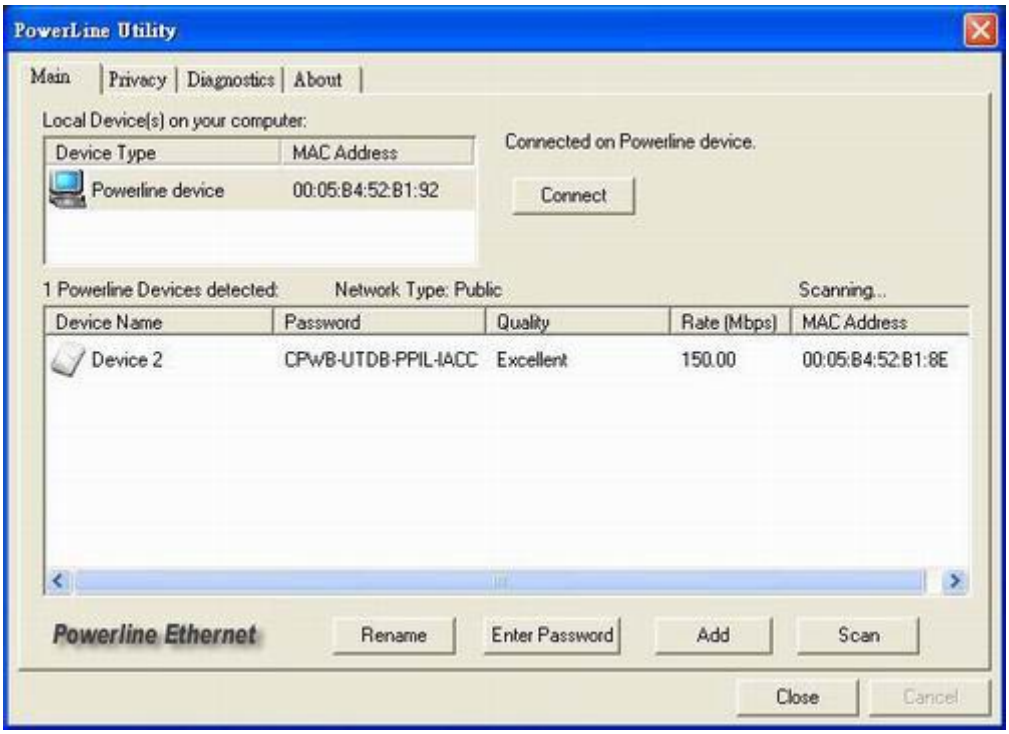


Figure 6: Main Screen of the Configuration Utility

4.3.2 Privacy Screen

The Privacy dialog screen provides a means for managing the local network and providing additional security.
All Powerline Ethernet devices are shipped using a default logical network (network name), which is normally "**HomePlug**".
The **Privacy** dialog screen allows user to make the network private by changing the network name (network password) of devices.
The user can always reset a Powerline Ethernet network to the universal one (public) by entering "HomePlug" as the network name or by clicking on the **Use Default** button.

Note: Changing the network name to any other name other than HomePlug will show the network type on the main screen as Private.

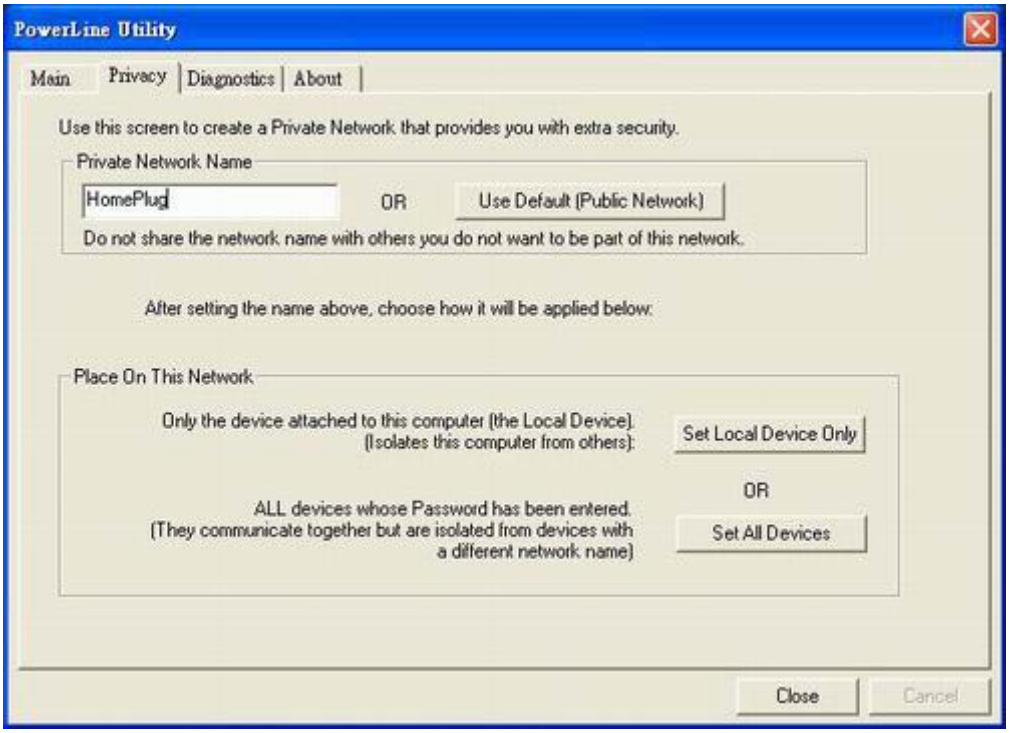


Figure 7: Privacy Screen

The **Set Local Device** Only button is used to change the network name (network password) for the local device only.

After doing this, all the devices seen on the Main panel prior to this will no longer be able to communicate or respond to the computer, as they will be on a different logical network. Devices previously set up with the same logical network (same network name) will appear in the device list afterward selecting this option.

The **Set All Devices** button is used to change the logical network of all devices that appear on the Main panel. The user must have entered the device's Password in order to set it to the new logical network. A notification message will appear to report the success of this operation.

4.4 Diagnostics Screen

The **Diagnostics** screen shows system information and a history of all devices seen.

The appearance is shown in *Figure 8*.

The **upper panel** shows technical data concerning software and hardware on the host computer used to communicate over Powerline Ethernet Network.

It shall include the following:

- Operating System Type/Version
- Host Network Name
- User Name
- MAC Address of all NICs (network interface card)
- Identify versions of all Driver DLLs and Libraries used (NDIS) and optionally
- MAC Firmware Version

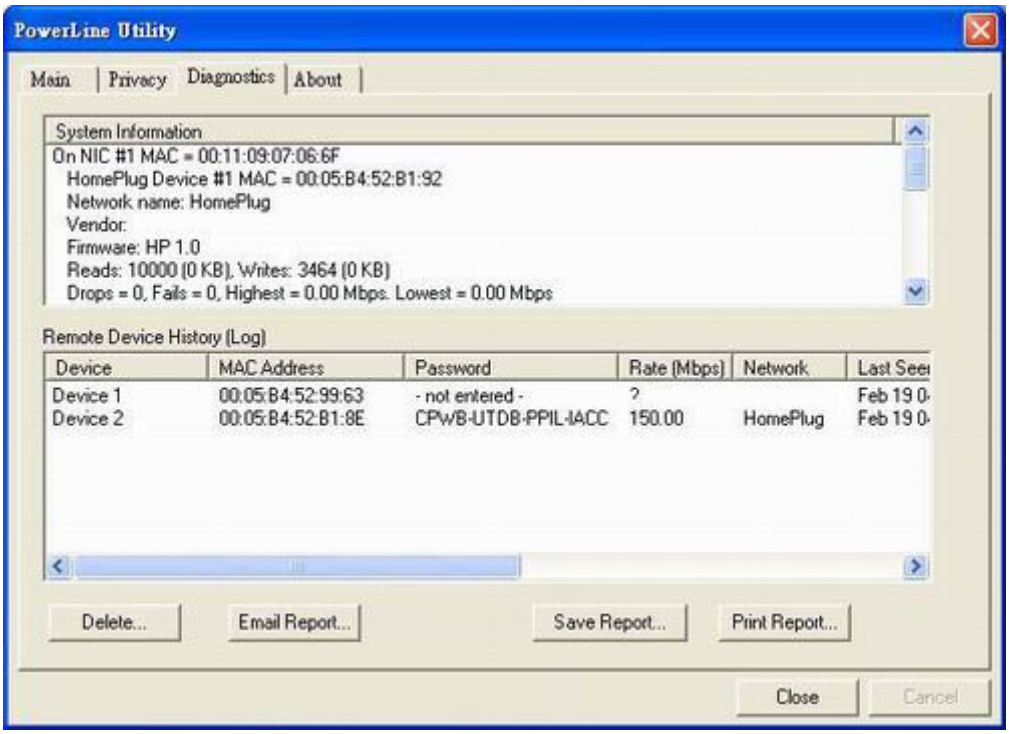


Figure 8: Diagnostics Screen

The **lower panel** contains a history of all remote devices seen on the computer, over time. Devices are shown here regardless of whether or not they are on the same logical network. Devices that are active on the current logical network will show a transfer rate in the Rate column; devices on other networks, or devices that may no longer exist are shown with an “?” in the Rate column.

The following remote device information is available from the diagnostics screen:

- Adapter Alias Name
- Adapter MAC Address
- Adapter Password
- Adapter Last known rate
- Adapter Last Known Network
- Date device last scanned
- MAC Firmware Version

The diagnostics information displayed may be saved to a text file for later emailing to technical support of a manufacturer or printed for reference during a technical support call. Devices no longer part of the network can be deleted using the delete button.

4.4.1 About Screen

The screen shows the software release date.

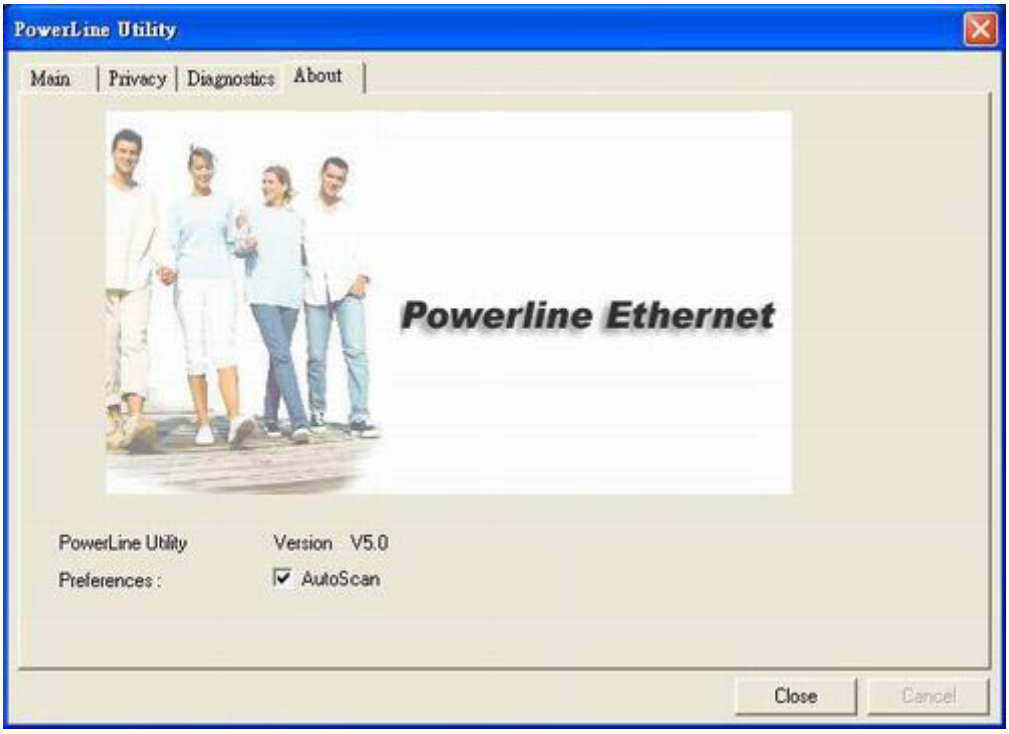


Figure 9: About dialog screen

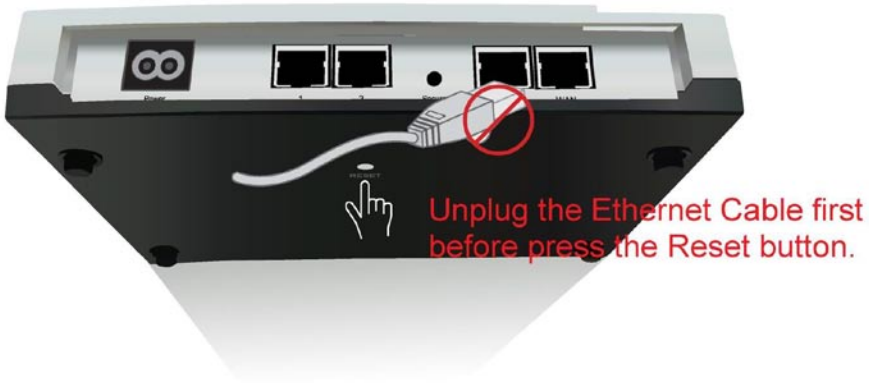
4.4.2 Preferences

The lower part of the panel may display options for user preferences (such as turning the auto-scan feature on or off) as shown *Figure 9* above.

5. Push Button Setting

There are 2 buttons in this device, one is Reset button the other is Secure button.

Reset: Push this button can reset to the factory default settings. **Be careful, when you press the reset button, please make sure unplug (remove) the Ethernet cable (RJ-45cable) first, and then press the reset button. After press the reset button (the time need < 3 sec) and then wait the PWR LED light again. Don't power off when the device is in reset process.**



Secure button can auto secure and group the Powerline devices, the follow is the scenario for secure button.

Two Push Button trigger state conditions

"Adder state" for a device providing the NMK for an existing AVLN

"Joiner state" for a device that will join an AVLN

Pushing buttons on any two devices results in one of them becoming an "adder" and the other one a "joiner"

Three possible scenarios

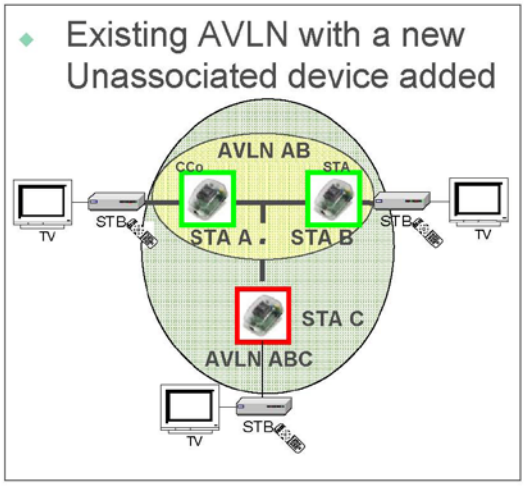
Unassociated device joining an existing AVLN

– Two Unassociated devices joining to form a new AVLN
– Special case: one device is a CCo, the other is a STA

Two Associated devices joining to form an AVLN with a new NMK

Possible Use Case Scenario 1: Unassociated device joining existing AVLN

- STA C wants to join AVLN AB
- STA A (or B) presses PB < 3 sec
- STA C presses PB < 3 sec (may precede of follow STA A/B PB)
- STA A (or B) becomes "Adder"
- STA C becomes "Joiner"
- AVLN ABC is formed using NMK of AVLN AB



Assumptions:
1) An Associated network consists of at least two Associated devices
2) All devices are delivered in matched groupings (preloaded NMK)
3) Customer-provided device's NMK is different from Associated NMK

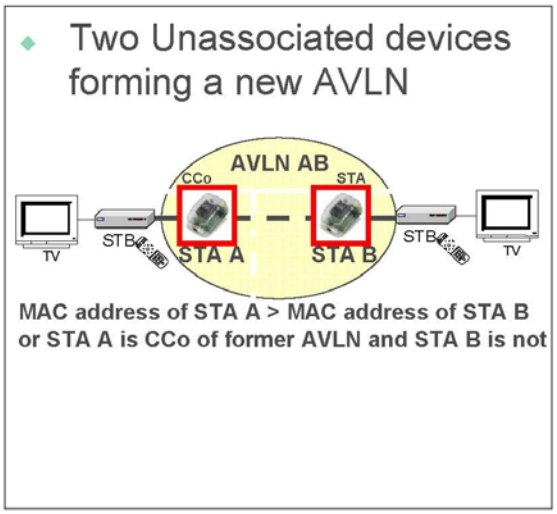
Unassociated NMK Device

Associated NMK Device

Possible Use Case Scenario 2: Two devices joining to form new AVLN

Before this scenario begin, please make sure to press each device secure button > 10 sec till all LEDs re-flash to generate the random network password key first.

- STA B wants to join with STA A (CCo with pre-existing NMK or a device with higher MAC address)
- STA A (or B) presses PB < 3 sec
- STA B presses PB < 3 sec (may precede of follow STA A PB)
- STA A (CCo or higher MAC value STA) becomes "Adder"
- STA B becomes "Joiner"
- AVLN AB is formed using NMK of STA A



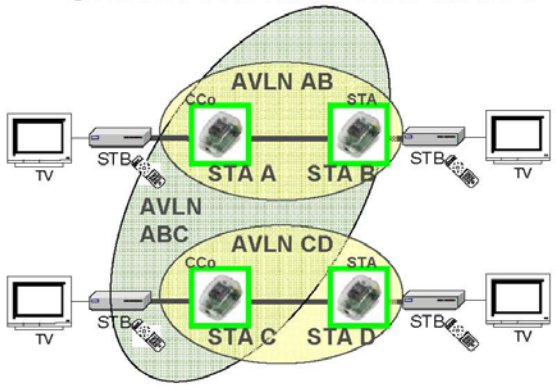
Assumptions:
1) At least one device has a pre-existing [original] NMK (CCo)
2) All devices are delivered in matched groupings (preloaded NMK)
3) Customer-provided device's NMK is different from original NMK

Unassociated NMK Device

Possible Use Case Scenario 3: Reset

- STA C wants to join AVLN AB
- STA C presses PB > 10 sec to reset its NMK to random value
- AVLN CD is removed; Case 1 scenario exists and implemented
- STA A (or B) becomes “Adder” (after PB depressed < 3 sec)
- STA C becomes “Joiner” (after PB depressed < 3 sec)
- AVLN ABC is formed using NMK of AVLN AB

- Existing AVLN with a new Unassociated device added



Assumptions:
1) An Associated network consists of at least two Associated devices
2) All devices are delivered in matched groupings (preloaded NMK)
3) Two distinct and different NMK's exist for AVLN

Associated NMK Device

6. Trouble Shooting

1. Why my utility can not work properly after finish install steps?

Ans:

Please follow the steps to check the problem.

Check the Windows version, the utility only can support windows 2000, XP, 2003, vista 32, Vista 64.

Reinstall the utility again, you can remove it and reinstall the utility again.

If the OS is vista 64, make sure you install the correct utility for vista 64. You can see it in CD auto run utility page.

2. What kind of windows OS can install the Powerline utility?

Ans:

Now the Powerline utility only supports Windows 2000, XP and 2003, Vista 32/64.

3. Why the throughput of Powerline 200M bridge is bad?

Ans:

Please follow the steps to check the problem.

Due to the master/slave structure, you need to avoid plugging two Powerline bridge in the same time, so you had better plug the Powerline to the power outlet sequence.

Please unplug the Powerline bridge and plug again, please remember plug them in sequence.

Check the Powerline utility and check the throughput again.

4. Why the Powerine 200M device can not work stable?

Ans:

In some respects, User had better to adjust the NB/PC NIC's connection type setting to 100MBaseTx half duplex while connect to powerline 200M device. It will keep the performance to the best status and stable. When user found the link is unstable or not good, please change the NIC's connection type setting to half duplex.

Appendix A Glossary

Address mask

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

AAL5

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

ADSL

Asymmetric digital subscriber line.

ATM

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

AWG

American Wire Gauge - The measurement of thickness of a wire.

Bridge

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

Broadband

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

CO

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

CPE

Customer Premises Equipment located in a user's premises.

DHCP (Dynamic Host Configuration Protocol)

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

DMT

Discrete Multi-Tone frequency signal modulation

Downstream rate

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

DSLAM

Digital Subscriber Line Access Multiplex

Dynamic IP Addresses

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

Encapsulation

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

Ethernet

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

FTP

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

Hop count

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

HTML

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

HTML browser

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

http

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

ICMP

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

Internet address

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

Internet Protocol (IP)

The network layer protocol for the Internet protocol suite

IP address

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

ISP

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

MAC

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

MIB

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

NAT

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

NVT

Network Virtual Terminal

PAP

Password Authentication Protocol

PORT

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

POTS

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

PPP

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

PPPoE

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

Remote server

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

RFC

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

Route

The path that network traffic takes from its source to its destination. The route a datagram may follow can include many routers and many physical networks. In the Internet, each datagram is routed separately.

Router

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

Routing table

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

Routing Information Protocol

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

SNMP

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

SOCKET

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

Spanning-Tree Bridge Protocol (STP)

Spanning-Tree Bridge Protocol (STP) - Part of an IEEE standard. A mechanism for detecting and preventing loops from occurring in a multi-bridged environment. When three or more LAN's segments are connected via bridges, a loop can occur. Because a bridge forwards all packets that are not recognized as being local, some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

Spoofing

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

Static IP Addresses

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

Subnet

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

TCP

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

TFTP

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

Telnet

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

Transparent bridging

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

UDP

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

UNI signaling

User Network Interface signaling for ATM communications.

Virtual Connection (VC)

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

WAN

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

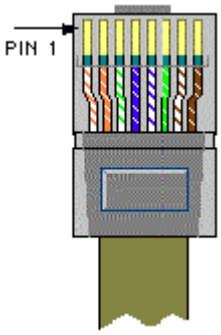
Appendix B Cabling / Connection

Network cables connect PCs in an Ethernet network Category 5, called "Cat5" for short is commonly used type of network cable today.

Cat 5 cables are tipped with RJ-45 connectors, which fit into RJ-45 port.

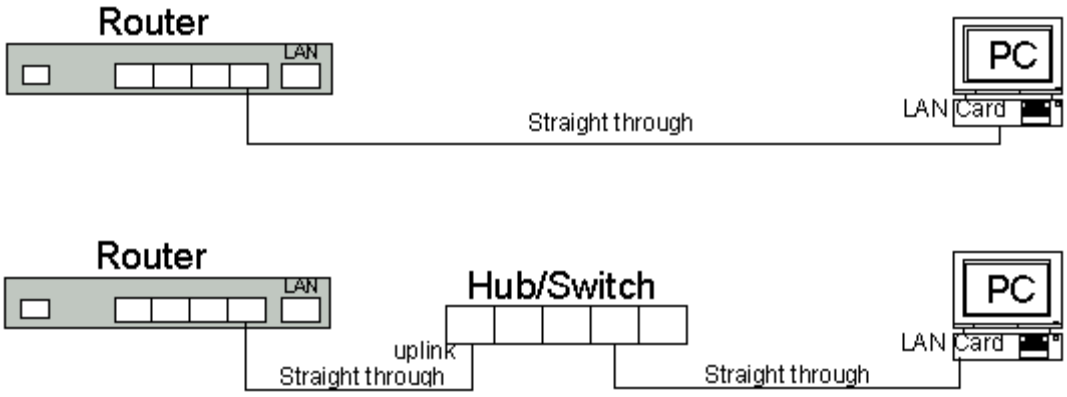
Straight-through vs. Crossover Cables:

Straight-through	
Wire	Becomes
1	1
2	2
3	3
6	6



Straight-through	
Wire	Becomes
1	1
2	2
3	3
6	6

LAN Connection:



To check LEDs light up when you finish connecting two pieces of hardware.