XAVi XG-6440b/g Gateway User's Manual

Copyright

Changes are periodically made to the information in this document. They will be incorporated in subsequent editions. The supplier may make improvements and/or changes in the product described in this document at any time.
Technical support
Up-to-date information
Your new purchased XAVi product is updated with the latest technology and design. However, we keep going to modify and update the product features to keep you with up-to-date technologies with firmware or software upgrade. You can visit our web site on www.xavi.com.tw to check if there is new software for your product.

Problem solving
If you have difficulty resolving problems in installation or have further technical questions, you can go www.xavi.com.tw to look for the latest FAQ or contact with us by following ways:

Web site: www.xavi.com.tw
Tech support: support@xavi.com.tw
Sales: sales@xavi.com.tw

Table of contents

CHAPTER 1 INTRODUCTION

1.1 PRODUCT OVERVIEW

The XG-6440 is an IEEE 802.11b compliant wireless gateway and the XG-6440g is an IEEE 802.11g compliant wireless gateway. The XAVi XG-6440 series gateway connects a LAN to other LANs and to wide area networks (WANs) such as the Internet or a corporate Intranet. The XG-6440G allows you to protect, share, store, and access data over any available network.

1.2 Features and benefits

XG-6540G 802.11g Wireless Gateway

XG-6540G is a state-of-the-art new Wireless Gateway with the latest advanced broadband wireless connectivity technology. Applying with 802.11g technologies, it features high speed and transfer rates can up to 54Mbps, compatible with 802.11b. Also, with a built-in 4 port 10/100 Base-TX switches, it is effortless to build a LAN and share Internet access via wire line and wireless.

XG-6540G features the integrated NAT technologies, including enhanced much higher level of security and firewall protection to shield your internal network and stop intruder and hackers from accessing your network.

XG-6540G flexible design lets it work with a variety of platforms, PC/Mac, and with different operation systems. It can also be connected with FTTH devices, cable modems or any one of the **XAVi** xDSL series modems/routers to obtain broadband Internet service. Web-based user interface facilitates the management and easy way to share files, resources and access with other LAN users.

Features

- Supports PPPoE, PPP, PPTP Client, ARP, DHCP Client and Server, TCP/IP, UDP, ICMP, DNS Proxy, Dynamic DNS, SNTP features
- Four 10/100M Base TX ports for PC or LAN connection and one10/100M Base TX WAN port for broadband connection
- 802.11g wireless access point supports up to 54Mbps
- Speeds up the gaming and multimedia connections dramatically
- Supports automatic hacker pattern detection to block malicious intrusion of local networks
- Network Address Translation (NAT) conceals private network from outside view while VPN pass through allows secure communication between offices
- Provides web-based user interface eases the installation, configuration

and management

- Virtual server feature, outside users will be able to access the internal servers via Internet
- Administrators can block specific interior users' Internet access by UPI (User Profile Identification)
- Supports UPnP for easy device discovery
- Allows LAN users to access Internet through Network Address Translation (NAT, IP sharing) simultaneously

1.2 What’s in the package?

To Be Determined.

1.3 Important rules for safe operation

In addition to the careful attention devoted to quality standards on the manufacture of network products, safety is a major factor in the design of every product. However, safety is your responsibility, too. This section lists the router and accessory equipment. Please read them carefully before operation and using the router.

- Read and follow instruction- You should read all the safety and operating instructions before operating the router.
- Retain Instructions- You should save all the safety and operating instructions, for your future reference.
- Heed Warning- Comply with all warnings on the products and in the operating instructions.
- Check Power Sources- Operate this product only from the type of power source indicated on the product’s marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Be Careful of Overloading- Do not overload wall outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard. Periodically examine the cord, and if its appearance indicates damage or deteriorated insulation, have it replaced by your service technician.
- Protect Power Cords – Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them.

Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the product.

- Check Ventilation – Slots and openings in the enclosure are provided for ventilation to ensure reliable operation of the product and to product and to protect it from overheating. Do not block or cover these openings, never block these openings by placing the product on a bed, sofa, rug, or other similar surface. Never place this product near or over a radiator or heat register, or any other hear source (including amplifiers). Do not place this product in a built-in installation, such as bookcase or equipment rack, unless you provide proper ventilation.
- Do Not Use Accessories – Do not use attachments, unless they are recommended by your vendor, as they may cause electrical or fire hazards.
- Use the Recommended Power Adaptor – Your must use the power adaptor that comes with your product.
- Do Not Use Near Water – Do not use this product near water. For example, near a swimming pool, bathtub, washbowl, and the like.
- Do Not place near high temperature source – For example near a steamer, kitchen range fire, and the like.
- Use Caution in Mounting this product – Do not place this product on an unstable surface support. The product may fall, causing serious injury to a child or adult, as well as serious damage to the product.
- Use Care in Moving Product-and-Cart Combinations – Quick stops, excessive, force and uneven surfaces may cause the product-and-cart combination to overturn.
- Unplug Power Before Cleaning – Do not use liquid cleaner or aerosol cleaner. Use a damp cloth for cleaning.
- Keep Objects Out of Openings – Never push objects of any kind into this product through openings, as they may touch dangerous voltage or “short-out” parts, which could result in a fire or electric shock. Never spill liquid on the product.
- Protect From Lighting – For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet, and disconnect the cable system. This will prevent damage to the product due to lightning and power line surges.
- Turn Off the Power Switch Between DC plugs Off and On.

- Do Not Remove Covers – Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous voltage or hazards.
- Unplug this Product From Wall Outlet Carefully, as the Power Adaptor May Be Hot.
- Refer Servicing to Qualified Service Personnel Under the Conditions Listed Below.

  >When the power supply cord or plug is damaged.

  >If liquid has been spilled or objects have fallen into the product.

  >If the product has been exposed to rain or water.

  >If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions.

  >If the product has been dropped or the cabinet has been damaged.

  >When the product exhibits a distinct change in performance, such as the inability to perform bask functions – this indicates a need for service.
- Require Safety Check – Upon completion of any service or repairs to this product, ask the service technician to perform safety checks recommended by service point to determine that the products is in safe operating condition.

1.4 Connecting The XAVi Wireless Gateway

To Be Determined.

Reset Button. Press the reset button for 5 seconds; the gateway will be restored to default value. All your old configurations will be gone, please backup your configuration.

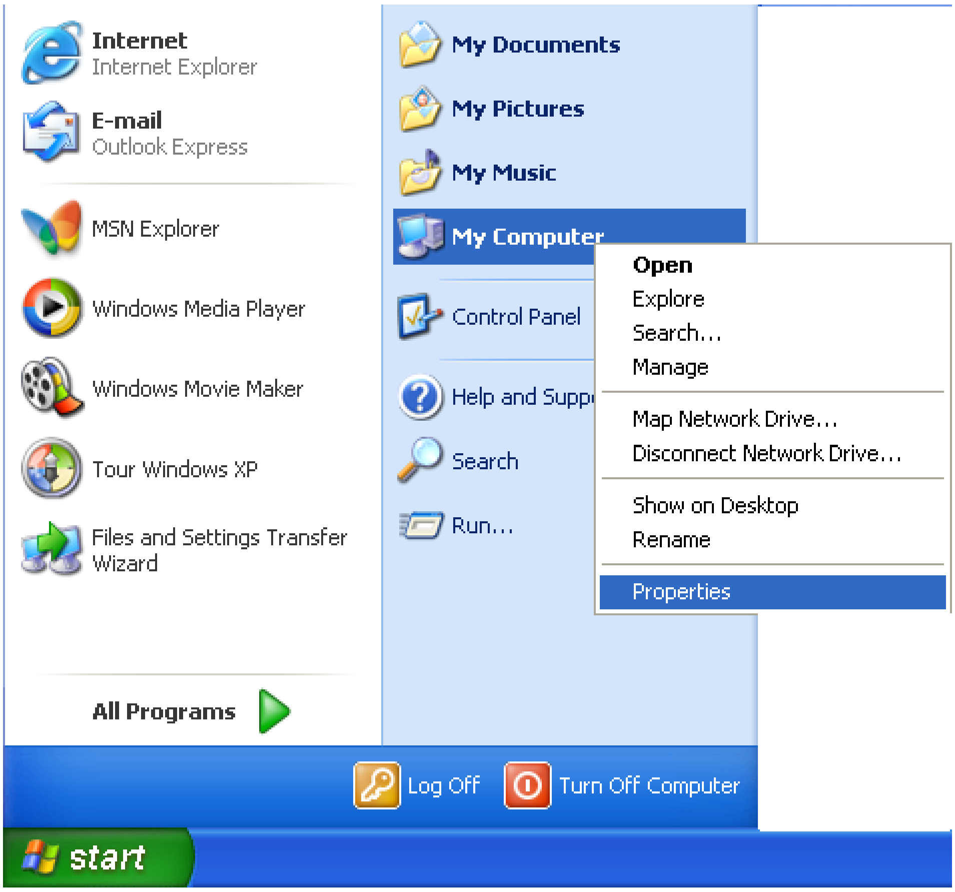
CHAPTER 2 CONFIGURING THE PCs

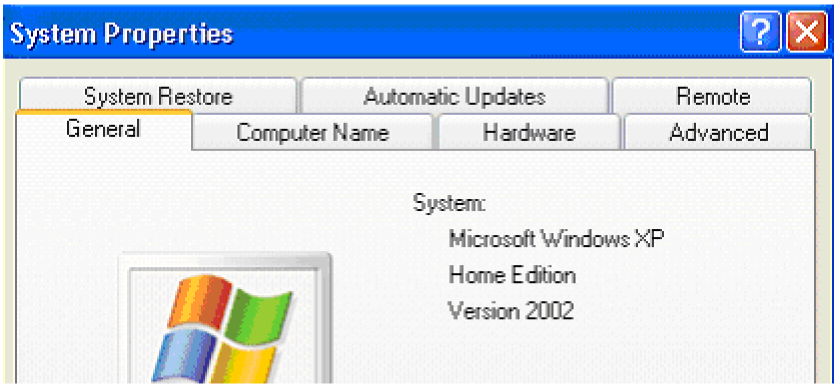
Overview

The instructions in this chapter will help you configure each of your computers to be able to communicate with the Router.

To do this, you need to configure your PC's network settings to obtain an address automatically, so your PC can function as a DHCP client. Computers use IP address to communicate with the Router and each other across a network, such as the Internet.

First, find out which Windows operating system your computer is running. You can find out by right clicking **My computer** on your desktop (if you can not find in on the desktop, click the Start button to find it). Then choose **contents** in the menu, the system information tells you which operating system you are using.





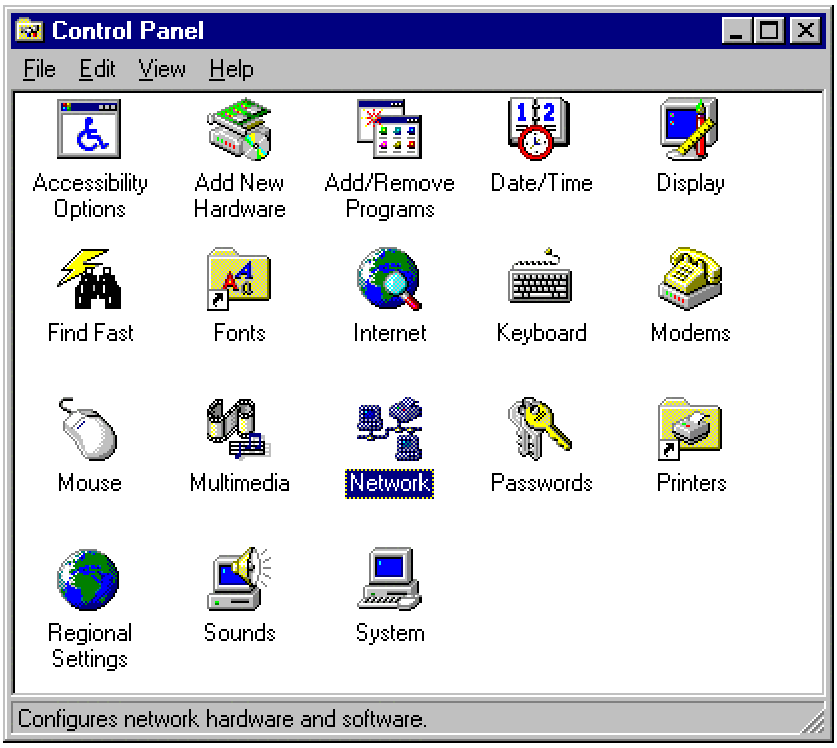
System:
Microsoft Windows XP
Home Edition
Version 2002

You may need to do this for each computer you are connecting to the Router.

The next few pages tell you, step by step, how to configure your network settings based on the type of Windows operating system you are using. Make sure that an Ethernet or wireless adapter (also known as a network adapter) has been successfully installed in each PC you will configure. Once you’ve configured your computers, continue to “chapter 3: configuring the wireless gateway”.

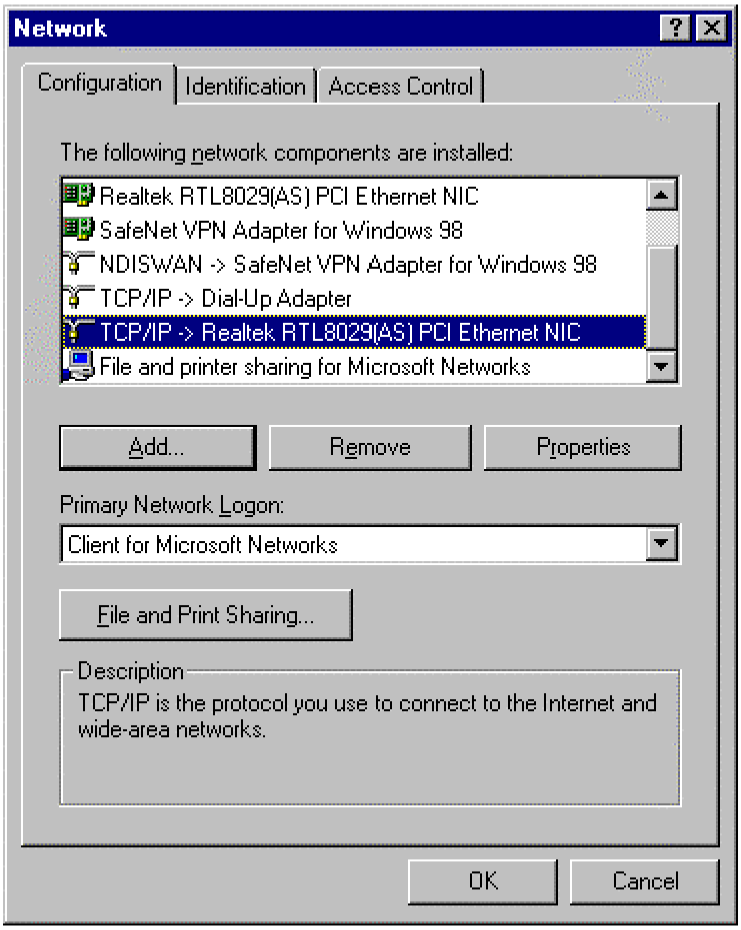
Configuring Windows 98 and Millennium PCs

1. Click the Start button. Select Settings and click the Control Panel icon. Double-click the Network icon.



Configures network hardware and software.

2. On the Configuration tab, select the TCP/IP line for the applicable Ethernet adapter. Do not choose a TCP/IP entry whose name mentions DUN, PPPoE, VPN or AOL. If the word TCP/IP appears by itself, select that line. Click the Properties button.



Network

Configuration | Identification | Access Control

The following network components are installed:

- Realtek RTL8029(AS) PCI Ethernet NIC
- SafeNet VPN Adapter for Windows 98
- NDISWAN -> SafeNet VPN Adapter for Windows 98
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Realtek RTL8029(AS) PCI Ethernet NIC
- File and printer sharing for Microsoft Networks

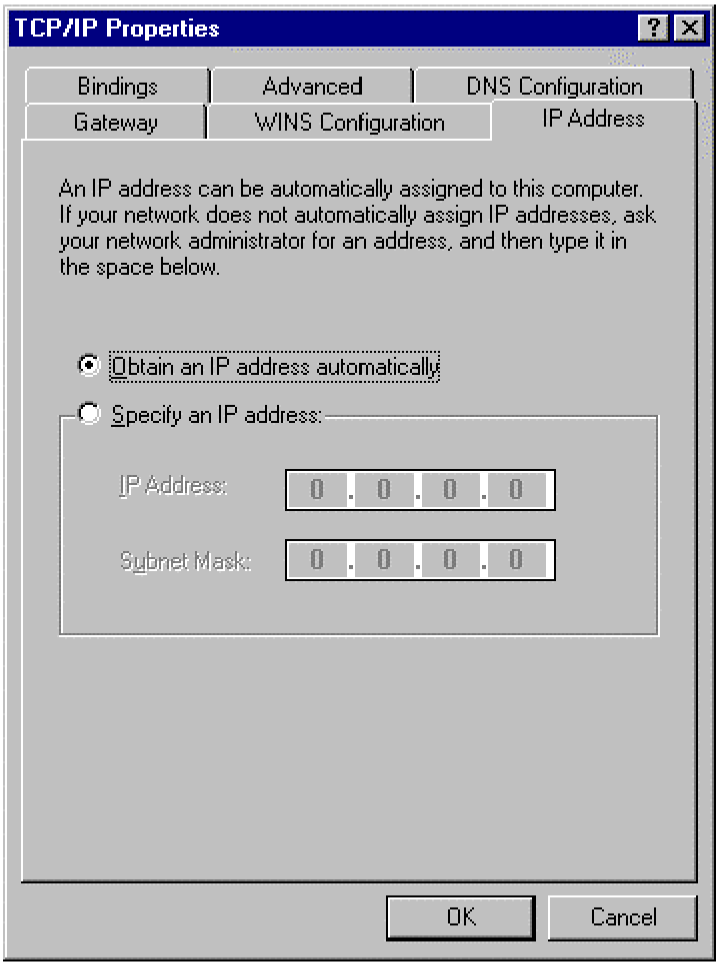
Primary Network Logon:

Client for Microsoft Networks

Description

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

3. Click the IP Address tab. Select Obtain an IP address automatically.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

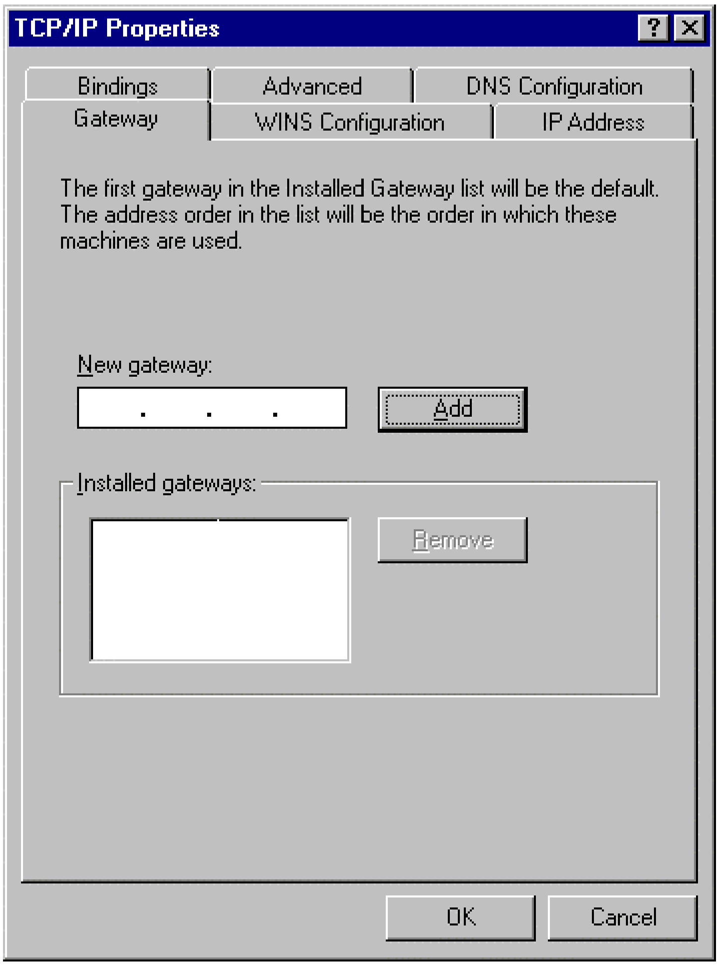
● Obtain an IP address automatically

○ Specify an IP address:

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

4. Now click the gateway tab, and verify that the Installed Gateway field is blank. Click the OK button.



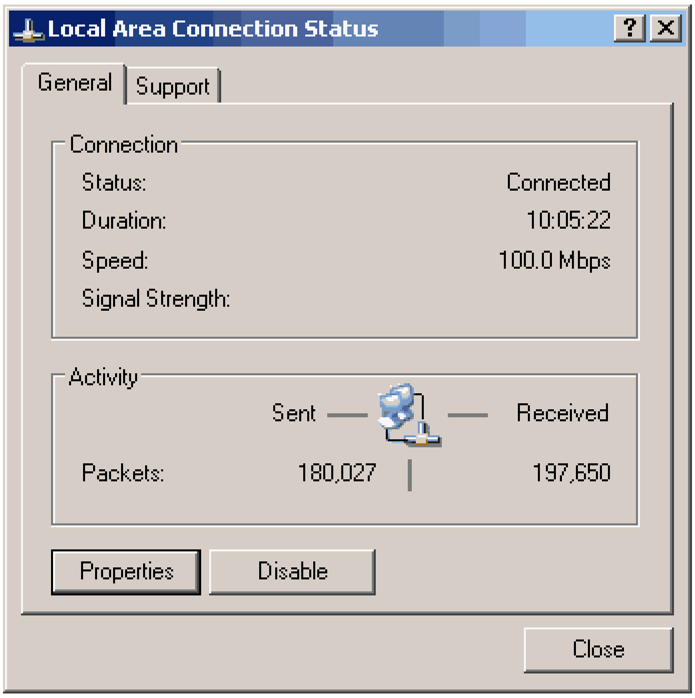
The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

5. Click the OK button again. Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into your CD-ROM drive and check the correct file location, e.g., D:\win98, D:\win9x, etc. (If “D” is the letter of your CD-ROM drive).
6. Windows may ask you to restart your PC. Click the Yes button. If Windows does not ask you to restart, restart your computer anyway.

Configuring Windows 2000 PCs

1. Click the Start button. Select Settings and click the Control Panel icon. Double-click Network and Dial-up Connections icon.

2. Select the Local Area Connection icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the Local Area Connection. Click the Properties button.



Connection

Status: Connected

Duration: 10:05:22

Speed: 100.0 Mbps

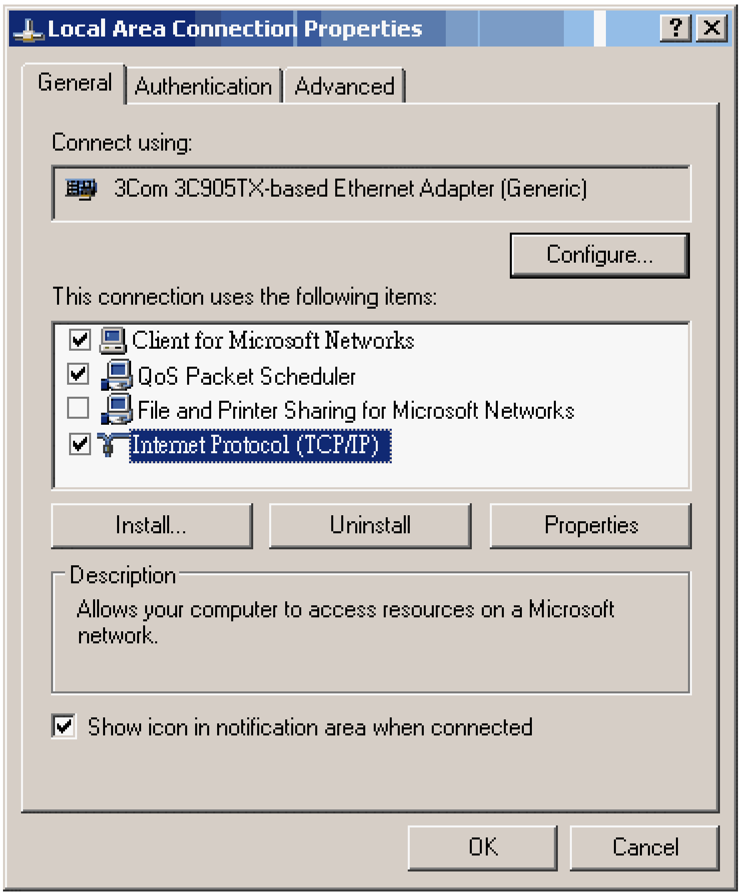
Signal Strength:

Activity

Sent — Received

Packets: 180,027 | 197,650

3. Make sure the box next to Internet Protocol (TCP/IP) is checked. Highlight Internet Protocol (TCP/IP), and click the Properties button.



Connect using:

3Com 3C905TX-based Ethernet Adapter (Generic)

This connection uses the following items:

☑ Client for Microsoft Networks

☑ QoS Packet Scheduler

☐ File and Printer Sharing for Microsoft Networks

☑ Internet Protocol (TCP/IP)

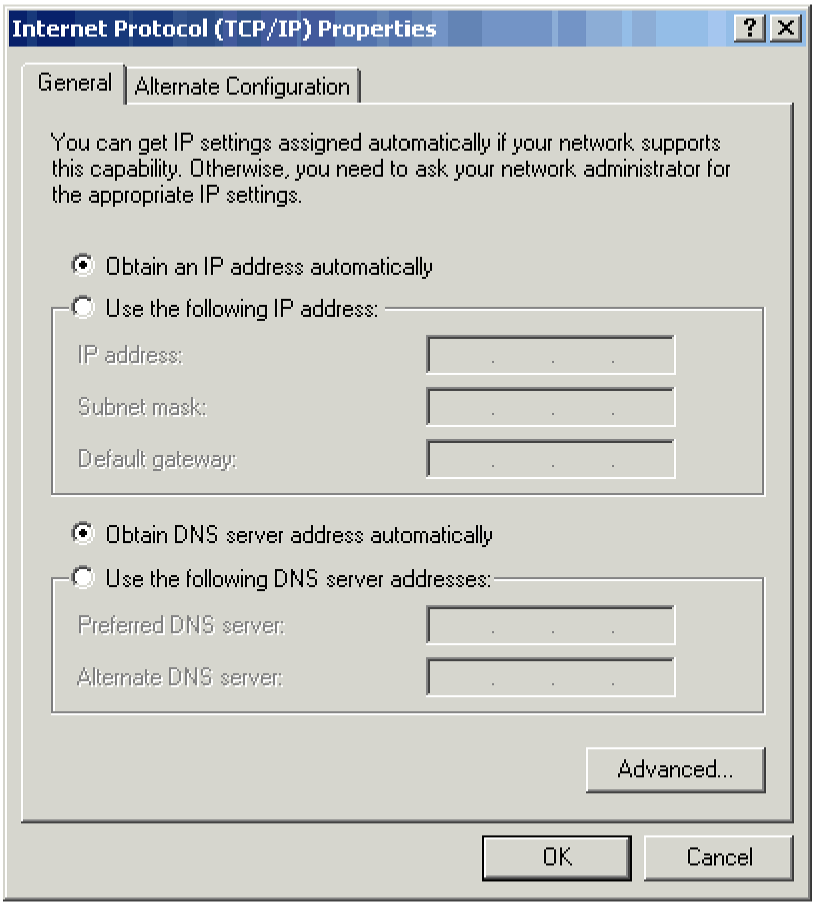
Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected

4. Select Obtain an IP address automatically. Once the new window appears, click the OK button. Click the OK button again to complete the PC

configuration.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

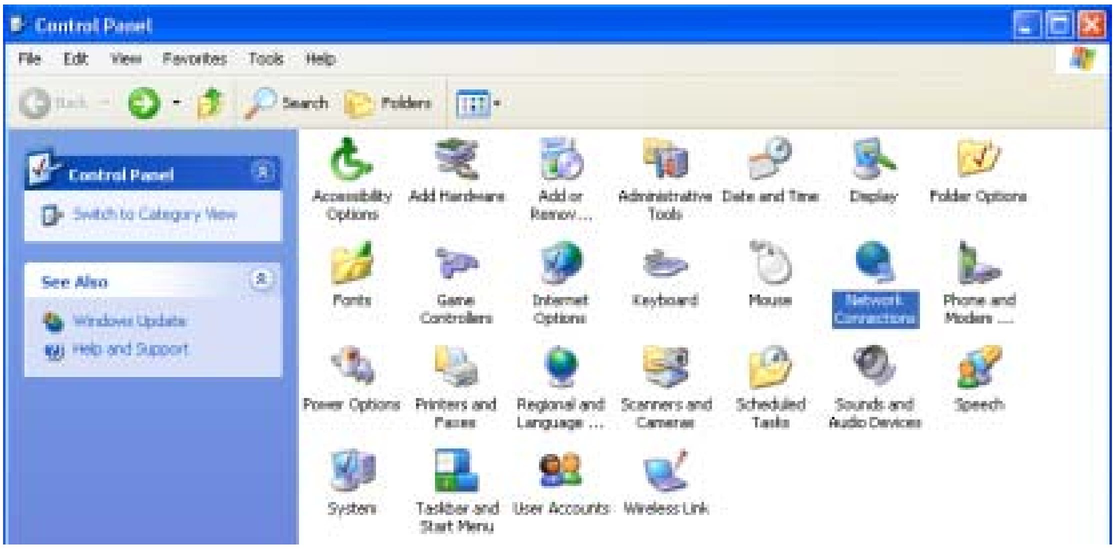
Alternate DNS server: . . .

5. Restart your computer.

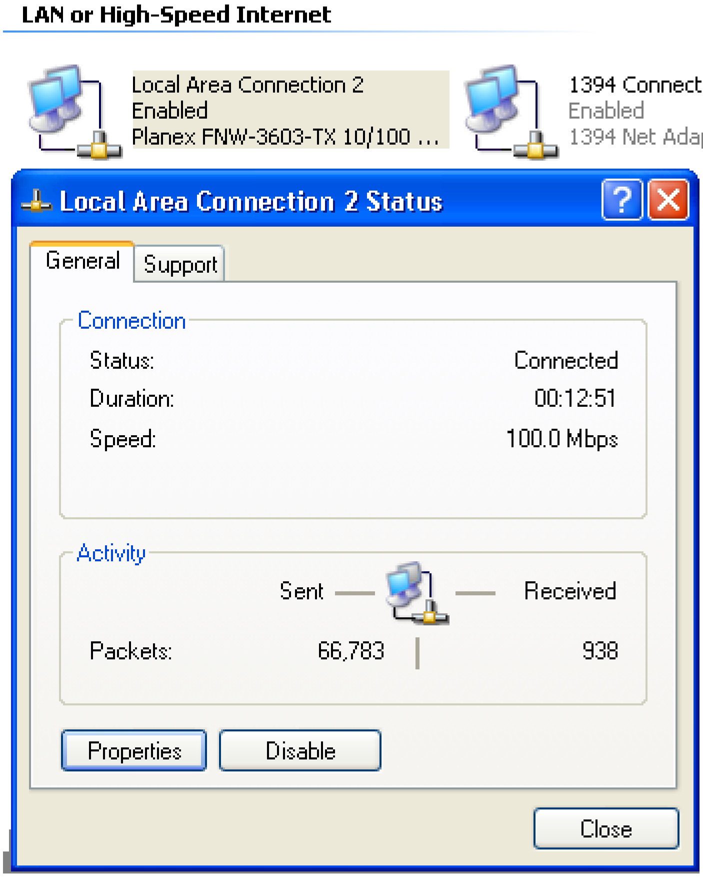
Configuring Windows XP PCs

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

1. Click the Start button and then the Control Panel icon. Click the Network and Internet Connections icon. Then click the Network Connections icon.



2. Select the Local Area Connection icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the Local Area Connection. Click the Properties button.



LAN or High-Speed Internet

Local Area Connection 2
Enabled
Planex FNW-3603-TX 10/100 ...

1394 Connection
Enabled
1394 Net Adapter

Local Area Connection 2 Status

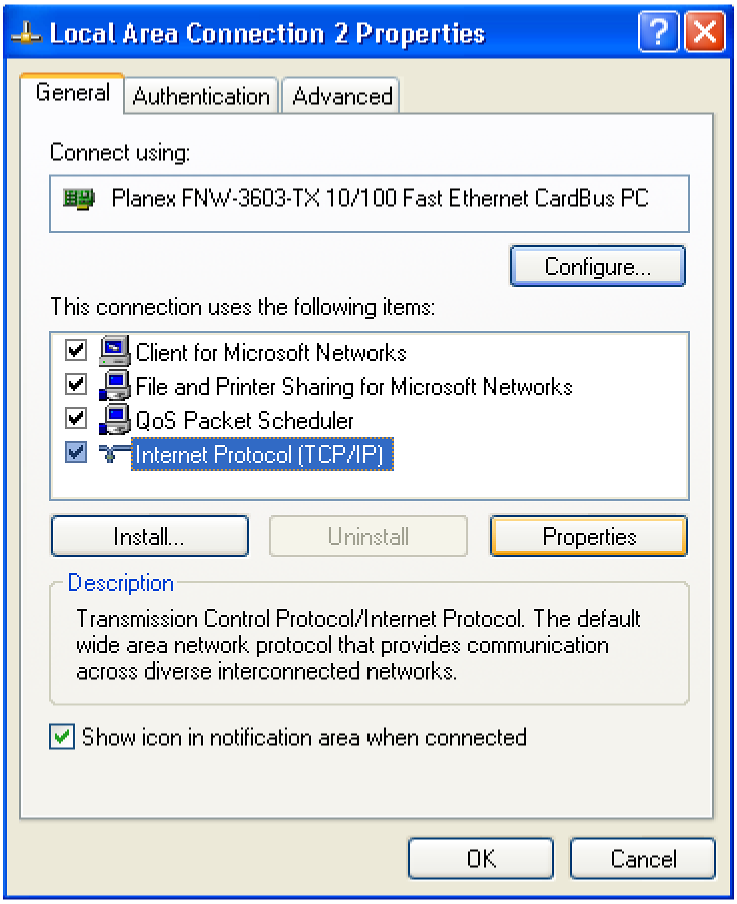
Connection

Status:	Connected
Duration:	00:12:51
Speed:	100.0 Mbps

Activity

	Sent	Received
Packets:	66,783	938

3. Make sure the box next to Internet Protocol (TCP/IP) is checked. Highlight Internet Protocol (TCP/IP), and click the Properties button.



Local Area Connection 2 Properties

General | Authentication | Advanced

Connect using:

Planex FNW-3603-TX 10/100 Fast Ethernet CardBus PC

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

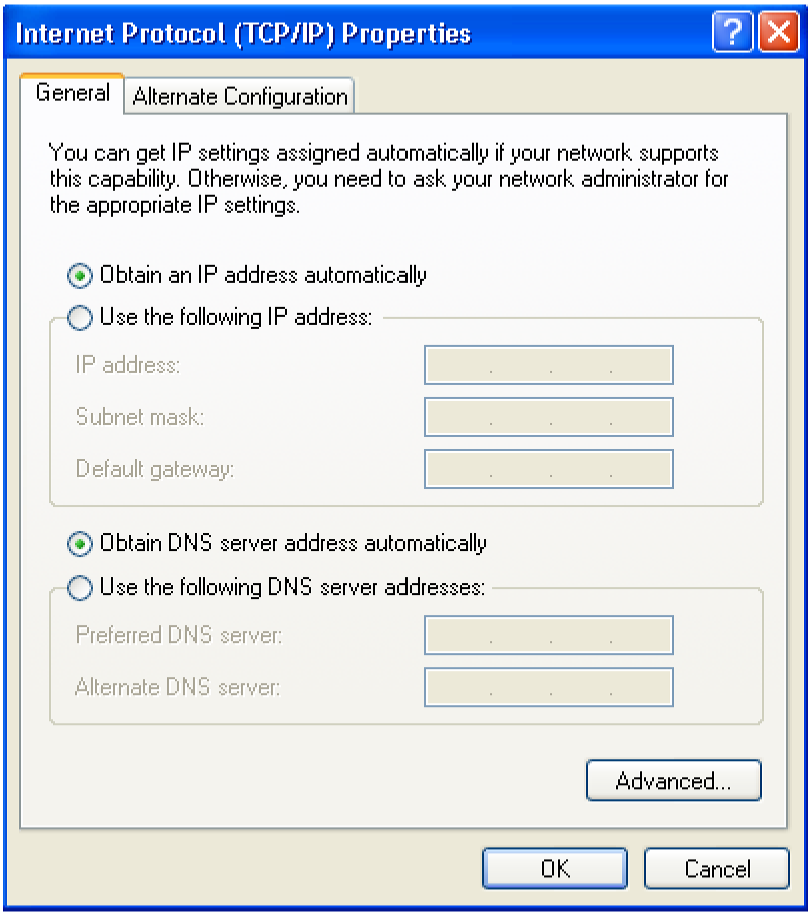
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

OK | Cancel

4. Select Obtain an IP address automatically. Once the new window appears, click the OK button. Click the OK button again to complete the PC configuration.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

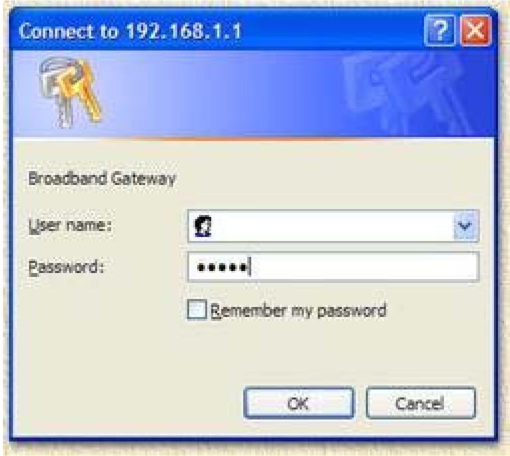
Preferred DNS server: . . .

Alternate DNS server: . . .

After you have successfully got an IP, please access the router by typing http://192.168.1.1 to configure the router. (If you have changed the route's IP address, please type http://<the new IP address of the gateway>.)

CHAPTER 3 CONFIGURING THE WIRELESS GATEWAY

The first time you start to configure the gateway by the web using the web browser with address **http://192.168.1.1**, the gateway will ask you to login with the user name and password, both the user name and password are "**admin**" for the default value. Please change the User Name and Password from the default value to your own settings. Otherwise, the others might use the default value to enter your gateway easily. Please refer to **3.2.4 Advanced Setup >> Remote Management** for more information.



Connect to 192.168.1.1

Broadband Gateway

User name:

Password: •••••

□ Remember my password

3.1 Basic Configuration

The basic configuration contains Internet Port, Local Port and the Wireless LAN configurations. After you finished the basic items, the gateway will work for most functions.

3.1.1 Internet Port

The Internet Port connects to your modem to get the access to the Internet. You will need to configure for the right settings that is assigned by your ISP.

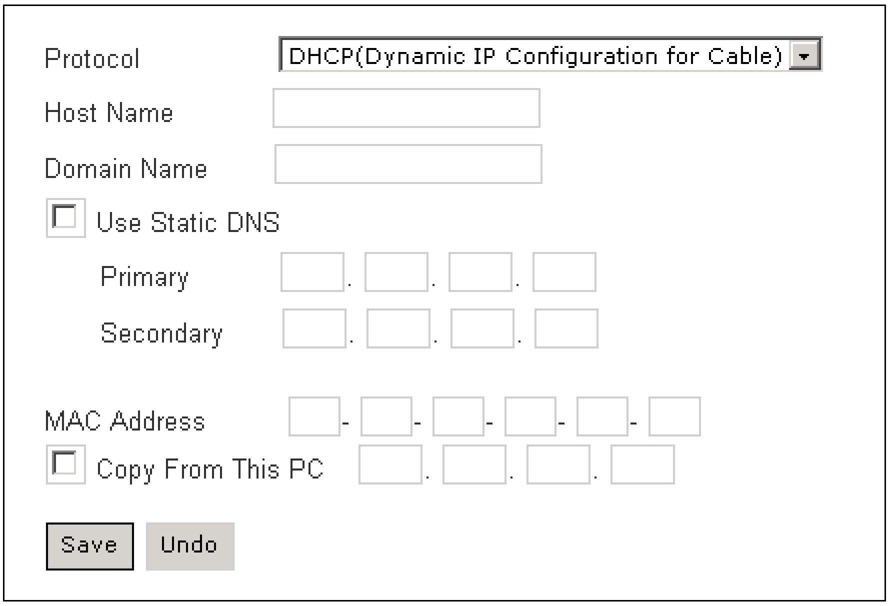
DHCP Configuration

The DHCP is the default service for the Internet Port; you will get the IP address from the ISP automatically.

Host Name/Domain Name. Some cable ISPs require the host name and domain name as identification, Your may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, assign on your own or leave it as blank will work.

Use Static DNS. If you want to use your own DNS instead of ISP’s provision, check this box, and give the IP address of the DNS in the field. (At least one in the primary field.)

MAC address. Some ISPs allow you to connect to them with specified MAC address only, you can enter the MAC address manually or copy it from a PC which is attached to the Local Port, you just type in its IP address, the gateway will copy the MAC address from that PC. The gateway comes with the factory default MAC address, no need to change the default value if the ISP is not checking the MAC address of your Internet Port.



Protocol: DHCP(Dynamic IP Configuration for Cable)

Host Name

Domain Name

□ Use Static DNS

Primary . . .

Secondary . . .

MAC Address - - - - -

□ Copy From This PC . . .

PPPoE Configuration

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP if they use PPPoE.

Host Name/Domain Name. Some ISPs require the host name and domain name as identification, if it is not specified, assign on your own or leave it as blank.

User Name, Password, Confirm Password. Enter your username, password and confirm again in the fields for the login to the ISP.

Service Name. Enter the ISP specified service name or assign on your own if the Service Name is not specified.

Packet Size (MTU). The Maximum Transmission Unit of an IP packet. The default value is 1492 Bytes, if your ISP requires a special value, please select from the pull down menu. The default value will work for most cases. Otherwise, contact your ISP for the MTU value.

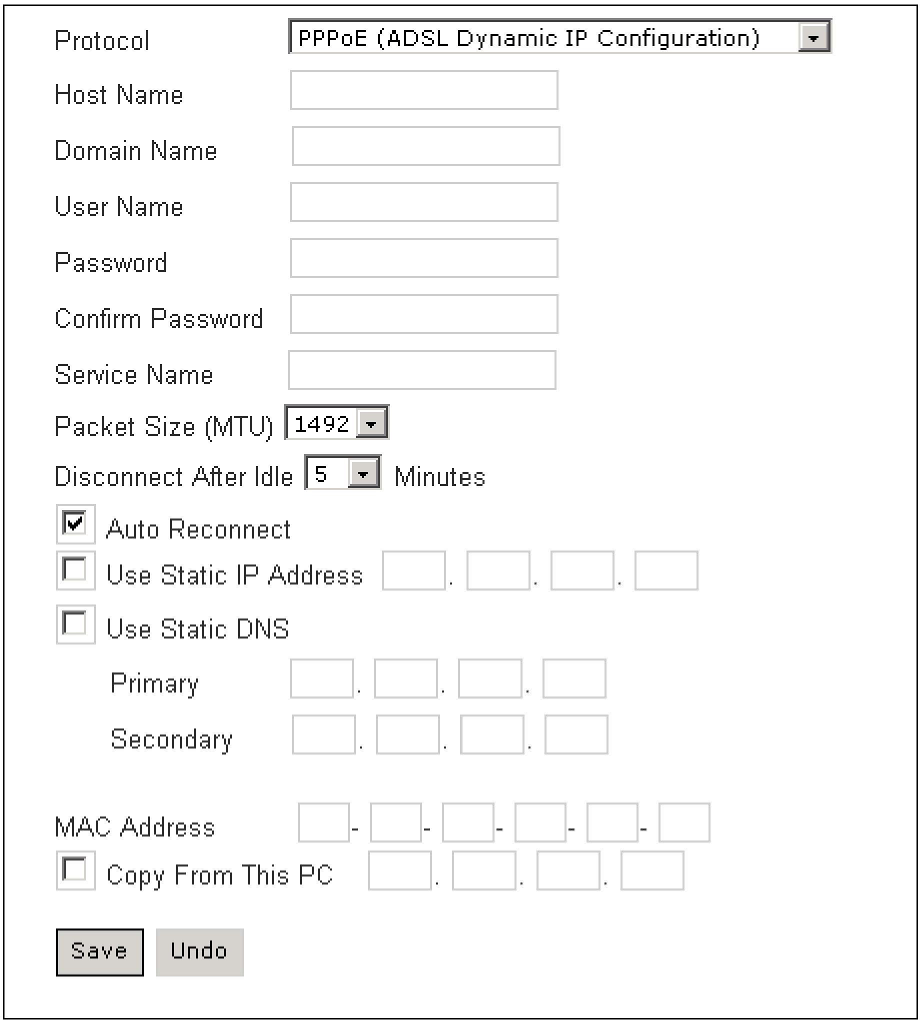
Disconnect after idle time. You can assign an idle time if there is no Internet traffic for the idle time you specified, the modem would be disconnected from the ISP by the gateway automatically. The default value is 5 minutes.

Auto Reconnect. The gateway will reconnect your modem to the ISP when you start the Internet access again after the idle time out you specified above. Leave the Auto Reconnect unchecked, the PPPoE connection will be always on, also the Disconnect after idle time will not work.

Use Static IP Address. If your ISP does not assign a dynamic address, you will use the static IP address, enter the IP address, subnet mask, and DNS address which your ISP assigned.

Use Static DNS. If you want to use your own DNS instead of ISP's provision, click the checkbox, and give the IP address of the DNS in the field. (At least one for the primary field.)

MAC address. Some ISPs allow you to connect to them with specified MAC address only, you can enter the MAC address manually or copy it from a PC which is attached to the Local Port, you just type in its IP address, the gateway will copy the MAC address from that PC. The gateway comes with the factory default MAC address, no need to change the default value if the ISP is not checking the MAC address of your Internet Port.



Protocol: PPPoE (ADSL Dynamic IP Configuration)

Host Name

Domain Name

User Name

Password

Confirm Password

Service Name

Packet Size (MTU): 1492

Disconnect After Idle: 5 Minutes

☑ Auto Reconnect

□ Use Static IP Address ___ . ___ . ___ . ___

□ Use Static DNS

Primary ___ . ___ . ___ . ___

Secondary ___ . ___ . ___ . ___

MAC Address ___ - ___ - ___ - ___ - ___ - ___

□ Copy From This PC ___ . ___ . ___ . ___

Static IP Configuration

If you connect to the Internet using permanent IP address, please select Static IP Configuration from the pull down menu, and fill the ISP specified values in the fields.

Host Name/Domain Name. Some ISPs require the host name and domain name as identification, if it is not specified, assign on your own or leave it as blank.

IP Address. The IP address of the gateway’s Internet port, please use the ISP specified address.

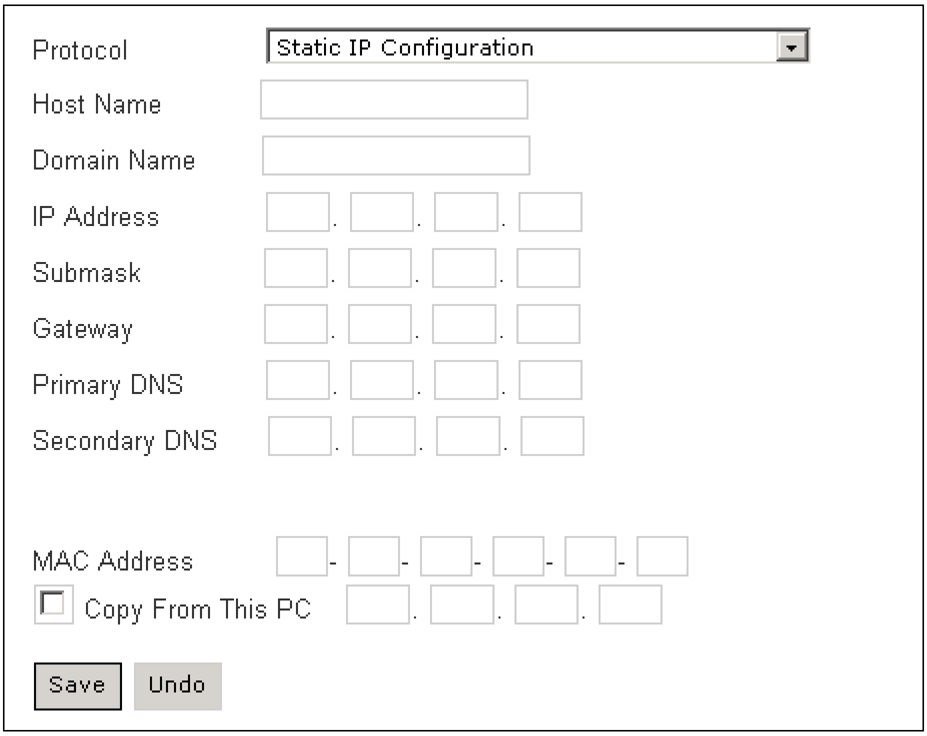
Subnet mask. The subnet mask supplied by your ISP.

Gateway. Your ISP will assign a gateway address for you, if you could not find one, please contact your ISP.

Primary DNS. The domain name server of the ISP or of your own.

Secondary DNS. The back up domain name server could be left blank if none.

MAC address. Some ISPs allow you to connect to them with specified MAC address only, you can enter the MAC address manually or copy it from a PC which is attached to the Local Port, you just type in its IP address, the gateway will copy the MAC address from that PC. The gateway comes with the factory default MAC address, no need to change the default value if the ISP is not checking the MAC address of your Internet Port.



Protocol: Static IP Configuration

PPTP Configuration

Some older modems in Europe use PPTP connection instead of PPPoE, it uses PPP session dial to the modem first, the modem will dial to your ISP, after the connection between the ISP and your modem established, you could share the connection with the modem.

Host Name/Domain Name. Some ISPs required the host name and domain name as identification, if it is not specified, assign on your own or leave it as blank.

User Name, Password, Confirm Password. Enter your username, password and confirm again in the fields for the login to the ISP.

Server IP. Your modem’s IP, you have to set your computer as the same domain as your modem’s (such as the modem’s IP address is 192.168.0.1 and the subnet mask is 255.255.255.0, your PC must be configured as 192.168.0.x, the x is from 2 to 254, the subnet mask should be same as the modem’s 255.255.255.0), then you can reach the modem, if you are not sure that your configuration is right, please try “ping <your modem’s IP>” in the command line from your PC. If you don’t know the modem’s IP, please refer to the modem’s manual or consult your ISP.

Packet Size (MTU). The Maximum Transmission Unit of an IP packet. The default value is 1492 Bytes, if your ISP requires a special value, please select from the pull down menu. The default value will work for most cases. Otherwise, contact your ISP for a specified value.

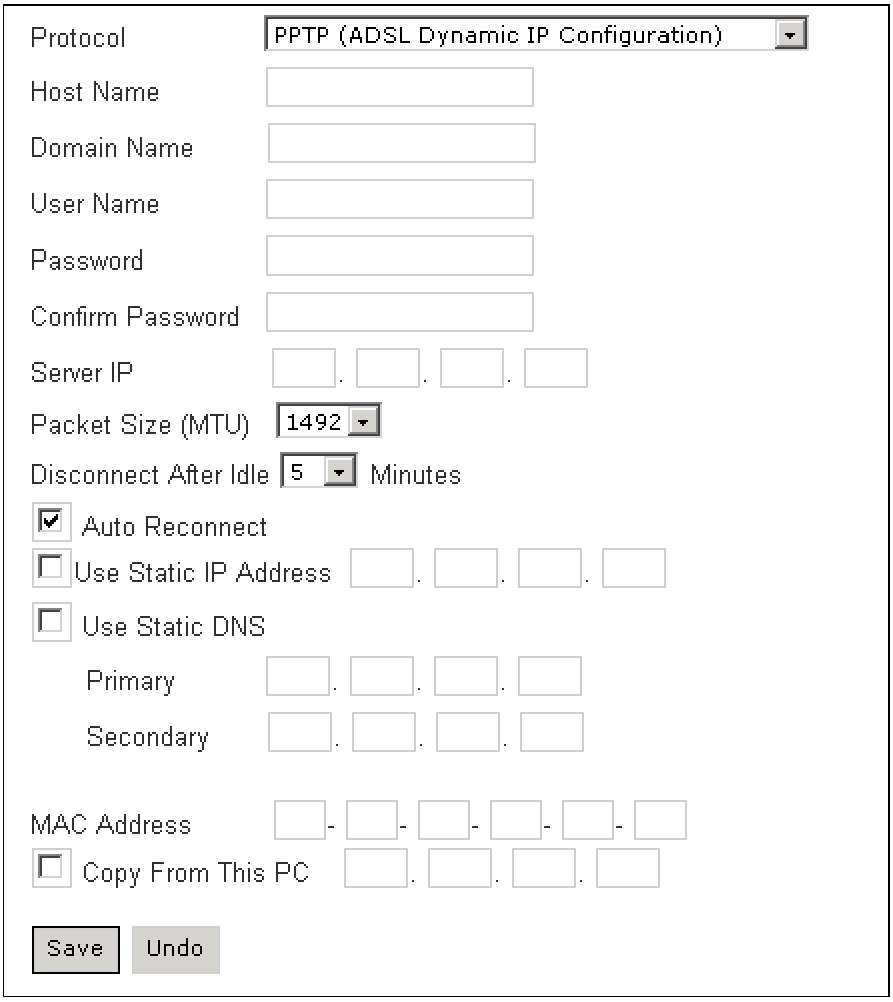
Disconnect after idle time. You can assign an idle time if there is no Internet traffic for the idle time you specified, the modem would be disconnected from the ISP by the gateway automatically. The gateway will reconnect your modem to the ISP when you start the Internet access again. The default value is 5 minutes, if you don’t want the gateway to disconnect your Internet connection automatically, please select 0 minute for permanent Internet connection.

Auto Reconnect. If the ISP dropped the connection, or the modem lost the connection accidentally, the gateway will reconnect your modem to the ISP immediately.

Use Static IP Address. If your ISP does not assign a dynamic address, you will use the static IP address, enter the IP address, subnet mask, and DNS address which your ISP assigned.

Use Static DNS. If you want to use your own DNS instead of ISP’s provision, check this box, and give the IP address of the DNS in the field. (At least one for the primary field.)

MAC address. Some ISPs allow you to connect to them with specified MAC address only, you can enter the MAC address manually or copy it from a PC which is attached to the Local Port, you just type in its IP address, the gateway will copy the MAC address from that PC. The gateway comes with the factory default MAC address, no need to change the default value if the ISP is not checking the MAC address of your Internet Port.



Protocol: PPTP (ADSL Dynamic IP Configuration)

Host Name

Domain Name

User Name

Password

Confirm Password

Server IP . . .

Packet Size (MTU) 1492

Disconnect After Idle 5 Minutes

☑ Auto Reconnect

□ Use Static IP Address . . .

□ Use Static DNS

Primary . . .

Secondary . . .

MAC Address - - - - -

□ Copy From This PC . . .

3.1.2 LOCAL PORT

Configure your gateway’s IP address of the local port here. It has to be a private IP address such as (10.x.x.x, 192.x.x.x are reserved for LAN use).

Subnet Mask. The subnet mask determines how many computers are allowed in this network. A class C network with the subnet mask 255.255.255.0 allows maximum 253 users (254-1, because gateway got one already) in your local area network. Usually a class C network is satisfactory for your local network.

To enable the **DHCP server** of the gateway, please click the check box.

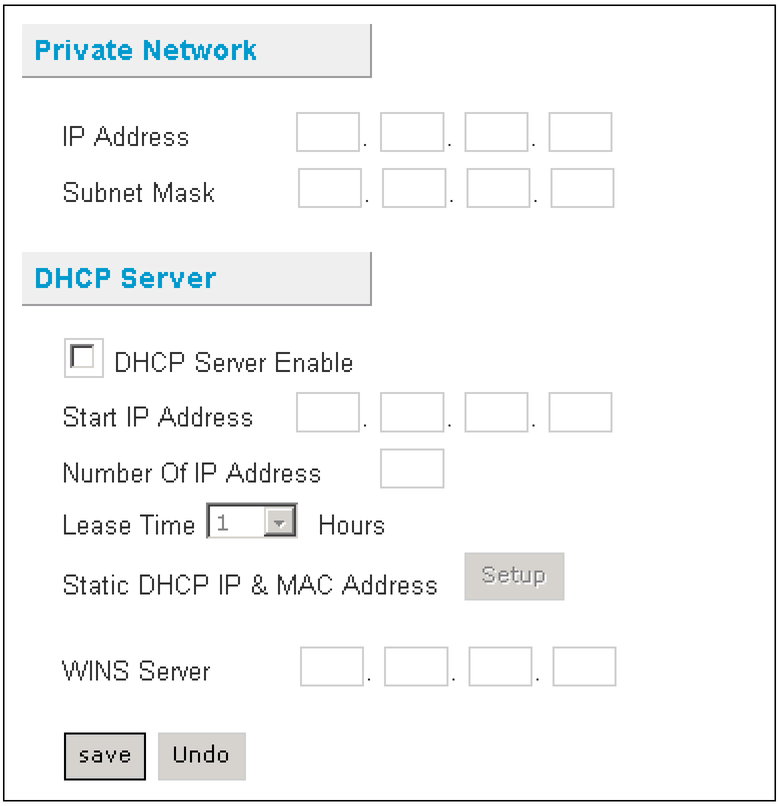
Start IP address. Specify the start of the IP address you want to assign to DHCP users. The default value is 192.168.1.2. (Please make sure there is no fixed IP address within your DHCP assignation range on the LAN, otherwise your DHCP client cannot get the IP address correctly.)

Number of IP address. Assign the number of users allowed to use the DHCP service. The default value is 128 users.

Lease Time. A DHCP user’s PC gets an IP address with a lease time, when the lease time is up the IP address assigned to that user’s PC will be expired. The user’s PC must connect to the DHCP server again to get a new IP address.

When there are lots of mobile users using DHCP service in your network, select an appropriate time to make sure you manage the IP addresses well, because when the user turns his computer off and leaves, the gateway might not be aware of that IP address is vacant, thus that IP address will be idle there until the lease time expired. The default value of the lease time is 168hours.

WINS Server. The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter WINS server's IP Address here. Otherwise, leave this blank.



Private Network

IP Address . . .

Subnet Mask . . .

DHCP Server

□ DHCP Server Enable

Start IP Address . . .

Number Of IP Address

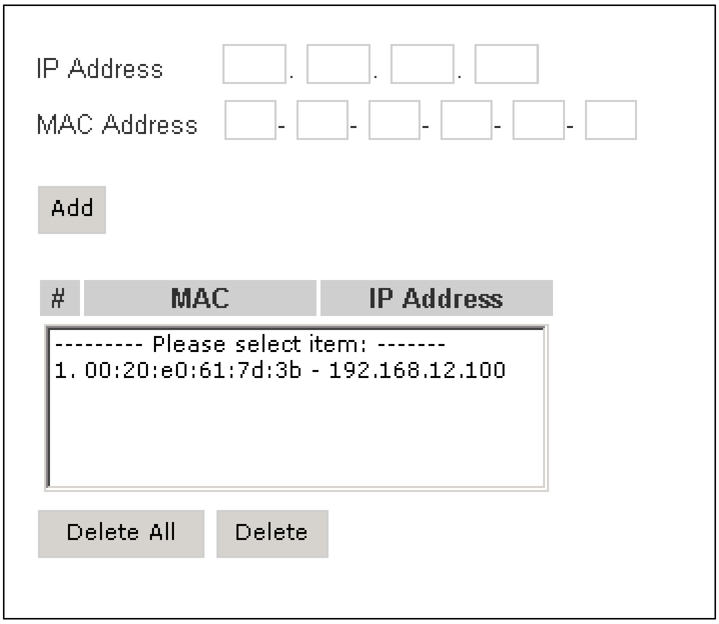
Lease Time 1 Hours

Static DHCP IP & MAC Address Setup

WINS Server . . .

save Undo

Static DHCP IP & MAC Address. Click Setup in the Local port configuration page to setup the Static DHCP IP. You can assign a fix IP to a computer for the DHCP server. Put the PC's IP address and MAC address in the fields and click add to add in the list. To delete one PC's IP address, please select it from the list then click Delete, or click delete all to delete all in the list.



IP Address ___ . ___ . ___ . ___

MAC Address ___ - ___ - ___ - ___ - ___ - ___

#	MAC	IP Address

```
--------- Please select item: -------
1. 00:20:e0:61:7d:3b - 192.168.12.100
```

3.1.3 Wireless LAN

Click **Enable Wireless Access** to enable the wireless function of the gateway.
SSID. (Service Set Identifier.) The SSID is the network name shared among all points in wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). For added security, you should change the default SSID to a unique name.

Hide SSID. The gateway will not broadcast the SSID, neither allows the SSID **Any** connecting to it. Hiding the SSID makes your wireless network more secured, unless the wireless user knows the SSID in advance, otherwise they cannot connect to the gateway.

Channel. Select an appropriate channel from the list. The default channel is 10. All devices in your wireless network must be set to the same channel as the gateway’s channel.

Operation Mode. The default value is 802.11b/g mixed mode. For the 802.11b/g mixed mode, you can use both 802.11b and 802.11g’s wireless network interface card to connect to it. If you need only one mode either 802.11b or 802.11g, please select from the pull down menu.

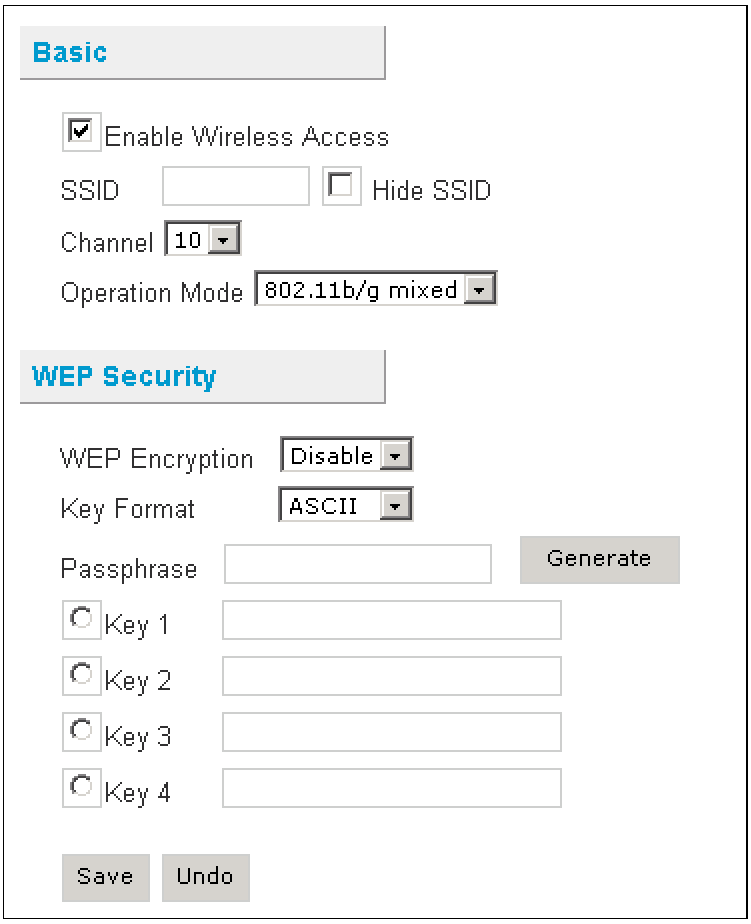
WEP Security. We strongly recommend you to use the WEP encryption to protect your local network. Otherwise the data might be stolen from your network easily if any other can get your wireless signals.

To enable the WEP, choose either 64bit or 128bit for encryption. The default value is Disable, this is for your convenience to connect to the wireless gateway at the first time. A 128bit encryption definitely has more safety than the 64bit encryption, but the 128bit encryption has a higher overhead over the wireless data transfer, it's a trade off, please choose an appropriate encryption for your network.

Key Format. The key format can be in ASCII that is easier to remember, or you can choose the HEX format from the pull down menu..

Passphrase. The gateway can help you to generate random keys, please input a phrase and click Generate. The keys will be generated automatically in the Key fields.

Key1-4. Click the radio button to decide which key to use for the wireless data encryption. The wireless network user's PC must assign to the same key as the gateway's current key.



Basic

☑ Enable Wireless Access

SSID □ Hide SSID

Channel 10

Operation Mode 802.11b/g mixed

WEP Security

WEP Encryption Disable

Key Format ASCII

Passphrase

3.2 Advanced Items

The advanced configurations allow you to manage your gateway safer and smarter.

3.2.1 Advanced Setup >> Access Control List

The Access Control List allows you to define Internet access rules for LAN users.

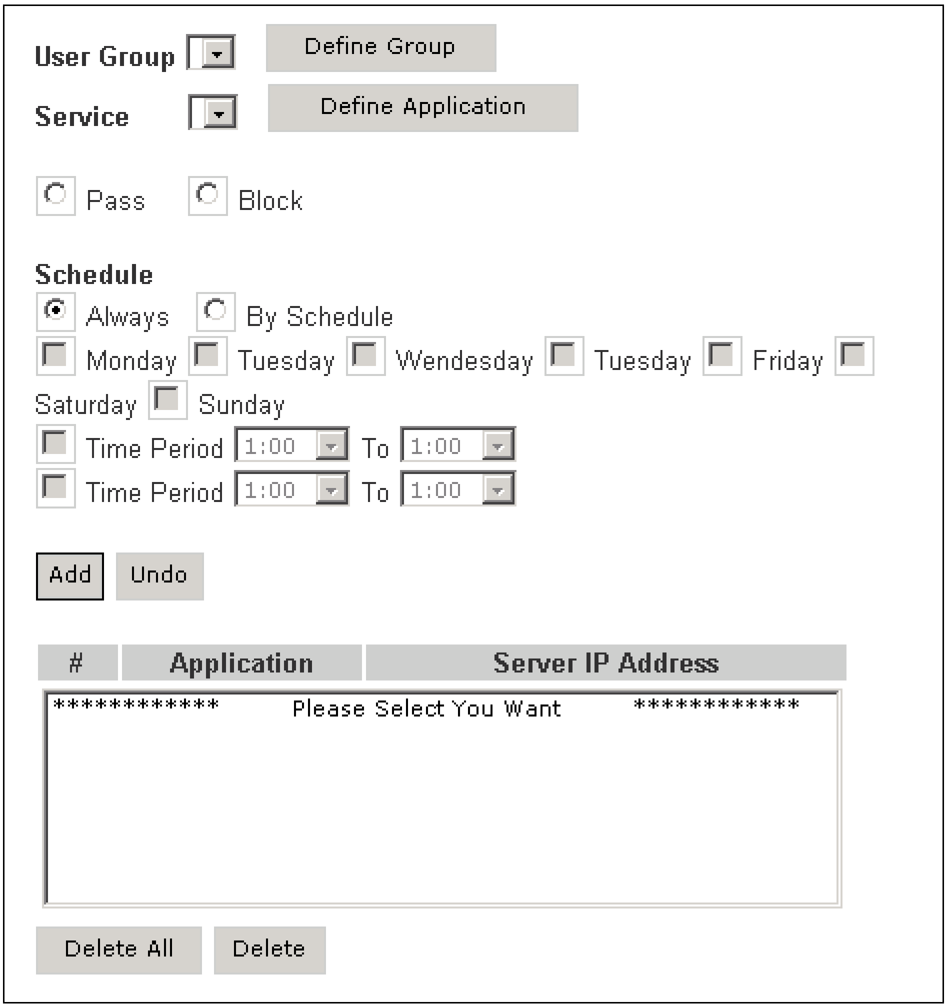
User Group. All LAN users can be defined into several groups, each group has different Internet access behavior depends on your configuration. To define the user group, click Define Group. (The Define Group is introduced below.)

Service. Select from the pull down menu, find the service you want to offer or block to the users. If you could not find the right service you need, please click Define Application. (The Define Application is introduced below.)

Forward / Block. Please click the radio button to decide this group user's access of the application to the Internet should be forwarded or blocked.

Schedule. The rules can be applied by schedule as you define here. The radio button Always means the rule is running all the time. By schedule-The rules are applied as the time and day you click below.
Monday thru Sunday. You can select one or more days you want the access control to be active.

When an access control rule is successfully added, it will be appended to list. Use the delete or delete all tabs to manage the control list.



User Group

Service

○ Pass ○ Block

Schedule

● Always ○ By Schedule

□ Monday □ Tuesday □ Wendesday □ Tuesday □ Friday □ Saturday □ Sunday

□ Time Period 1:00 To 1:00

□ Time Period 1:00 To 1:00

#	Application	Server IP Address

************ Please Select You Want ************

Define Group.

Group Name. Give a Group name for a group such as sales, R&D or accounting.

Click the radio button to choose the IP address you want to include for the group.

Every IP address. Selecting this will include all the IP address in your network.

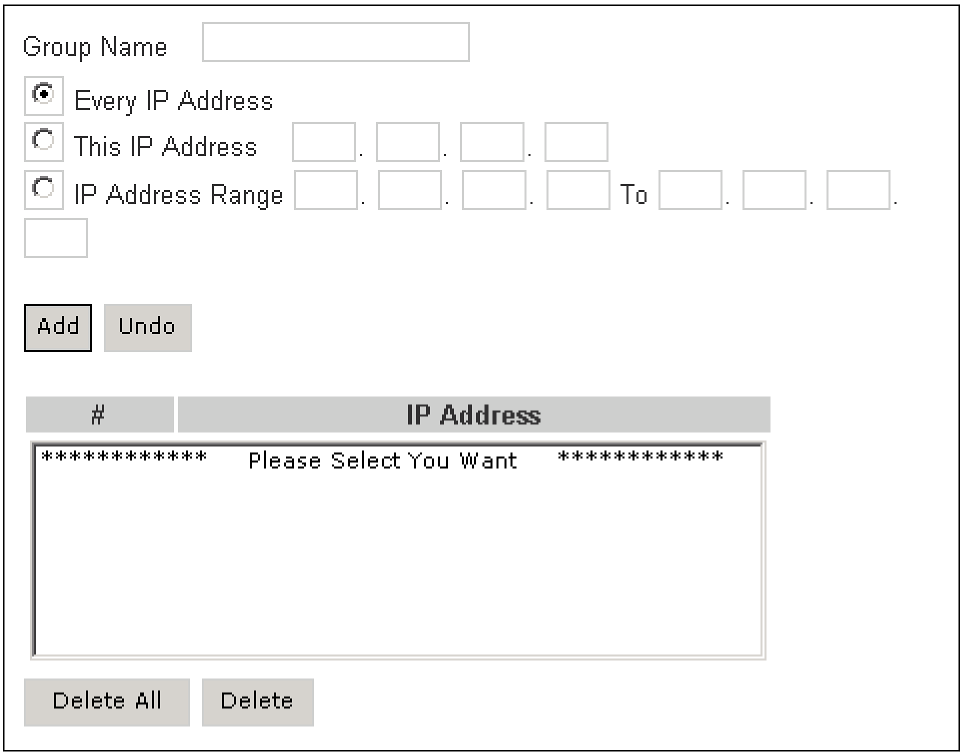
This IP address. Specify the IP address one at a time, type in the IP address you want to add in the fields.

IP Address Range. For a range of IP addresses, you need to specify the start and end IP address of the range in the fields.

Click Add to add your settings to the list, you can check all your IP address settings in this group by watching the list.

To delete an IP address from the list, click on that IP in the list, then click delete.

To delete all IP address in the list, click Delete All.


Group Name

● Every IP Address

○ This IP Address

○ IP Address Range . . . To . . .

#	IP Address
************ Please Select You Want ************	

After you have defined the user groups, return to the Access control list.

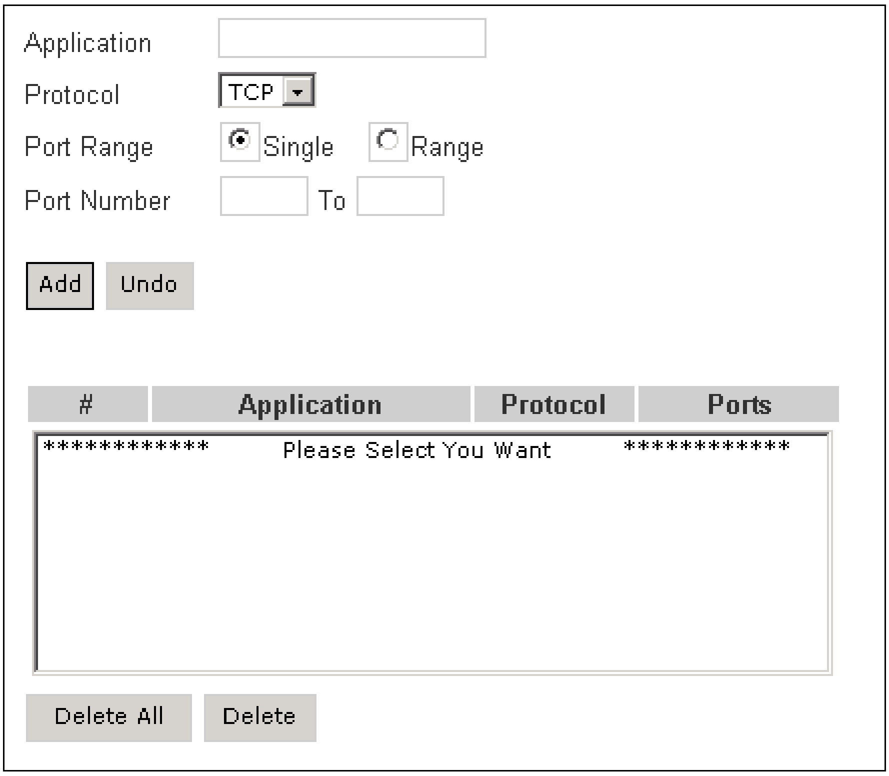
Define Application.

Application name. Give a name to the application you want to define.

Protocol. Select TCP or UDP for the protocol of the application.

Port Range. Define the port range, either **Single** or **Range** then put the port number in the fields. Click Add to finish the setting. You can check the applications you already defined in the list. Use the **delete** or **delete all** tabs to manage the list.

After you have defined your own applications, please return to the Access Control List menu, and choose from the pull down menu.



Application	
Protocol	TCP
Port Range	● Single ○ Range
Port Number	To

#	Application	Protocol	Ports

************ Please Select You Want ************

3.2.2 Advanced Setup >> Dynamic DNS

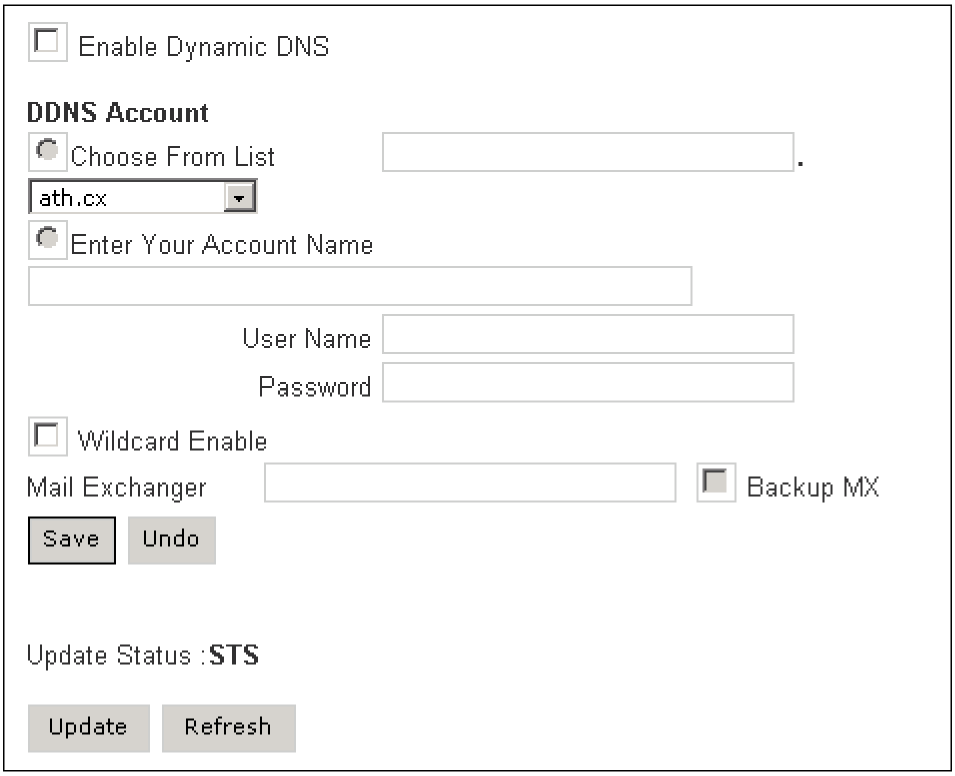
The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other servers behind the Gateway. Before you can use this feature, you need to sign up for DDNS service at www.dyndns.org or other DDNS service providers.

Enable Dynamic DNS. Check the box to enable the DDNS service.
DDNS Account. The **hostname** you want to use. Type the first part of the name in the input box, and select the second part of the name from the pull-down menu. This allows you to have anything.dyndns.org, anythingelse.homeunix.com, etc.
User Name, Password. These DDNS services require you to login, please enter the your name and password here.
Wild Card Enable. If you want anything_here.yourhost.dyndns.org to work (i.e. to make things like www.yourhost.dyndns.org work), check the Enable Wildcard box.
Mail Exchanger. If you wish to use a mail exchanger, put its hostname in the Mail Exchanger field.

Backup MX. If you need to backup the Mail Exchanger's address while you login to the DDNS service provider every time, please click the checkbox.

Update Status. The status of your DDNS service, please check the status of the DDNS service here, if you got an error message which is not the problem of your configuration, please contact your DDNS service provider. Please refer to the **Appendix E** for all Update Status messages.

Click the **Update** to check your current status of the DDNS service, or click **refresh** to refresh the web page display.



□ Enable Dynamic DNS

DDNS Account

○ Choose From List ______ .

ath.cx ▾

○ Enter Your Account Name

______

User Name ______

Password ______

□ Wildcard Enable

Mail Exchanger ______ □ Backup MX

Update Status :**STS**

3.2.3 Advanced Setup >> Firewall

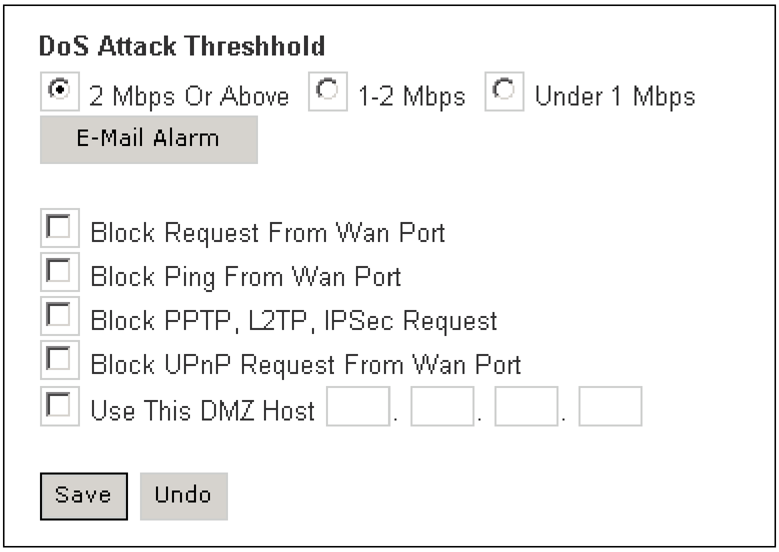
DoS Attack Threshold. When the gateway suffers a continuous attack from the Internet (Which is not a regular connection, usually they are lost of connection requests at a time to consume or exhaust the memory of the gateway.) The gateway will drop the traffics from the attack sources instead of treating them like normal traffics. Please select your own threshold bandwidth from the attack source on the Internet by clicking the radio button. (Normally when you have a smaller bandwidth to the Internet, you will have a correspondently smaller DoS Attack Threshold. Otherwise the DoS function will not work properly.)

Block Request from WAN Port. Block request from WAN port feature reinforces your network security by hiding your network ports; this makes it difficult for others to intrude into your network. This feature is enabled by default. But if you host servers on your LAN, you cannot enable this feature, otherwise the users from the Internet cannot reach your servers on the LAN.

Block Ping from WAN port. This feature can prevent your network from being “pinged”, or detected by other Internet users.

Block PPTP, L2TP, IPSec Request. This feature blocks all VPN connection requests from the hosts outside your network.

Use the DMZ host. The DMZ feature allows one local network user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ forwards all the ports to this computer.



DoS Attack Threshhold

● 2 Mbps Or Above ○ 1-2 Mbps ○ Under 1 Mbps

□ Block Request From Wan Port
□ Block Ping From Wan Port
□ Block PPTP, L2TP, IPSec Request
□ Block UPnP Request From Wan Port
□ Use This DMZ Host ___ . ___ . ___ . ___

Email Alarm

The E-mail alarm feature enables you to receive the access log through e-mails regularly. Click the checkbox, if you want to receive the e-mails from the gateway.

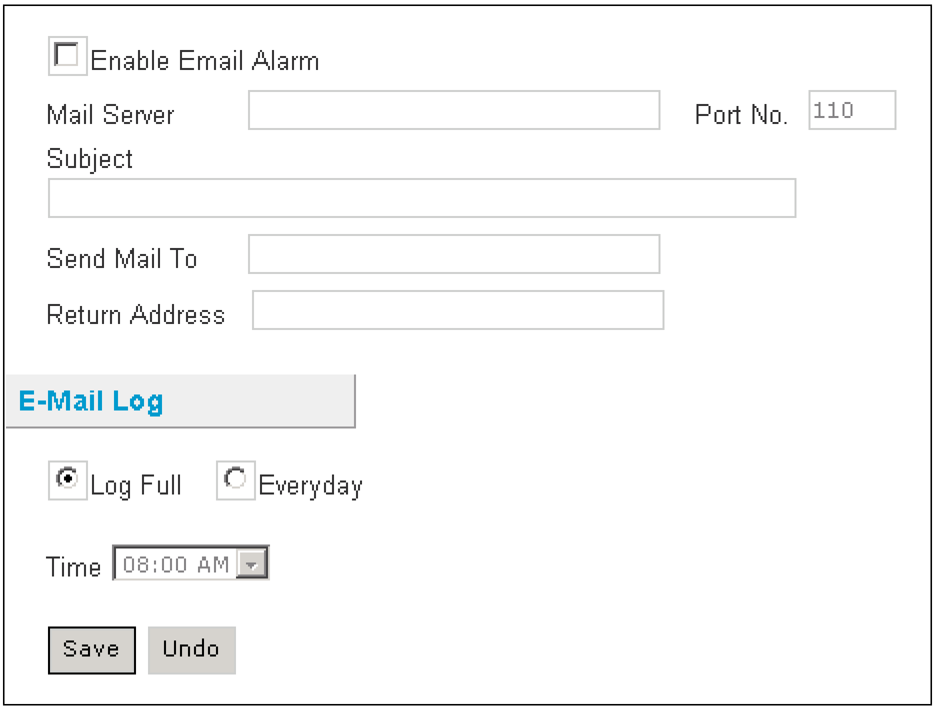
Mail Server. This is the e-mail server address on your network or on the Internet. The mail server should relay your mails without user name and password login. Otherwise, the mails cannot be sent out. The standard SMTP port for sending e-mails is 110; if you have special settings, otherwise lease it as default.

Subject. The subject will appear as the subject of the e-mails that gateway sent you. So the user can tell by the subject which mail is from the gateway.

Send mail to. Please enter your e-mail address or the e-mail address you want the gateway send to.

Return address. If your gateway cannot send to the receiptant successfully or the users want to reply a message from the mail, this is the address to reply.

E-mail log. You can specify the behavior of the gateway sending the e-mail logs. By clicking the radio button log full, the alarm e-mails will be sent only when the log of the gateway is full. The other option Everyday, the gateway will send e-mails daily weather there is message or not.
Time. Please specify the time you like the gateway to send alarm mails everyday.



☐ Enable Email Alarm

Mail Server

Port No. 110

Subject

Send Mail To

Return Address

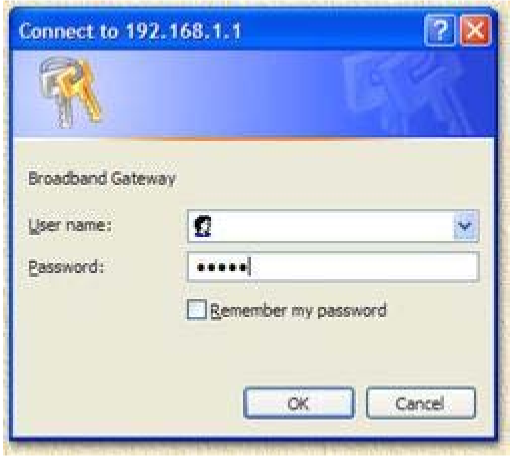
E-Mail Log

● Log Full ○ Everyday

Time 08:00 AM

3.2.4 Advanced Setup >> Remote Management

User Name, Password, Confirm Password. You can change the user name and password here. Type in your new user name, password and confirm it again, then click save to change the username and password. Please use passwords more than 6 characters and no simple phrases. After you changed the user name and password, the gateway will require you to login with the new user name and password immediately.
It is strongly recommended you change the user name and password from the default value to your own setting when your first access to the gateway. Otherwise, the default value is easy for unauthorized person to login.



Connect to 192.168.1.1

Broadband Gateway

User name:

Password: •••••

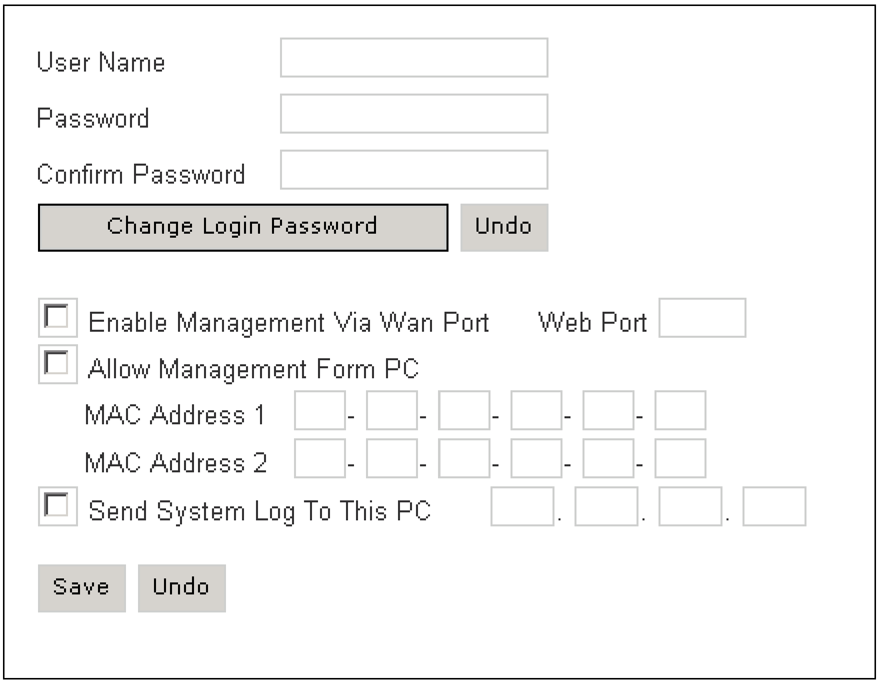
□ Remember my password

Enable Management from WAN port. The remote management can be enabled or disabled by clicking the checkbox. When enabled the user from the Internet can configure the gateway via the web.

Web Port. The well-known port of the web is 80; if you have your own web site on your LAN for Internet access, please assign another number that is unique to your virtual server settings.

Allow Management From PC. Check the box you can restrict management access from the LAN, only the PC with the MAC address you specified here can manage the gateway. If you keyed in with wrong MAC and saved accidentally, your PC might lose access right to the gateway. Please press the reset button (on the rear side of the gateway) for 5 seconds to restore the gateway to factory default value.

Send System Log To this PC. The gateway will send the system logs to the PC with the IP address specified here.



User Name

Password

Confirm Password

□ Enable Management Via Wan Port Web Port

□ Allow Management Form PC

MAC Address 1 - - - - -

MAC Address 2 - - - - -

□ Send System Log To This PC . . .

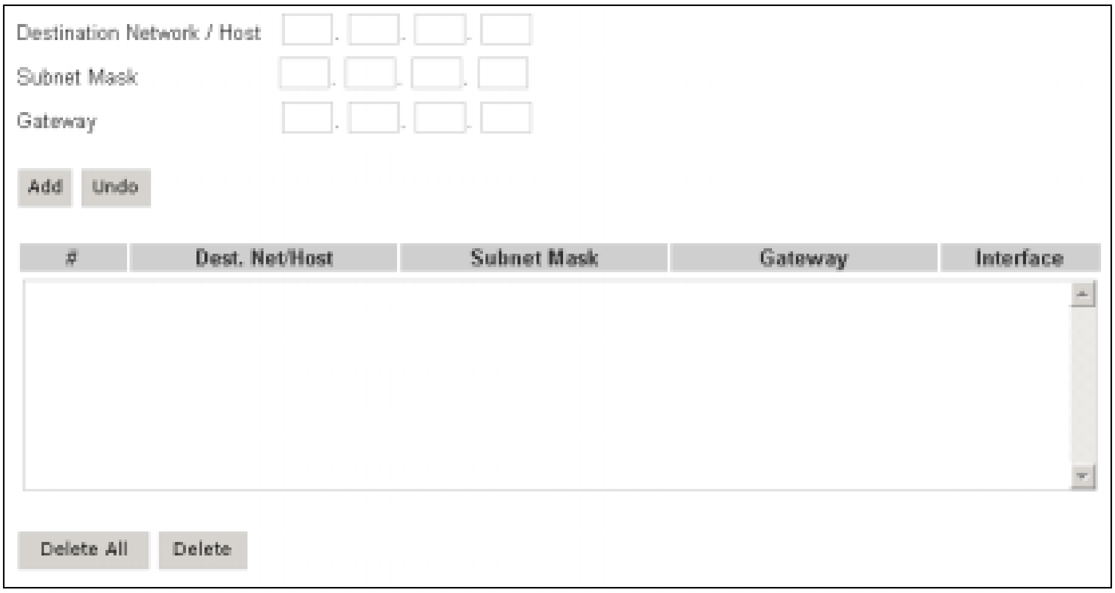
3.2.5 Advanced Setup >> Static Routes

When you have more than one network on your LAN, and you want to route certain IP addresses of network to another network, add them in the static routes.

Destination Network / Host. The destination network is the address of the remote network or host you to which you want to assign a static route.

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

Gateway. This is the IP address of the gateway device that allows for connection between the Router and the remote network or host.



Destination Network / Host . . .

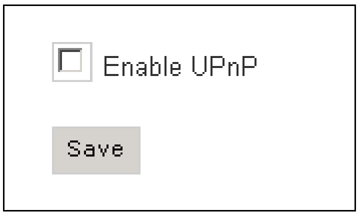
Subnet Mask . . .

Gateway . . .

#	Dest. Net/Host	Subnet Mask	Gateway	Interface

3.2.6 Advanced Setup >> UPnP

UPnP is a function that allows the gateway to self-discover, self configure and communicate easily with one another. To enable UPnP click the checkbox.



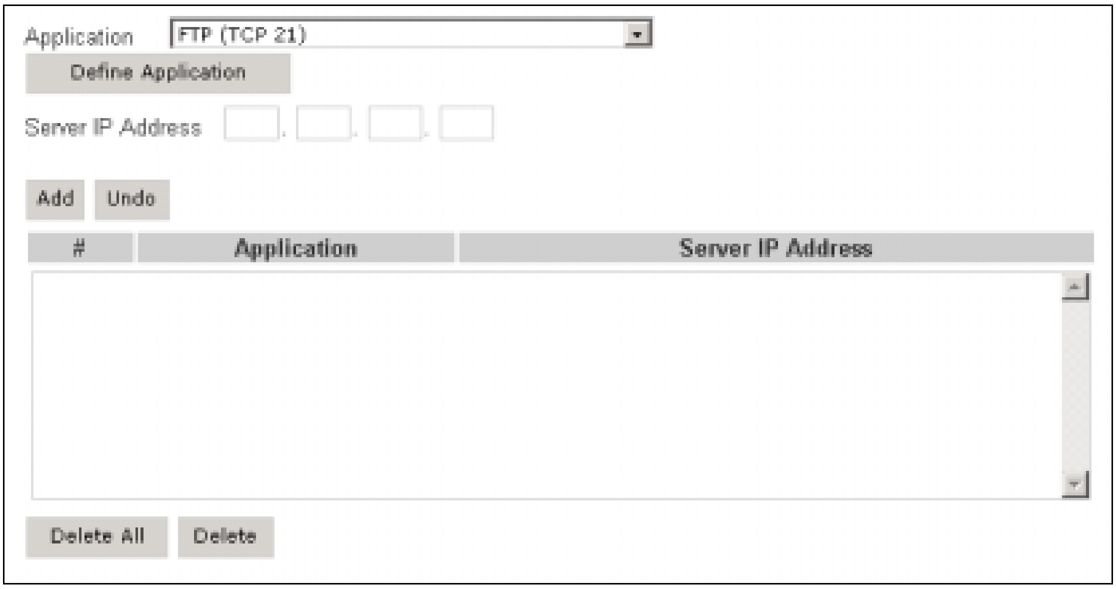
□ Enable UPnP

3.2.7 Advanced Setup >> Virtual Server

The virtual server allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

Application. Choose the application in the pull down menu, if you cannot find the applications you want in the list, please click Define Application to define on your own.

Server IP address. Input the server address for the application you selected above. Then click Add to proceed. After a successful adds, it will be shown in the list.



Application FTP (TCP 21)

Server IP Address . . .

#	Application	Server IP Address

Define Application

Some applications need specified ports opened for Internet connection, such as games, Instant Messengers and so on.

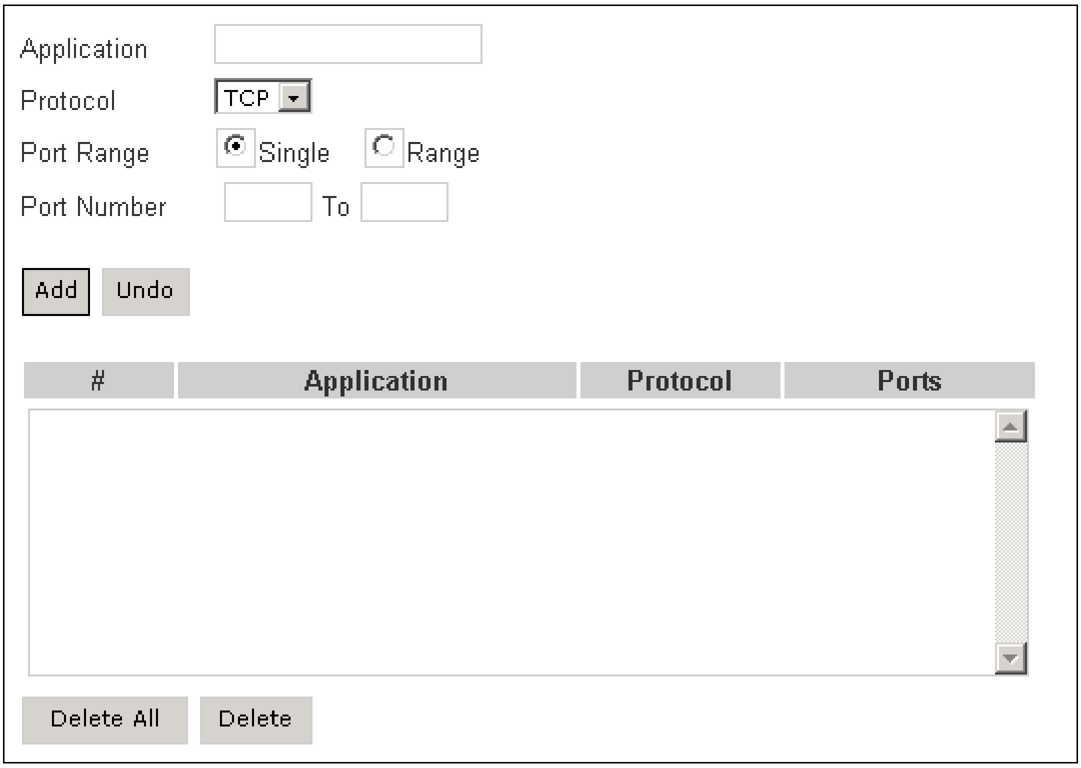
Application. Type in the application name that is easy to remember.

Protocol. TCP or UDP, if you are not sure, check manuals of the application.

Port Range. Choose Single if there is one port to be opened, or choose Range for a range of port numbers.

Port Number. Type in the Port number or a Port range.

Click Add to finish your setting, it will be shown on the list.



Application

Protocol: TCP

Port Range: ● Single ○ Range

Port Number To

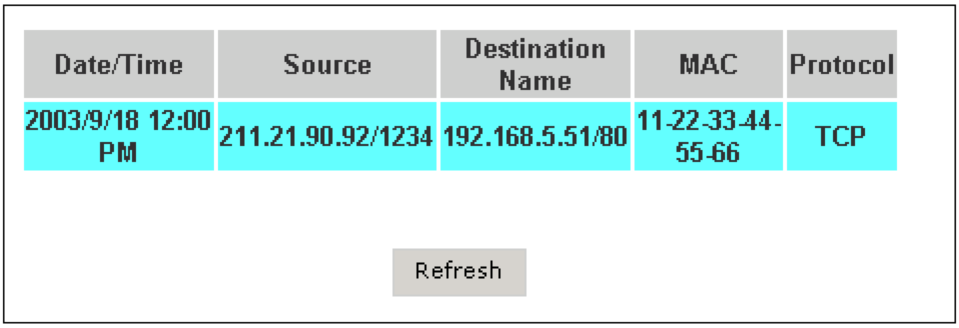
#	Application	Protocol	Ports

3.3 Management

These management items help you to manage your gateway well.

3.3.1 Management >> Access Log

The Access Log allows you to browse the gateway's traffic of a period of time and log the records in files for reference (Need an access log software? please see **APPENDIX F SYSLOG SOFTWARE**). Click refresh button to renew the list for the most current records.



Date/Time	Source	Destination Name	MAC	Protocol
2003/9/18 12:00 PM	211.21.90.92/1234	192.168.5.51/80	11-22-33-44-55-66	TCP

3.3.2 Management >> Factory Reset

Click the button to set all configurations to factory default.

The default values are:

User Name: admin

Password: admin

Internet Port: DHCP.

Local port address: 192.168.1.1

Subnet mask: 255.255.255.0

DHCP server: enable

DHCP start address: 192.168.1.2

Number of DHCP clients: 128

Wireless: Enabled

SSID: XAVi

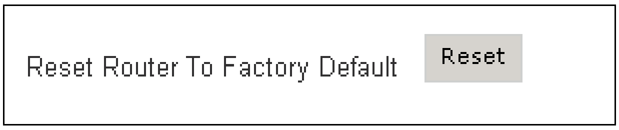
Channel: 10

Operation Mode: 802.11b/g mixed

WEP security: No

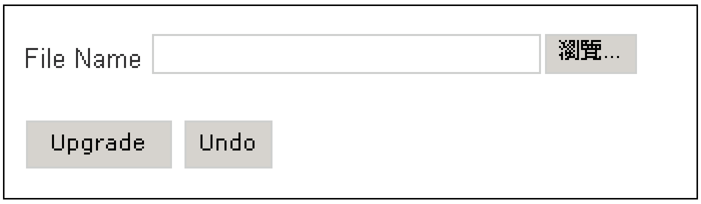
Remote Management: Enabled

UPnP: Enabled



3.3.3 Management >> Firmware Upgrade

Firmware can be upgraded by clicking the **Upgrade** button after browsing for the firmware, which you can download from the XAVi website. Do not upgrade your firmware unless you are experiencing problems with the gateway. After a successful upgrade, the modem will reboot by itself, you current page will be brought back to the first page of the configuration.

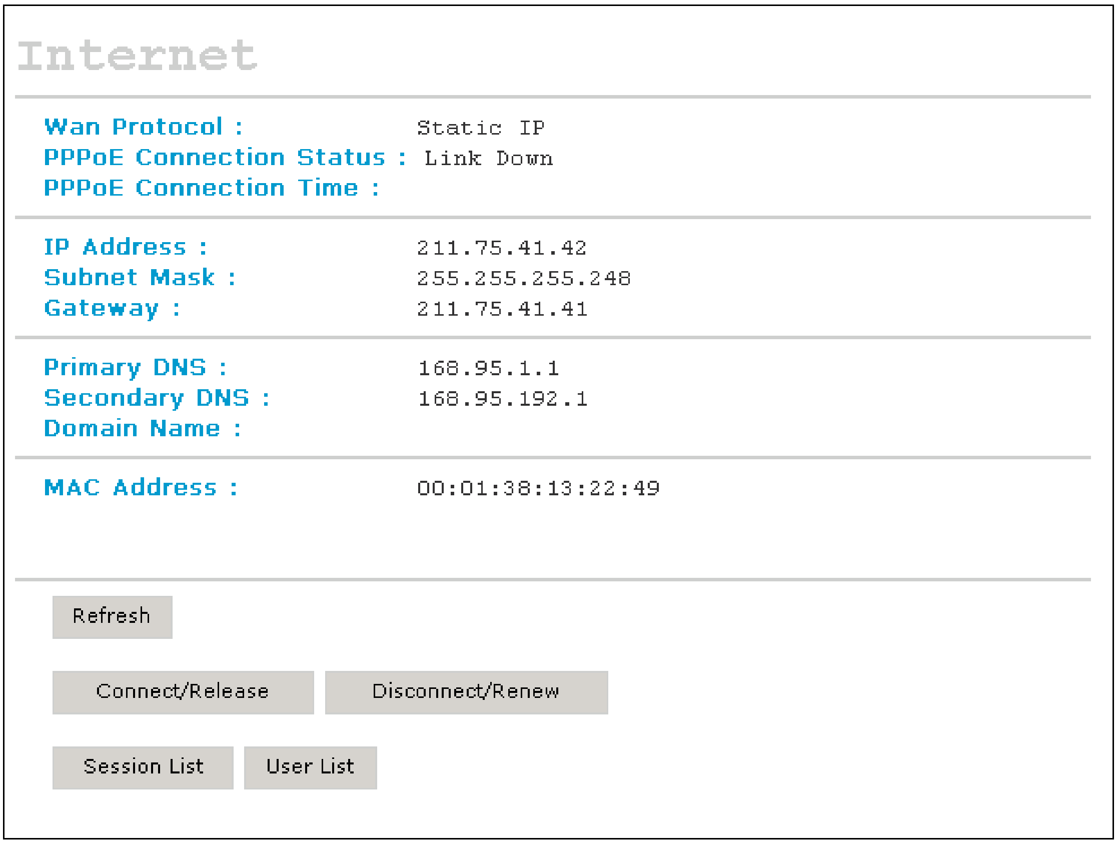


3.3.4 Management >> Network Status

The network status shows the service type, IP address, Subnet mask, Gateway, DNS and MAC address of your WAN. Click Refresh to display the latest information.

When using PPPoE, PPTP, you can click Connect/Release to establish the connection of the Internet port. Click Disconnect/Renew to break the Internet port connection.

When using DHCP, please click Connect/Release to release your current IP address, click Disconnect/Renew to get a new IP address from the DHCP server.

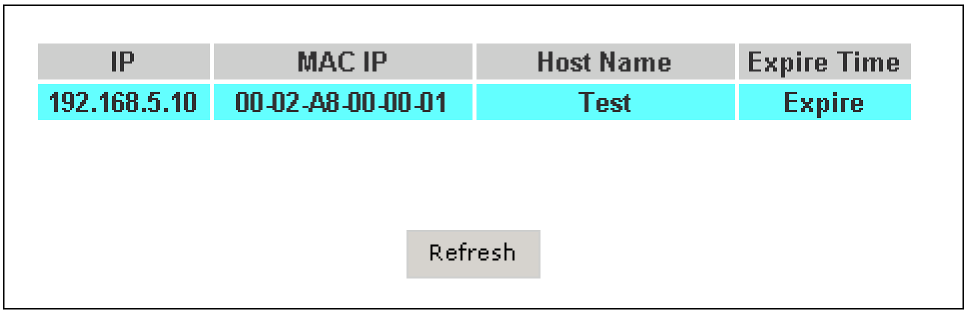


Internet

```
Wan Protocol :                 Static IP
PPPoE Connection Status :      Link Down
PPPoE Connection Time :

IP Address :                   211.75.41.42
Subnet Mask :                  255.255.255.248
Gateway :                      211.75.41.41

Primary DNS :                  168.95.1.1
Secondary DNS :                168.95.192.1
Domain Name :

MAC Address :                  00:01:38:13:22:49
```

User List

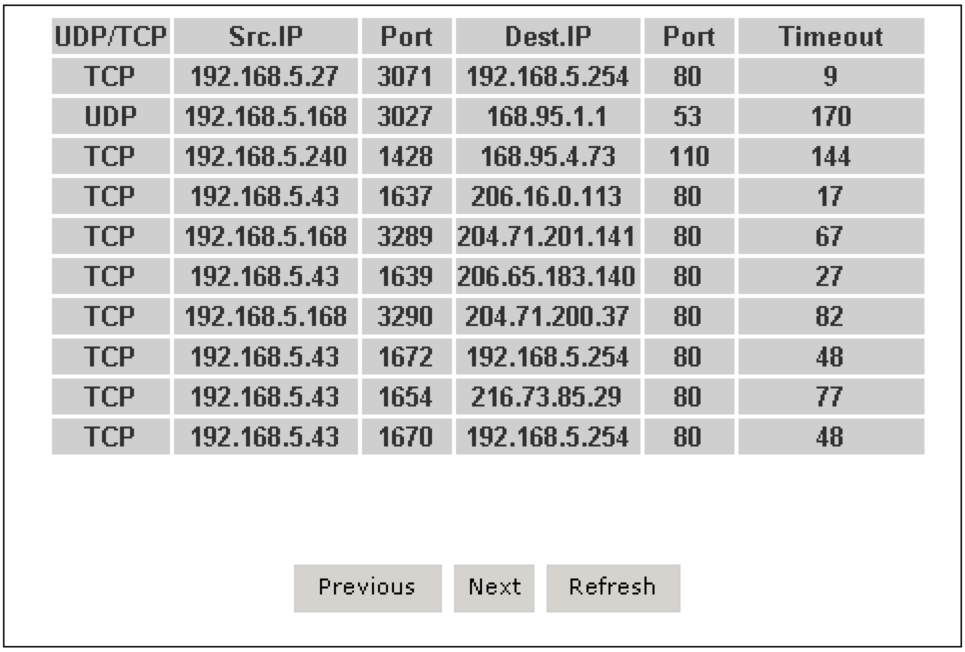
The user list shows users who are using the DHCP service, and their IP address, MAC address, Host name and the time to the expiration time of that leased IP address. Click Refresh to update the latest users list.



IP	MAC IP	Host Name	Expire Time
192.168.5.10	00-02-A8-00-00-01	Test	Expire

Session List

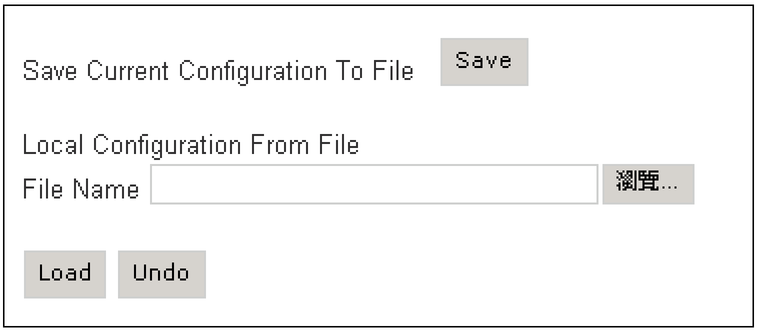
List the sessions currently established. By watching the session list, you will observe that who are using the Internet service, what type of services and the other information you need. The session list also helps you to debug the Internet connection problem. Click **previous** or **next** to browse the whole list.



UDP/TCP	Src.IP	Port	Dest.IP	Port	Timeout
TCP	192.168.5.27	3071	192.168.5.254	80	9
UDP	192.168.5.168	3027	168.95.1.1	53	170
TCP	192.168.5.240	1428	168.95.4.73	110	144
TCP	192.168.5.43	1637	206.16.0.113	80	17
TCP	192.168.5.168	3289	204.71.201.141	80	67
TCP	192.168.5.43	1639	206.65.183.140	80	27
TCP	192.168.5.168	3290	204.71.200.37	80	82
TCP	192.168.5.43	1672	192.168.5.254	80	48
TCP	192.168.5.43	1654	216.73.85.29	80	77
TCP	192.168.5.43	1670	192.168.5.254	80	48

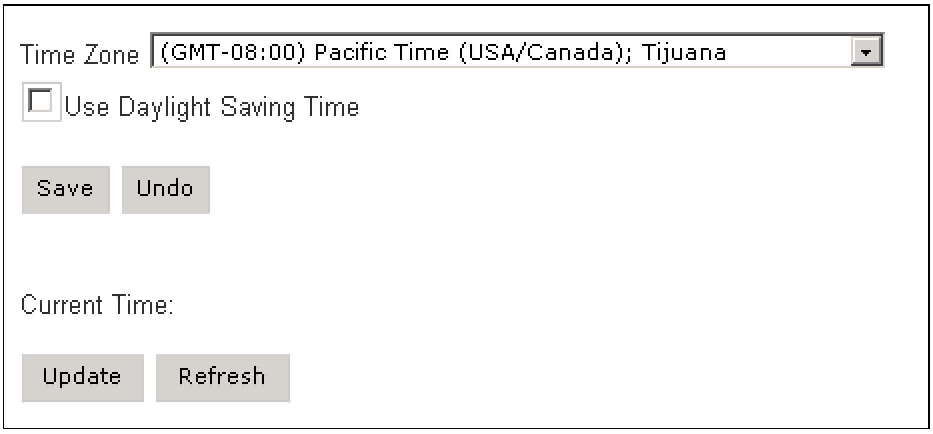
3.3.5 Management >> Save Configuration

To save your current configuration to files in your PC, click the Save button, the system will prompt you to save the configuration file, click save to proceed. To load a backup configuration file from the PC, click browse and choose the path and the file, then click load to proceed. After a successful load, please restart your gateway by unplugging the power then plugging back in.


Save Current Configuration To File
Save
Local Configuration From File
File Name
瀏覽...
Load
Undo

3.3.6 Management >> Time

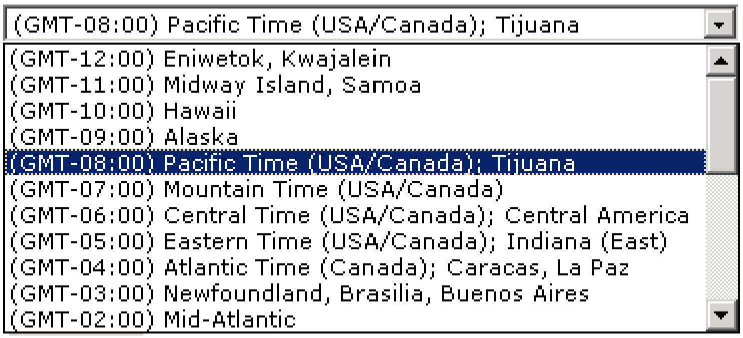
Change the time zone to the area you are in. The default value is the **GMT-8.00 Pacific Time (USA/Canada)**. When in daylight saving period, please check the **Use Daylight Saving Time** box.



Time Zone (GMT-08:00) Pacific Time (USA/Canada); Tijuana

□ Use Daylight Saving Time

Current Time:



(GMT-08:00) Pacific Time (USA/Canada); Tijuana

(GMT-12:00) Eniwetok, Kwajalein
(GMT-11:00) Midway Island, Samoa
(GMT-10:00) Hawaii
(GMT-09:00) Alaska
(GMT-08:00) Pacific Time (USA/Canada); Tijuana
(GMT-07:00) Mountain Time (USA/Canada)
(GMT-06:00) Central Time (USA/Canada); Central America
(GMT-05:00) Eastern Time (USA/Canada); Indiana (East)
(GMT-04:00) Atlantic Time (Canada); Caracas, La Paz
(GMT-03:00) Newfoundland, Brasilia, Buenos Aires
(GMT-02:00) Mid-Atlantic

Appendix A. TECHNICAL SPECIFICATIONS

Specifications

■ Standard IEEE 802.3, 802.3u, 802.11g and 802.11b

■ Channels 11 Channels: US, Canada
13 Channels: Europe
14 Channels: Japan

■ Access Interface

- WAN: One 10/100 Base TX port, Auto sensing, Auto MDIX, RJ-45 connector
- LAN: Four 10/100 Base TX ports, Auto sensing, Auto MDIX, RJ-45 connector

- Wireless: External Antenna, Frequency: 2.412~2.484 GHz, support 14 channels, data rates supports 6, 9, 12, 18, 24, 36, 48 and 54 Mbps auto fallback function,

■ LED Indicators

- PWR: Green LED, indicates power and operation
- DIAG: Green LED, indicates hardware abnormal operation
- LAN 10/100: indicates LAN port connection, yellow, 10Mbps, green, 100Mbps
- WAN 10/100: indicates ISP connection
- WLAN : Green LED, indicates Wireless LAN function

■ Reset Button (Factory default-setting button)

■ Environment

- Operation Temperature: 0°C ~ 45°C
- Operation Humidity: 5% ~ 95%
- Storage Temperature: -20~+85°C
- Storage Humidity: 5%~95%

■ Power

- AC Adapter: Input 110VAC/220VAC; Output 12V/1A DC
- Maximum power consumption: 10 Watts

■ Dimensions & Weight

- 180mm x 143mm x 40.5mm (W x D x H)
- ?? g without holder

■ Certificates

- EMI: CE & FCC Part 15 class B
- Safety: CB (EN60950)

Appendix B Frequent Asked Questions

Q: When should I modify the MAC address for global port settings?

A: Some ISPs identify their clients by the accessing MAC address and the host names, therefore, entering these information is the process required to prove they are who they claim to be. MAC address required for global port settings is the adapter address for the device you are now configuring. Most ISPs use automatic registration and do not limit network MAC addresses. But, if they do, you can change your MAC address to meet the registration.

Q: What is DMZ?

A: DMZ (demilitarized zone), a barrier between the Internet and a company's Intranet. It is a subnet that contains a firewall and proxy server, which can be in separate servers or in one server. The firewall connects to an external firewall on the Internet side, which may be at the ISP's location and is often called a "boundary router". The double firewall architecture adds an extra measure of security for the Intranet.

Q: What is Dynamic DNS?

A: The Dynamic DNS service, an IP Registry provides a public central database where information such as email addresses, hostnames, Ips etc. can be stored and retrieved. This solves the problems if your DNS server uses an IP associated with dynamic IP. The Dynamic DNS service acts like old-style phone operators: other users call the operator, and ask to speak to you, and the operator, who knows your extension, will make the connection. Every time your computer comes online, it will inform the Dynamic DNS server what the current IP address is. Users who need to connect to your server, through the magic of DNS service, will be sent to the right place. Please visit http://www.dyndns.org for more information.

Q: Why "Dynamic DNS"?

A: With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register with a Dynamic DNS Client to sue this service. Please go to http://www.dyndns.org for more information.

Q: What is Wildcard?

A: A wildcard alias is a method that is used to give your hostname multiple identities. If you were to register yourhost.com, everything (*).yourhost.com would be aliased to yourhost.com. This includes host names such as www.yourhost.com or ftp.yourhost.com . Once Wildcard feature was enabled, your host can be reached by *.yourhost.dyndns.org. First, you need to register a dynamic DNS account with www.dyndns.org. To use this service, you must register with the Dynamic DNS client. The Dynamic DNS client service provider will give you a password or key. Refer to what's Dynamic DNS? Question above for more information.

Q: What's MX (Mail Exchanger)? And why MX?

A: The Internet email system for both machines and network connections are prone to error. With this, a chain of email hubs into the email architecture is thus built. If the "primary" mail host goes down, instead of queuing up the mails in the unreliable host on the Internet, they get sent to the "secondary" or “backup” mail exchanger for delivery, until the primary mail server becomes functional again. In technical term, such service is called Backup Mail Exchanger.

Q: What is PPPoE (PPP Over Ethernet)?
A: PPPoE is know as a dial-up DSL service. It is designed to integrate the broadband services into the current widely deployed, easy-to-use, and low-cost dial-up-access networking infrastructure. Thus, customer can get greater access speed without changing the operation concept.

Q: What is MTU?
A: A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet. The Internet's Transmission Control Protocol uses the MTU to determine the maximum size of each packet in any transmission. Too large an MTU size may mean retransmissions if the packet encounters a router that can't handle that large a packet. Too small an MTU size means relatively more header overhead and more acknowledgements that have to be sent and handled. Most computer operating systems provide a default MTU value that is suitable for most users. In general, Internet users should follow the advice of their Internet service provider (ISP) about whether to change the default value and what to change it to.

Appendix C Troubleshooting

This chapter is intended to help you troubleshoot problems you may encounter while setting up and using the XAVi route. It also describes some common hardware and software problems and gives some suggestions to troubleshoot them.

Refresh your IP address (MS Windows)
Sometimes you will wonder what my computer’s IP is or you want to refresh your IP address. There is a tool for this comes with Windows. For Windows 95/98/98se/ME, please click **Start > Run**, enter **winipcfg** and click **OK**. Select the correct Network Adaptor, click **release all** to release all current configuration first, then click **renew all** to renew the IP information again.

For Windows NT4.0/2000/XP, run **ipconfig.exe** in DOS mode. (**ipconfig.exe/?**

to list all parameters). Run **ipconfig /release** and then run **ipconfig /renew**.

IP address conflict

When you see the message box prompted for IP address conflict on any of the workstations in the network, this means two or more workstations have the same IP address. If you have setup the device as a DHCP server, on the problem workstation, please run the "winipcfg", utility, select the correct Network Adapter, click release all to release all current configuration first, then click renew all to renew the IP information again (for Windows 2000/NT4.0/XP, run ipconfig/release and then run ipconfig /renew). If the DHCP function is disabled and static IP addresses are assigned to each workstation, please double check each workstation's IP address for any duplicate IP.

Cannot access the Internet

- Check the physical connectivity of local network.
- Check if both the LEDs of local and Global on the product's front panel are lit. Make sure you are using the correct cables and the cables are connected to the network devices properly.
- Check the physical connectivity of broadband device.
- Examine the LED of LAN port and the LED of the broadband signal input on the Cable Modem/xDSL Modem. If the LAN LED is off, make sure you are using the correct cables and the cables are connected to the devices properly. If the LED of the broadband signal is off, please contact your ISP.
- Check the status of this product.
- After checking the cabling, you also have to check if you have entered the correct user name and password that your ISP provided. While checking, please note that the information is case sensitive.
- To check the Internet connection status, open the browser to start the web configuration, select **Network Status > WAN IP Status**. Check if Link Status displays "Connect successfully". If not, you may have to contact your ISP to see if their Internet service is available.
- Check the logical connectivity from your computer to the Internet.

Appendix D Government compliance notices

FCC compliance

This equipment complies with Part 15 of the FCC Rules. On this equipment is a label that contains, among other information, the FCC registration number and Ringer Equivalence Number (REN) for this equipment. You must, upon request, provide this information to your telephone company.

This equipment has been tested and found to comply with the limits for a Class A digital devices, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communication.

Operation of this equipment in residential area is likely to cause harmful interference in which case the will be required to correct the interference at this own expense. The user should not modify or change this equipment without written approval from company name. Modification could void authority to use this equipment.

For the safety reason, people should not work in a situation which RF exposure limits be exceeded. To prevent the situation happening, people who work with the antenna should be aware of the following rules:

1. **Install the antenna in a location where a distance of 20cm from the antenna may be maintained.**
2. **While installing the antenna in the location, please do not turn on the power of wireless card.**
3. **While the device is working, please do not contact the antenna.**

APPENDIX E DDNS UPDATE STATUS MESSAGES

(1) When starting the DDNS service.
Updating dynamic DNS server, please wait.

(2) When DHCP Client or PPPOE cannot get IP on the Internet Port.
Could not resolve IP address for the device.

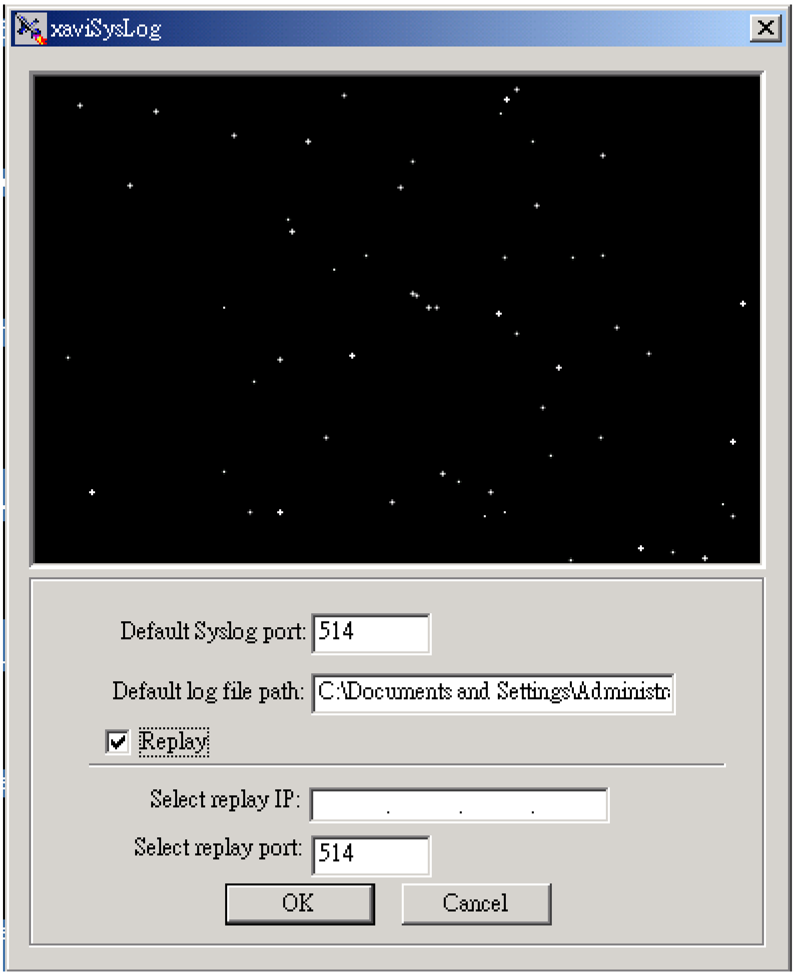
(3) When DDNS update successful.
Update dynamic DNS server successful IP: <Your Internet IP address> (eg. 211.21.190.99)

Update dynamic DNS server successful IP: <Your Internet IP address> (eg. 211.21.190.99) again.
Update successful, a feature requested is only available to donators, please donate.

(4) When DDNS update fail.
Update fail, cannot connect to server: members.dyndns.org
Update fail, strange server response.
Update fail, invalid hostname: user.dyndns.org .
Update fail, malformed hostname: user.dyndns.org .
Update fail, hostname: user.dyndns.org is not under your control.
Update fail, hostname: user.dyndns.org has been blocked for abuse. You need to be logged in dyndns.org.
Update fail, invalid username and password.
Update fail, invalid parameter.
Update fail, this user agent has been blocked.
Update fail, too many or too few hosts found.
Update fail, dyndns internal error, please report this number to their support people: error message.
Update fail, 911!
Update fail, 999!
Update fail, wait response received, waiting for 60 seconds before next update.
Update fail, error processing request
Update fail, invalid username and password!
Update fail, server response: server message.

APPENDIX F SYSLOG SOFTWARE

The XAVi Syslog Program is on the CD which comes with the gateway.
You do not have to install it, just copy it to your PC and double click it to run the program.
You will see the first page.



xaviSysLog

Default Syslog port: 514

Default log file path: C:\Documents and Settings\Administr

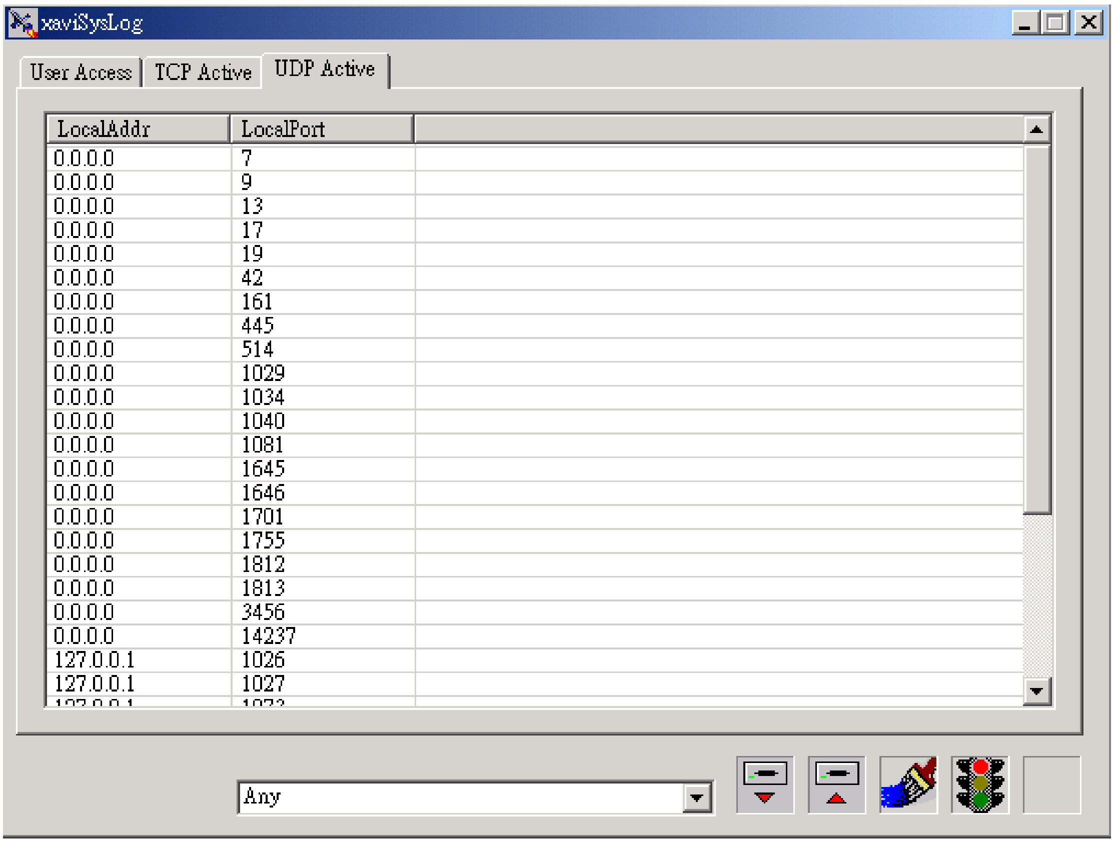
☑ Replay

Select replay IP: . . .

Select replay port: 514

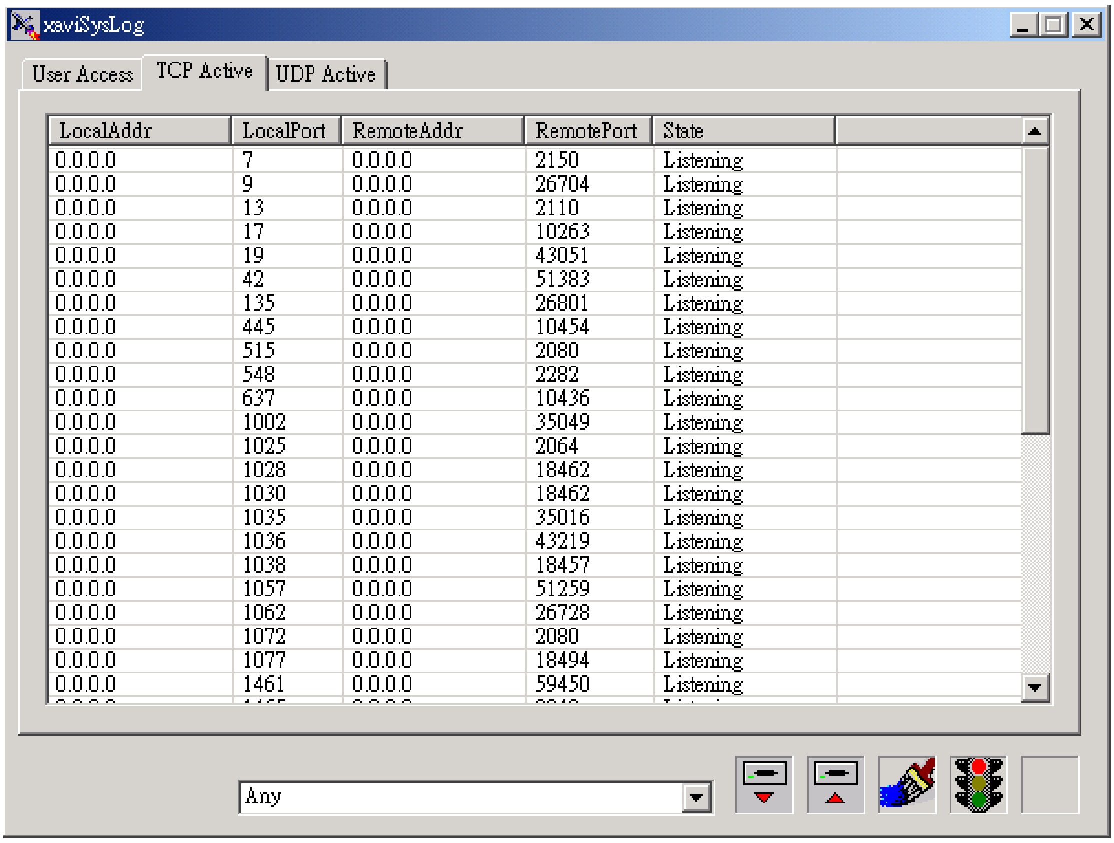
The **default Syslog port** is 514, no need to change the port number.
The **default log file path** is the current directory of the syslog program. Change it to the directory you wish the log file stored.

Replay. If the others also need the syslog message from the gateway, you can redirect your to it. The gateway only send its log information to one IP address, thus you have to replay it, check the box for a replay. Also please specify an IP address and the port number for the replay. Click **OK** after you finished the setting of this page.



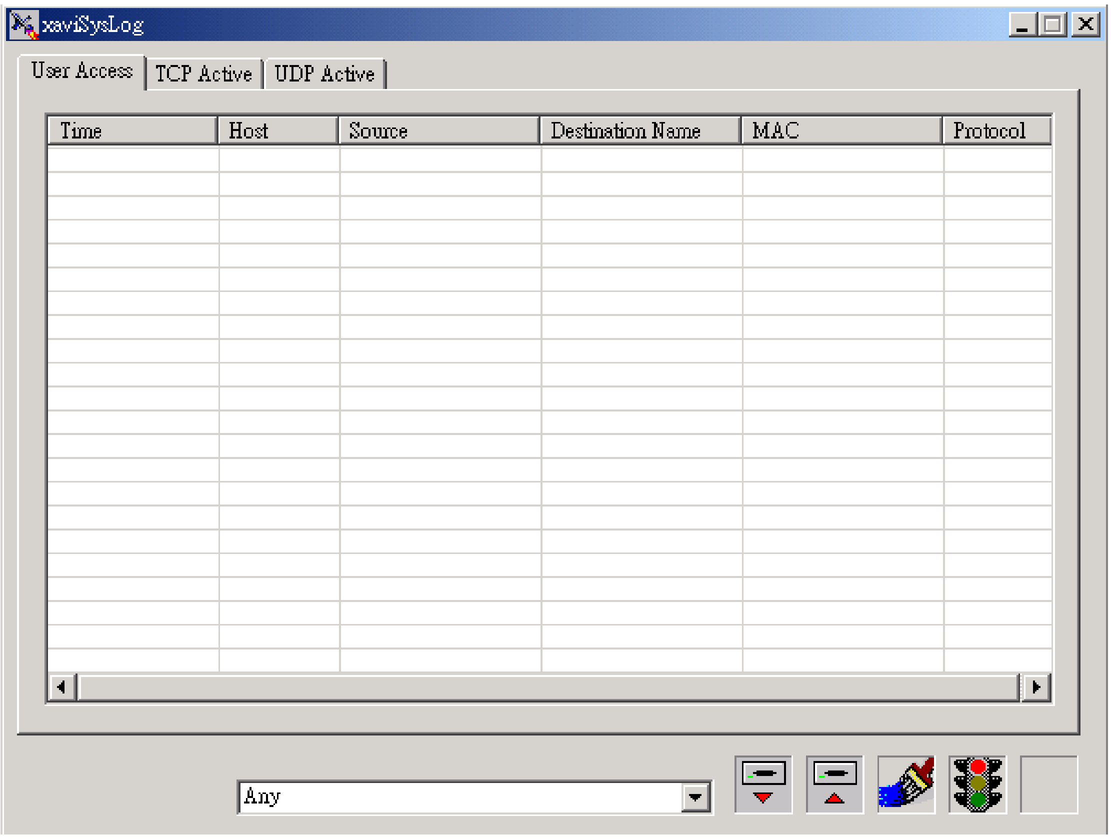
LocalAddr	LocalPort
0.0.0.0	7
0.0.0.0	9
0.0.0.0	13
0.0.0.0	17
0.0.0.0	19
0.0.0.0	42
0.0.0.0	161
0.0.0.0	445
0.0.0.0	514
0.0.0.0	1029
0.0.0.0	1034
0.0.0.0	1040
0.0.0.0	1081
0.0.0.0	1645
0.0.0.0	1646
0.0.0.0	1701
0.0.0.0	1755
0.0.0.0	1812
0.0.0.0	1813
0.0.0.0	3456
0.0.0.0	14237
127.0.0.1	1026
127.0.0.1	1027

UDP Active. Shows the UDP sessions of your PC.



LocalAddr	LocalPort	RemoteAddr	RemotePort	State
0.0.0.0	7	0.0.0.0	2150	Listening
0.0.0.0	9	0.0.0.0	26704	Listening
0.0.0.0	13	0.0.0.0	2110	Listening
0.0.0.0	17	0.0.0.0	10263	Listening
0.0.0.0	19	0.0.0.0	43051	Listening
0.0.0.0	42	0.0.0.0	51383	Listening
0.0.0.0	135	0.0.0.0	26801	Listening
0.0.0.0	445	0.0.0.0	10454	Listening
0.0.0.0	515	0.0.0.0	2080	Listening
0.0.0.0	548	0.0.0.0	2282	Listening
0.0.0.0	637	0.0.0.0	10436	Listening
0.0.0.0	1002	0.0.0.0	35049	Listening
0.0.0.0	1025	0.0.0.0	2064	Listening
0.0.0.0	1028	0.0.0.0	18462	Listening
0.0.0.0	1030	0.0.0.0	18462	Listening
0.0.0.0	1035	0.0.0.0	35016	Listening
0.0.0.0	1036	0.0.0.0	43219	Listening
0.0.0.0	1038	0.0.0.0	18457	Listening
0.0.0.0	1057	0.0.0.0	51259	Listening
0.0.0.0	1062	0.0.0.0	26728	Listening
0.0.0.0	1072	0.0.0.0	2080	Listening
0.0.0.0	1077	0.0.0.0	18494	Listening
0.0.0.0	1461	0.0.0.0	59450	Listening

TCP Active. Shows the TCP sessions of your PC.



Time	Host	Source	Destination Name	MAC	Protocol

User Access. Show all users' sessions of the gateway.

Pull down menu. From the pull down menu, you will see the list of the gateways on your network, choose from the list, or choose **Any** to get messages from all gateways.

Open Record. Open a saved record from the PC.

Save Record. Save the records on the list to the file.

Clean Record. Clean the records on the list.

Stop Record. Stop receiving new records from the gateway.