Broadband Gateway with 4 Port / 7 Port NWay Switching Hub

User's manual

CE Declaration of conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class A for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limitations are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if no installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into a different outlet from that the receiver is connected.
- Consult your local distributors or an experienced radio/TV technician for help.
- Shielded interface cables must be used in order to comply with emission limits.

Changes or modifications to the equipment, that are not approved by the party responsible for compliance could affect the user's authority to operate the equipment.

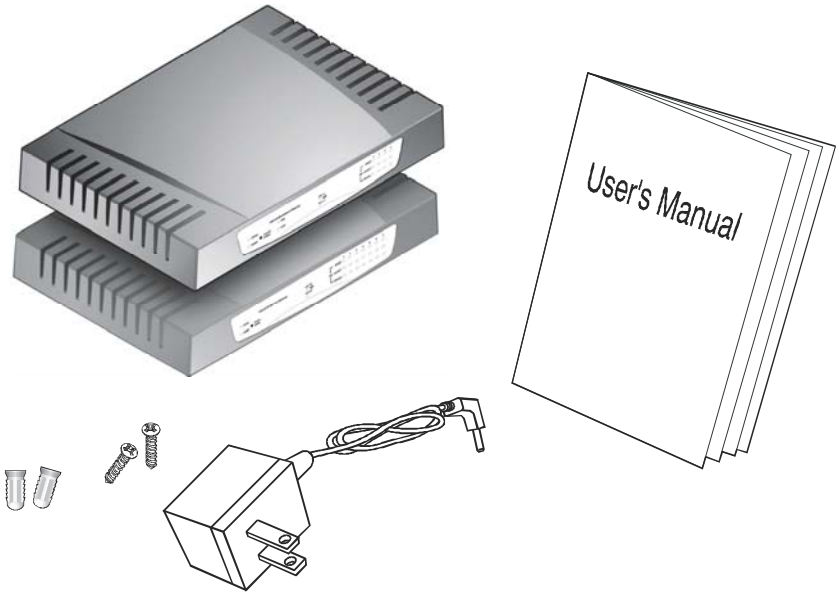
Table of Contents

1. Unpacking Information

Thank you for purchasing the internet broadband gateway. Before you start, please check all the contents of this package.

The product package should include the following:

1. **One broadband gateway**
2. **One power adapter**
3. **Wall-mount kit**
4. **User's Manual**



2. Introduction To Internet Broadband Gateway

2.1 General Description

The broadband gateway device has a 4-port / 7-port 10/100Mbps Fast Ethernet switch on LAN side and one 10Mbps Ethernet WAN port. This device has been specifically designed to provide Local Area Network (LAN) users with multiple accesses to the Internet at the cost of a single public IP address. Connections can be made via Cable or ADSL modems allowing secure and high-speed Internet access. Firewall protection secures your network from being accessed by outside users. All incoming data packets are monitored and filtered. It can also be configured to block internal users from accessing to the Internet.

This device provides the most cost-effective method for multiple network users to access the Internet using Cable or ADSL. Moreover, the built-in 4-port / 7-port 10/100Mbps switch lets users plug the network cable into the device without buying additional switch. With the functions of the IP sharing, you can enjoy the true Plug & Play installation.

For network connection:

The LAN switch can use the following types of cabling:

- 10BASE-T: Category 3, 4 or 5 UTP/STP
- 100BASE-TX: Category 5 UTP/STP

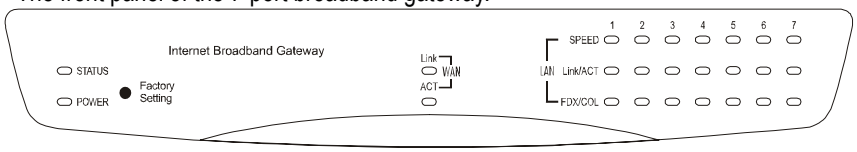
2.2 Key Features

The switch provides the following key features:

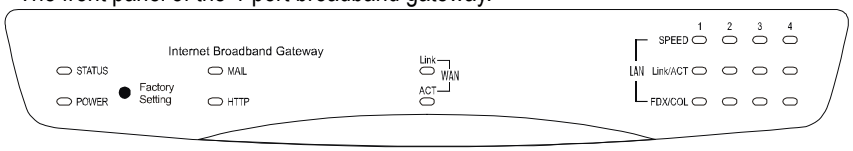
- Complies with 10BASE-T specifications of IEEE802.3 standard
- Complies with 100BASE-TX specifications of IEEE802.3u standard
- Seven / four RJ-45 ports for 100BASE-TX and 10BASE-T connectivity on LAN side.
- One 10BASE-T port on WAN side
- Connects to a broadband backbone such as ADSL modem, Cable modem. Acts as both DHCP client and DHCP server for receiving WAN IP address from ISP and configuring IP addresses to LAN clients.
- Supports DHCP and fixed IP address configuration for host IP address assignment
- Embedded web support for easy configuration and management through web browser like Netscape Communicator 4.0 and Internet Explorer 3.0 or update version
- Compatible with all popular Internet applications
- Built-in firewall security function to protect internal hosts from outside intruders
- Allows administrators to block certain users from accessing specific applications, or certain web sites on the Internet
- Supports unrestricted two-way communication between one PC on your LAN and certain Internet services like conferencing, video and gaming applications
- Enhances the routing performance by static routing setting
- The Virtual Server function allows a fixed IP address to be setup on the local area network. External Internet users are able to access and obtain information of the internal target host.
- Supports PPPoE function
- Supports extensive LED indicators for network diagnostics
- External power adapter
- FCC Class A, CE

2.3 The Front Panel

The front panel of the 7-port broadband gateway.



The front panel of the 4-port broadband gateway.



The auto-negotiation feature of the switch allows each port of the device running at one of the following four operation modes:

1. 100Mbps full-duplex
2. 100Mbps half-duplex
3. 10Mbps full-duplex
4. 10Mbps half-duplex

2.3.1 System LEDs

System LED indicators are located on the front panel for showing the operating status of the whole device.

2.3.1.1 Power LED

This indicator lights green when the gateway is receiving power; otherwise, it is off.

2.3.1.2 Status LED

The LED will be green for 2~3 seconds when the system is started. After that, the LED will blink once per second to show the gateway is working normally. If the LED stay green that means the system is fail, you need to contact your agent or try to reboot the system. When the LED is dark always, there are two reasons, one is LED is broken and the second one is system fail.

2.3.1.3 HTTP LED (4-port)

The LED will blink green when there is any HTTP packet on the network.

2.3.1.4 Mail LED (4-port)

The LED will blink green when there is any SMTP packet (mail) on the network.

2.3.2 Port LEDs (WAN side)

Port LED (WAN side) indicators are located on the front panel for showing the operating status of WAN port.

2.3.2.1 Link LED

The LED stays light (green) means the port has good linkage to its associated devices.

If the port is connected but the Link LED is dark, check the following items:

1. The gateway and the connected device's powers are on or not
2. The port's cable is firmly seated in its connectors in the gateway and in the associated device.
3. The connected cable is good and has correct type
4. The connected device, including any network adapter is functioning.

2.3.2.2 ACT LED

The activity LED will blink green when there is traffic transverse the port.

2.3.3 Port LEDs (LAN side)

Port LEDs (LAN side) indicators are located on the front panel for showing the operating status of 10/100Mbps Fast Ethernet switching ports.

2.3.3.1 Speed LED

The Speed LED indicates the link speed of each port. If the LED lights green then the connection speed is 100Mbps, off for 10Mbps.

2.3.3.2 Link/Act LED

Every port has a Link/Activity LED. Steady green (link state) indicates that the port has good linkage to its associated devices. Flashing green indicates that the port is receiving or transmitting data between its associated devices.

Speed LED	Link/Activity LED	Status
Off	Off	No Connection
Off	Green	Connect as 10Mbps
Green	Green	Connect as 100Mbps

2.3.3.3 FDX/COL LED

A collision occurs when two stations within a collision domain attempt to transmit data at the same time. Intermittent flashing amber of the collision LED is normal; the contending adapters resolve each collision by means of a wait-then-retransmit algorithm. Frequency of collisions is an indicator of heavy traffic on the network.

If the FDX/COL lights amber which means the port is under full-duplex operation or dark for half-duplex mode. The following table is a summary of LAN Port LEDs.

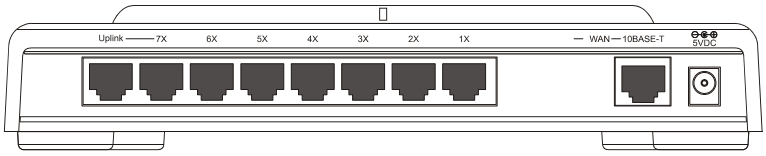
LED	Operation
100M	100Mbps (Green), 10Mbps (Off)
Link/Act	Link is present (Green), Activity (Blinking Green)
FDX/COL	Full-Duplex (Amber), Half-Duplex (Off), COL (Blinking Amber)

2.3.4 Factory Setting button

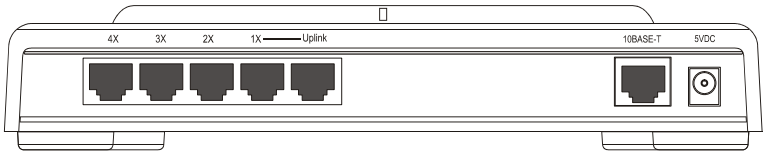
Push the button, the system will return to factory default setting and reboot.

2.4 The Rear Panel

The rear panel of the 7-port broadband gateway.



The rear panel of the 4-port broadband gateway.



2.4.1 Power Connecting

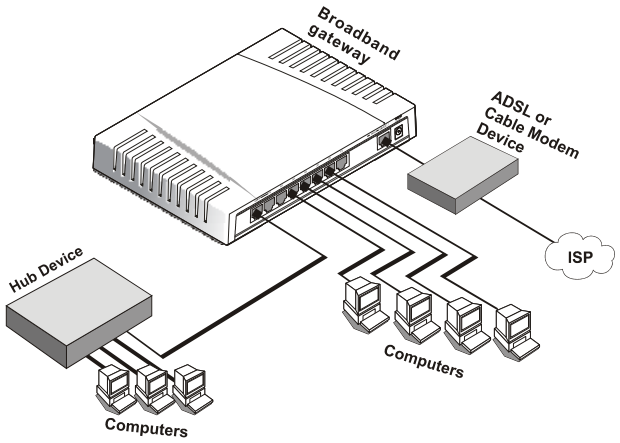
Plug the circle end of the power adapter firmly into the rear panel of the gateway, and the other end put into an electric service outlet then the system is ready.

3. Installing And Using Internet Broadband Gateway

This Chapter provides a step-by-step guide to the installation and configuration of the broadband gateway. It assumes that your computers use the Windows 95 / 98 or newer version and a web browser is installed for configuration purposes. We suggest you go over the whole chapter and then do more advanced operation.

3.1 Network configuration setup

The following drawings are typical network wiring for Internet access.



Drawing 1: ADSL/Cable modem connection

Steps to build up the network:

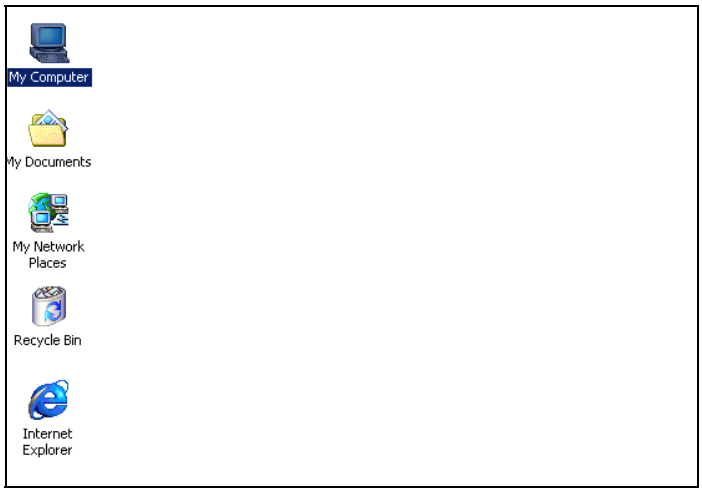
1. Connect the ADSL or Cable modem to the Ethernet WAN port on the back of the broadband gateway by using the category 3 or 5 UTP cable.
2. Connect the phone line from the wall socket to the line-in port on the ADSL modem, or the coaxial cable to the line-in port on the Cable modem.
3. Plug-in the power adapter to the modem and turn on the power. Install the Ethernet card into the computer by referring to the User Guide that came with the card.
4. Connect the computer to the broadband gateway by using standard twisted-pair Ethernet cable from the computer's Ethernet card to an 10/100Mbps Ethernet port on the back of the broadband gateway.
5. Plug-in the power adapter to the gateway and the other side to the wall outlet.

3.2 Computer configuration setup

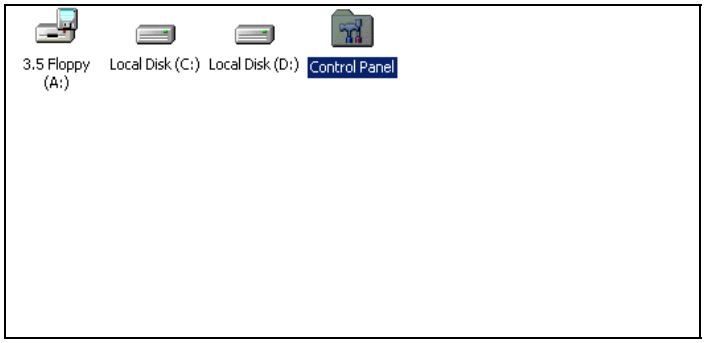
In order to communicate with broadband gateway, the connected computer needs to install the TCP/IP protocol and setup the related address information.

Steps to build up the computer:

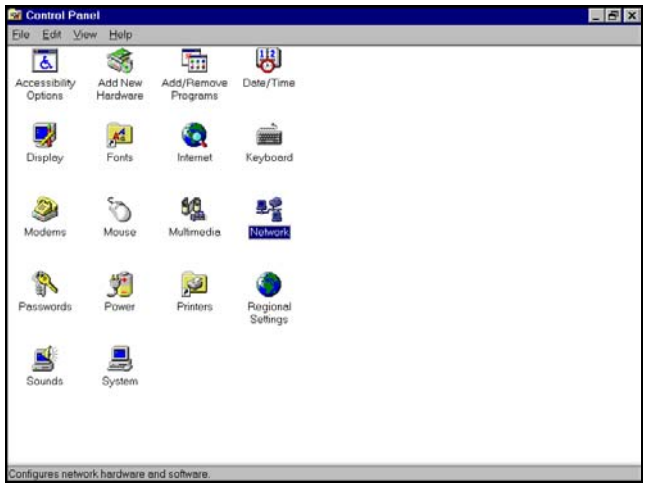
1. Double click the **"My Computer"** icon on the desktop screen



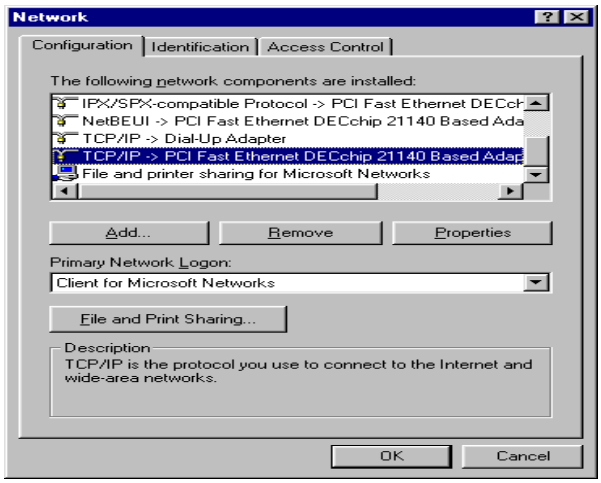
2. Double click the **"Control Panel"** icon on the My Computer window



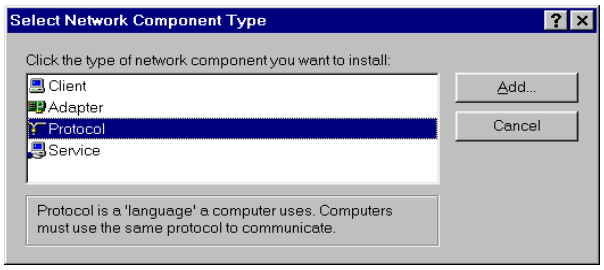
3. Double click the **"Network"** icon on the Control Panel window



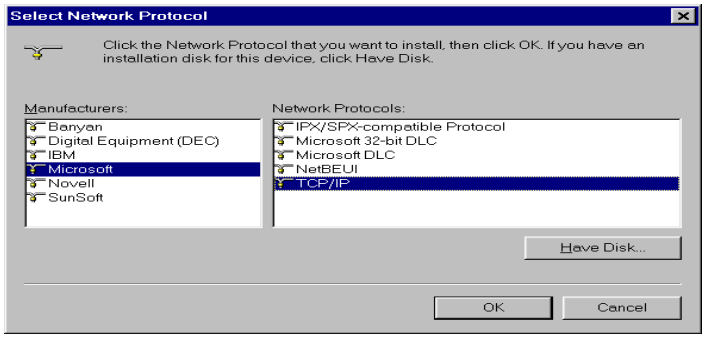
4. Click the **"Configuration"** tab and check the TCP/IP protocol is available or not. If yes, skip the procedures 5 ~ 6. If no, click the **"Add"** button.



5. Select **"Protocol"** item on the Select Network Component Type window. After that, click **"Add"** button

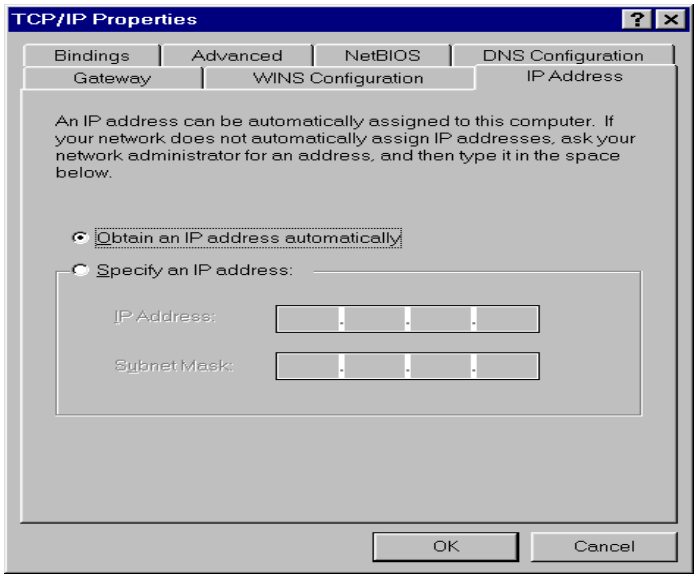


6. Select **"Microsoft"** item on the left side of Select Network Protocol window. After that, select **"TCP/IP"** protocol on the Network Protocols block and click **"OK"** button.



7. Select the **"TCP/IP"** component in the Configuration tab of the Network window. Click **"Properties"** button.

8. The screen will show up the TCP/IP Properties window then start the setting. First of all, you need to choose the IP address is dynamically assigned by a DHCP server or fixed.



Dynamically assigned:

- Select the **"IP Address"** tab and select **"Obtain an IP address automatically"** (default setting)
- Select the **"Gateway"** tab and click **"Remove"** to clear any existing entry of gateway IP address
- Select the **"DNS Configuration"** tab and click **"Disable DNS"**
- Click **"OK"** button

Fixed:

If there are some clients who need to get fixed IP addresses for some reasons and the nodes also need to access Internet through the broadband gateway then the following steps used to configure system

- Select **"Specify an IP address"** in the IP Address Tab of the TCP/IP Properties window and enter 192.168.1.*** in the IP Address field (the *** is a number between 2 and 254 used by the internet gateway to identify individual computers)

NOTE: The default IP address of broadband gateway is 192.168.1.1 and subnet mask is 255.255.255.0

- Select the **"Subnet Mask"** field and enter 255.255.255.0
- Select the **"DNS Configuration"** tab and click **"Enable DNS"**
- Enter the DNS IP Address obtained from your ISP in the **"Server Search Order"** location. Click **"OK"** button.

NOTE: For the new network computers to use dynamic IP addresses provided by the broadband gateway DHCP server, they should not use the range of fixed IP addresses. For example,
If the fixed IP addresses already use 192.168.1.2 to 192.168.1.68 the DHCP server must be setup to allocate the dynamic addresses out of this range.

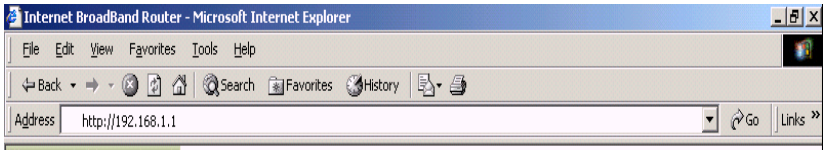
9. The screen will return back to Network window then click **"OK"** button. At this moment, the system will prompt you for restarting the Windows. Click **"Yes"**

3.3 Broadband gateway configuration setup

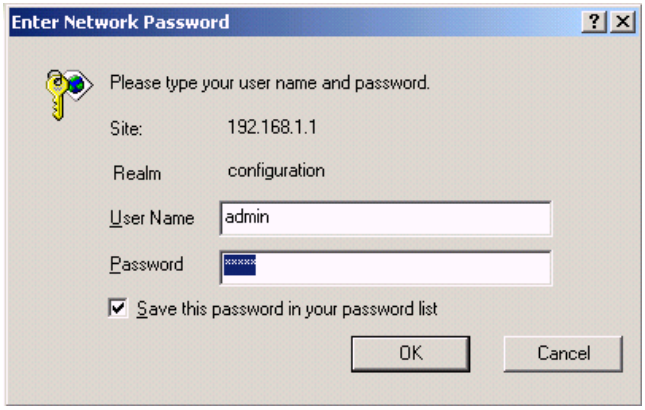
In order to make the whole network operate successfully, it is necessary to configure the broadband gateway through your computer has a web browser installed. Please follow up the steps listed below.

1. Double click the Internet web browser icon on your desktop screen (Netscape Communicator 4.0 and Internet Explorer 3.0 or update version)

2. Type 192.168.1.1 into the URL web address location and press Enter.



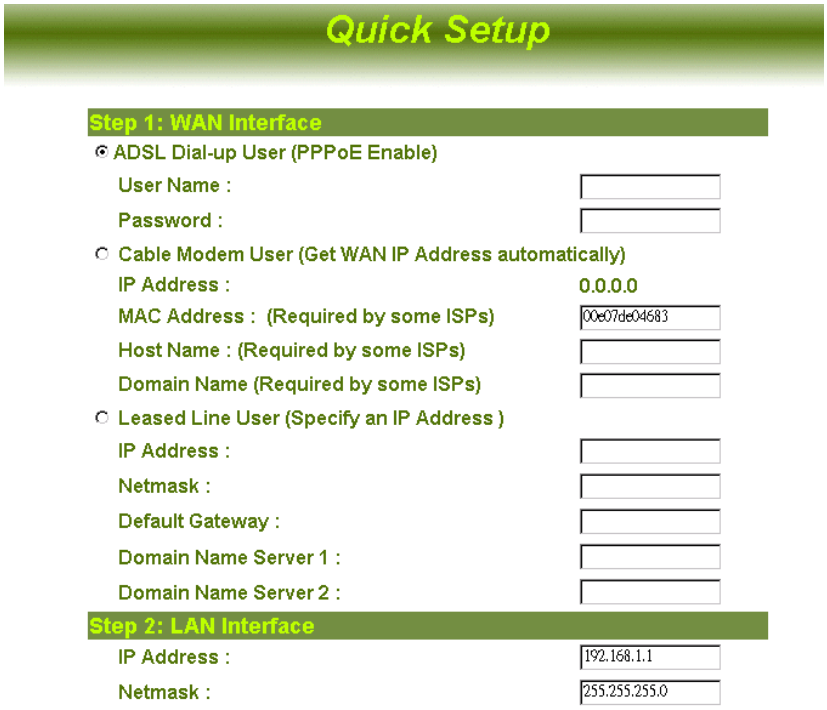
3. The Username and Password Required window appears.
   - Enter **admin** in the User Name location (default value).
   - Enter **admin** in the Password location (default value).
   - Click **"OK"** button



4. In the home page of broadband gateway, the left navigation bar shows the options to configure the system. The items include **Quick Setup, PPPoE Setup, Administration, DHCP Server, Static Route, Access Control, Virtual Server, Virtual Computer, Traffic Log, Statistics, Special Application,** and **Software Update**.

3.3.1 Quick Setup

After click the “Quick Setup” item, the following screen will be displayed.



WAN Interface setup

There are three kinds of WAN interface options, including ADSL user, Cable Modem user and Leased line user. Select one option that fits your case.

ADSL Dial-up User (PPPoE Enable)

Some ISPs provide DSL-based service 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 select this item.

User Name: Enter User Name provided by your ISP
(maximum 60 characters)

Password: Enter Password provided by your ISP.
(maximum 60 characters)

Cable Modem User (Get WAN IP Address automatically)

IP Address: If you are connected to the Internet through a Cable modem line then a dynamic IP address will be assigned.

MAC Address: Some ISP may require your MAC address of your PC for identification. Please key-in the MAC address.

Host Name: Some ISP may require the host name of your PC for identification.

Leased Line User (Specify an IP Address)

If you are a leased line user with a fixed IP address, fill out the following items with the information provided by your ISP.

IP Address: check with your ISP provider

Netmask: check with your ISP provider

Default Gateway: check with your ISP provider

Domain Name Server 1: check with your ISP provider

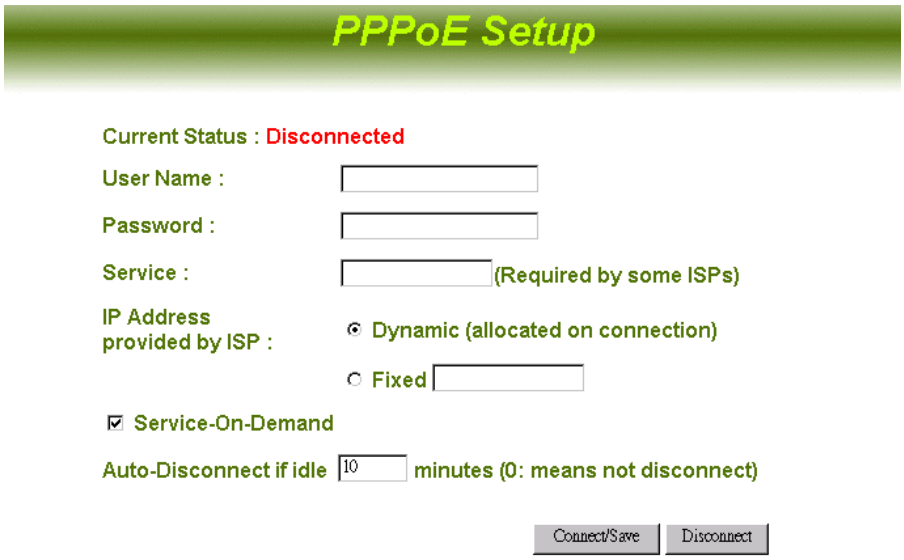
Domain Name Server 2: check with your ISP provider

LAN Interface setup

IP Address: Enter the IP address of internal LAN. The default value is 192.168.1.1

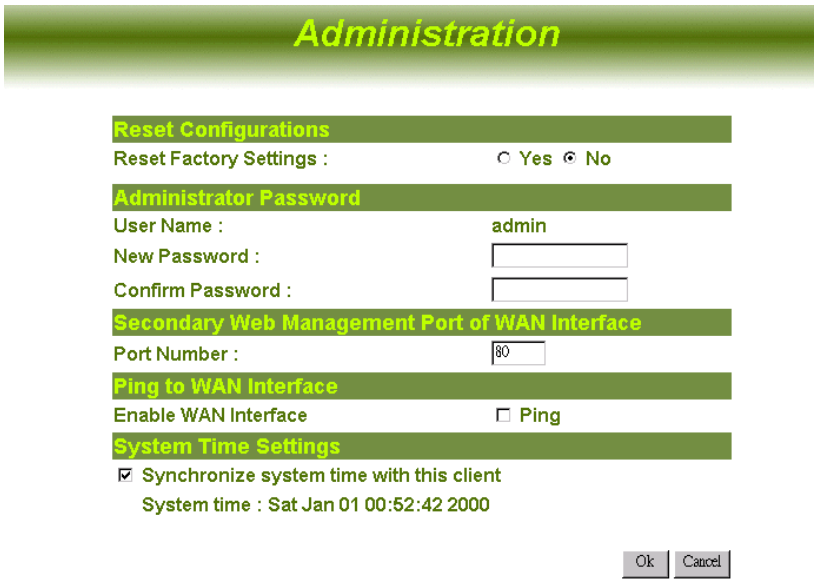
Netmask: Enter the network mask of internal LAN. The default value is 255.255.255.0.

3.3.2 PPPoE Setup



Current Status: This item displays the link status of PPPoE (read only) , the possible status would be Connected/Disconnected
User Name: Enter the user name provided by your ISP for PPPoE connection (maximum 60 characters)
Password: Enter the password provided by your ISP for PPPoE connection (maximum 60 characters)
Service: Enter the service name provided by your ISP (if required)
IP Address provided by ISP: IF you are a fixed IP user, choose "Fixed" then fill in the IP address.
Service-On-Demand: Check this box and this device is configured to auto-connect whenever you log-on.
Auto-Disconnect : Enter a number as a predetermined period of time for auto-disconnection. This device can then be configured to auto-disconnect from the Internet when there's no activity on the line. To keep the line always connected, set the number to 0. The range of the number is between 1 to 99999.

3.3.3 Administration



Reset Configurations: Reset this device to the factory default settings and you will clear all the existing settings of the device.

Administrator Password: Set the password for adminstration purpose. It is recommended that you set the password and leave it in a safe place. Maximum 6 characters

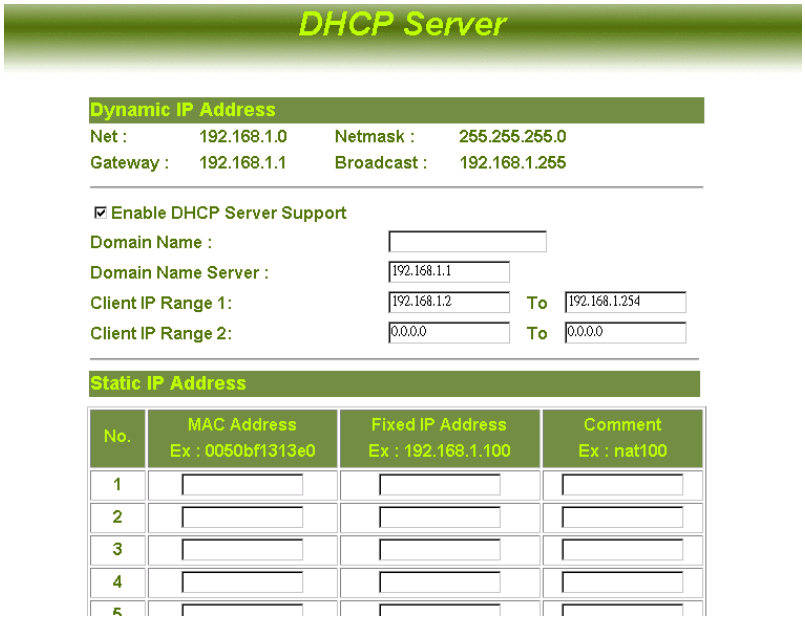
Secondary Web Management Port of WAN Interface: You can change the port number to prevent intruders from accessing the management interface.

Ping to WAN Interface: Leave the **Ping** check box empty can prevent client user from knowing the real IP of WAN interface by using the "ping" tool.

System Time Settings: The time that this device was set in factory may be different from your computer. However, you can synchronize this device and your computer for accurate management purpose. Check this box to set this system synchronized with your computer.

3.3.4 DHCP Server Configuration

If you setup this device as a DHCP Server, that will allow this broadband gateway assign dynamic IP addresses to your local clients. In this case, you need to click **Enable DHCP Server Support.**



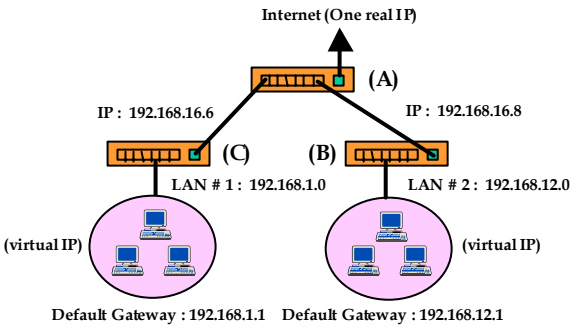
When you need to assign static IP addresses to your local clients, you need to enter the MAC addresses of the local computers and the IP addresses you assigned to them. Moreover, you can even add Comment to name your IP clients.

Enable DHCP Server Support

1. Click **Enable DHCP Server Support**.
2. **Domain Name Server :** Your ISP will provide you at least one DNS IP address, enter the IP address of DNS.
3. **Client IP Address Range 1:** Enter the first range of starting IP address and ending IP address, assigned to the LAN clients.
4. **Client IP Address Range 2:** Enter the second range of starting IP address and ending IP address, assigned to the LAN clients.
5. **Static IP Address** (Optional, can not overlap with the address range 1 and range 2)
   MAC Address: The MAC address of network interface card.
   Fixed IP Address: The assigned IP address.
   Comment: Notes about the client
6. Click Ok

3.3.5 Static Route Configuration

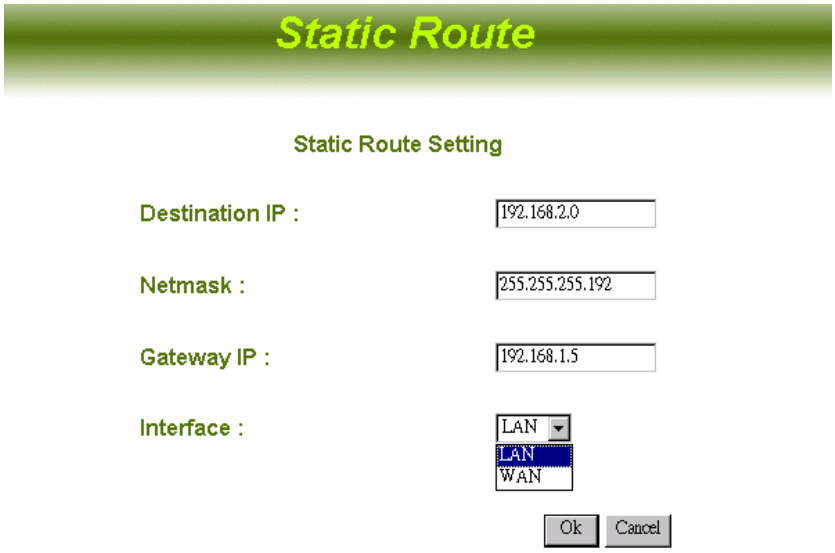
The function of Static Routing feature allows the clients in the same LAN subnet of broadband gateway to communicate with the clients in other respective LAN segment that is connected to the broadband gateway. The following are typical diagrams show the examples of physical connections that need to use Static Routing.



In the diagram above, the clients in LAN#2 connect to broadband gateway (B) can not communicate with the clients in LAN#1 without configuring the static routing function. You can set a static route to manually administrate the network topology/ traffic when dynamic routing is not effective enough. The definition of the items:

Interface: WAN or LAN interface
Destination IP: LAN IP address of the destination network.
NetMask: Network mask of the destination network.
Gateway IP: The Gateway IP address to the destination network.
Configuration: Configure the static routing settings.

Interface	Destination IP	Netmask	Gateway IP	Configuration
LAN	192.168.2.0	255.255.255.192	192.168.1.5	Modify Delete



To start the configuration, click the **New Entry** and fill in the IP address and Subnet Mask of the destination LAN that the broadband gateway LAN segment plan to communicate with. For example, in the above diagram, you need to fill in the following data.

Broadband gateway (C)
Destination LAN IP: **192.168.12.0**
Netmask: **255.255.255.0**
Gateway IP: **192.168.16.8**

Broadband gateway (B)
Destination LAN IP: **192.168.1.0**
Netmask: **255.255.255.0**
Gateway IP: **192.168.16.6**

In the **Interface** location, you should choose **WAN** if the Destination LAN is on the WAN side of Broadband Gateway, otherwise, you should choose **LAN**. According to the above diagram and proper setting, LAN#1 can access to LAN#1, LAN#2 and Internet, however, LAN#2 can also access LAN#2, LAN#1 and Internet.

3.3.6 Outgoing Policy

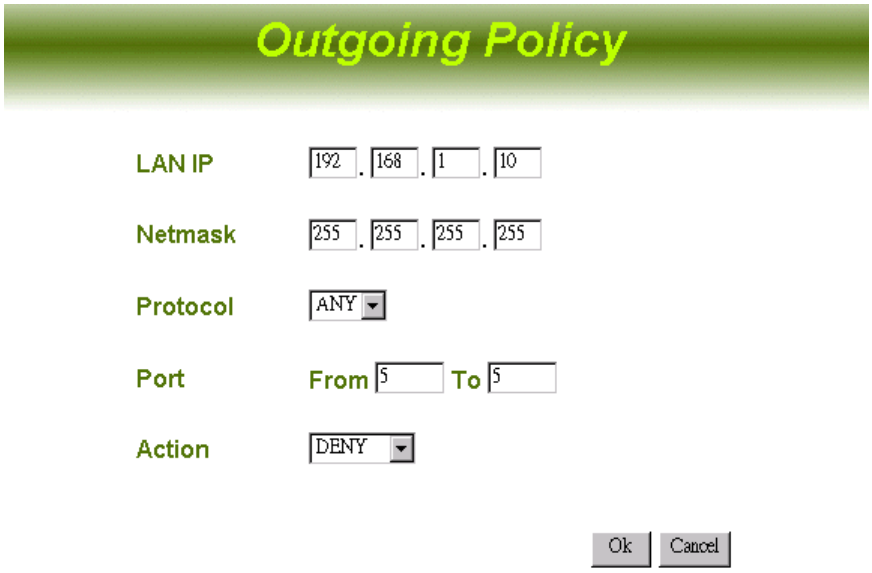
The broadband gateway could filter the outgoing packets for security or management consideration. You can set up the filter against the IP addresses to block specific internal users from accessing the Internet. The outgoing policy settings are:

LAN IP: The IP address of local computer.
Protocol: Protocol type.
Port: The specify range of service port.
Action: Deny (block) or permit (forward).
Configure: You can select to pause, modify or delete this filter.

LAN IP	Protocol	Port	Action	Configure
192.168.1.10	ANY	---	DENY	Pause Modify Delete

Add Outgoing Policy:
Click **New Entry** for adding a new outgoing policy.
LAN IP: Enter IP address of the local computer.
NetMask: The network mask of the LAN IP address.
For example:
1. LAN IP: 192.168.1.192, NetMask: 255.255.255.255
   ➔ Only one IP address 192.168.1.192 be controlled
2. LAN IP: 192.168.1.192, NetMask: 255.255.255.192
   ➔ The IP address in the range 192.168.1.192 ~ 192.168.1.254 will be controlled
3. LAN IP: 192.168.1.192, NetMask: 255.255.255.254
   ➔ The IP address in the range 192.168.1.192 ~ 192.168.1.193 will be controlled

Protocol: Click the down arrow (▾) to select the appropriate protocol.
Port: Select a specify range of service port
Action: Select DENY or ACCEPT to drop or forward packets from the specified IP address.
Click **Ok** to add a new outgoing policy or **Cancel** to abort.



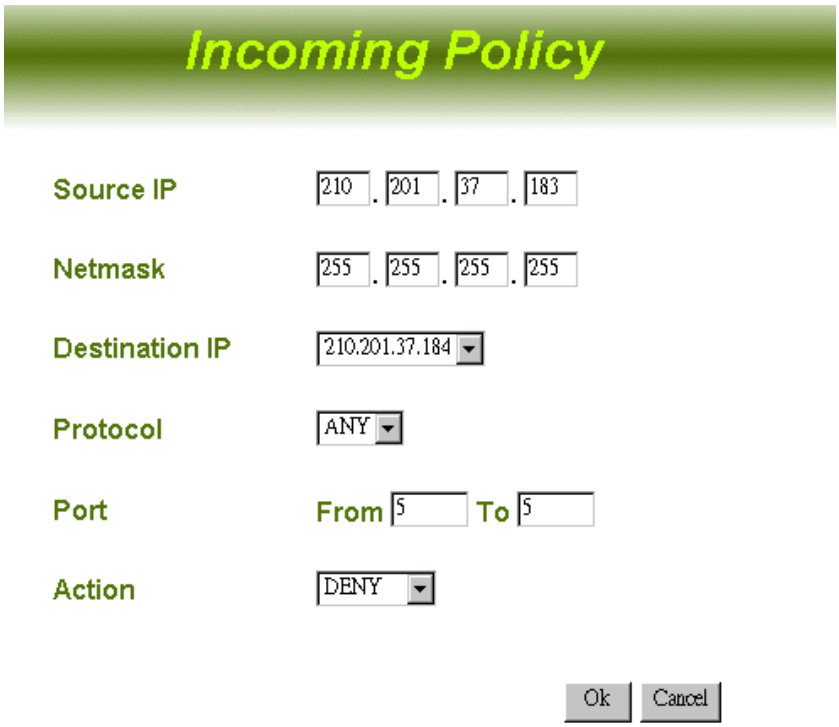
3.3.7 Incoming Policy

The broadband gateway could filter the incoming packets for security or management consideration. You can set up the filter against the IP addresses to block specific IP addresses if there are suspicious intentions. The incoming policy settings are:

Source IP: Source IP addresses.
Destination IP: The WAN IP that the policy will apply.
Protocol: The specify range of service port.
Port: Port number mapping to the LAN IP address.
Action: Deny (block) or permit (forward).
Configuration: You can select to modify or delete this filter.

Add Incoming Policy:
Click **New Entry** for adding a new incoming policy
Source IP: Enter the remote IP address you want to setup the policy.
NetMask: The network mask
For example:
1. Source IP: 210.201.37.186, NetMask: 255.255.255.255
   ➔ Only one IP address 210.201.37.186 will apply to the policy.
2. Source IP: 210.201.37.186, NetMask: 255.255.255.192
   ➔ The IP address in the range 210.201.37.128 ~ 210.201.37.191 will apply to the policy.
3. Source IP: 210.201.37.186, NetMask: 255.255.255.254
   ➔ The IP address in the range 210.201.37.186 ~ 210.201.37.187 will apply to the policy.

Destination: The WAN IP address you want to apply to the policy.
Protocol: Click the down arrow (▾) to select the appropriate protocol.
Port: Select a specify range of service port
Action: Select DENY or ACCEPT to drop or forward packets from the specified IP address.
Click **Ok** to add a new incoming policy or **Cancel** to abort.



3.3.8 Virtual Server Configuration

"Natural firewall" allows requests for Internet access from the local network. However, any request from the Internet to the local network is blocked. By setting the Virtual Server function, computers outside the Intranet are allowed to access specific ports of local client.

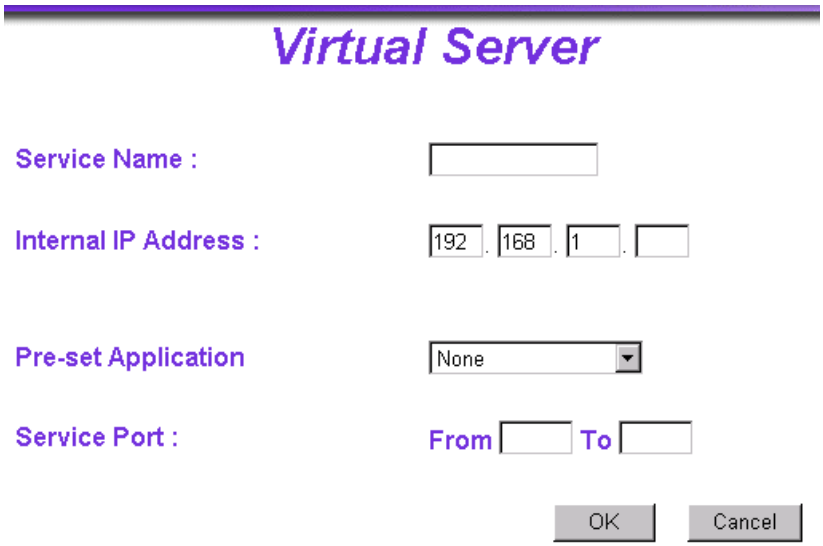
How to set a Virtual Server

Service Name: Assign a name to the service appropriately for easy identification, for example, HTTP, …

Internal IP Address: Assign the internal IP address for mapping to the service port.

Pre-set Application: Click the down arrow (▾) to select the pre-set application that you want to be accessed through virtual server.

Service Port: Enter the range of the port number assigned for virtual server. If you select the pre-set application then the service port will be automatically filled in.



3.3.9 Mapped IP Configuration

Mapped IP is a host that comes without the protection of firewall. It allows an internal computer to be exposed to unrestricted 2-way communication with other Internet users. This function is useful when proprietary client software and/or 2-way user communication, for example, video-conferencing and gaming, are required.

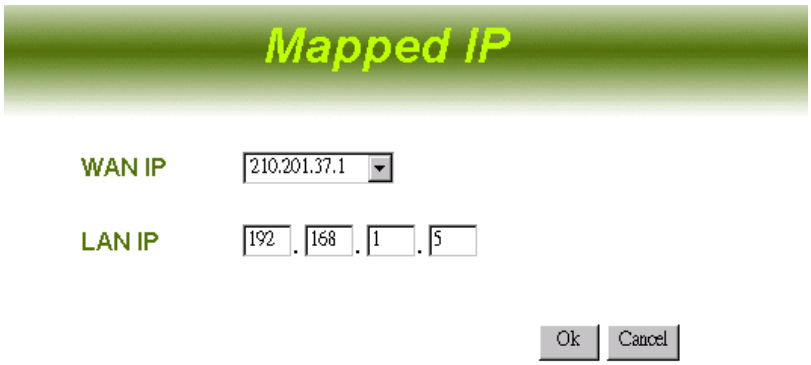
Add a Mapped IP Computer

Click **Mapped IP** then click New Entry.

WAN IP: Click the down arrow (▾) to select the WAN IP.

LAN IP: Enter the IP address of the local client that you want to use as the Mapped IP computer.

Click **Ok** to add a new Mapped IP computer.



NOTE: The WAN IP must be extra IP addresses got from ISP and the WAN IP address of broadband gateway is not allowed to map to a Mapped IP because the gateway will be no longer available.

3.3.10 Special Application Configuration

NAT (Network Address Translation) function prohibits some applications, e.g. Internet games, Video conferencing, Internet telephony, to work when multiple connections are required. Special Application, however, enables these applications to work in this device. If **Special Application** is not enough for multiple applications to work correctly, try **Mapped IP** function as described in the previous section.

Name	Outgoing		Incoming		Configure
AOE_II_(Client)	47624	47624	2300	2400	Modify Delete
Sudden_Strike	47624	47624	2300	2400	Modify Delete
Baldurs_Gate_II	47624	47624	2300	2400	Modify Delete

Add a Special Application

Click Special Application then click New Entry.

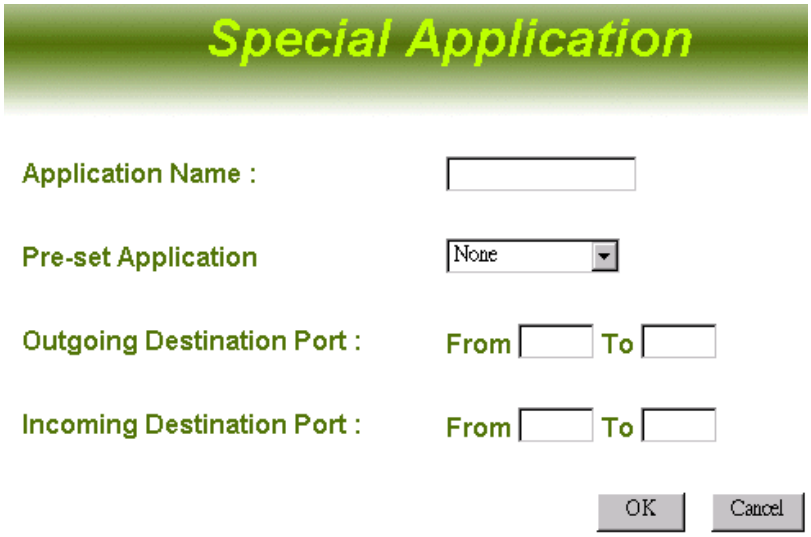
Application Name: Name the application appropriately for easy identification. Or you may skip this field to next for a Pre-set Application.

Pre-set Application: Click the down arrow (▾) to select a pre-set application you want to access via Internet.

Outgoing Destination Port: Enter the range of the outgoing packet's specified port numbers mapping to the pre-set application.

Incoming Destination Port: Enter the range of the incoming packet's specified port numbers allowed to pass this device.

When finishing , click **Ok** to add a new special application.



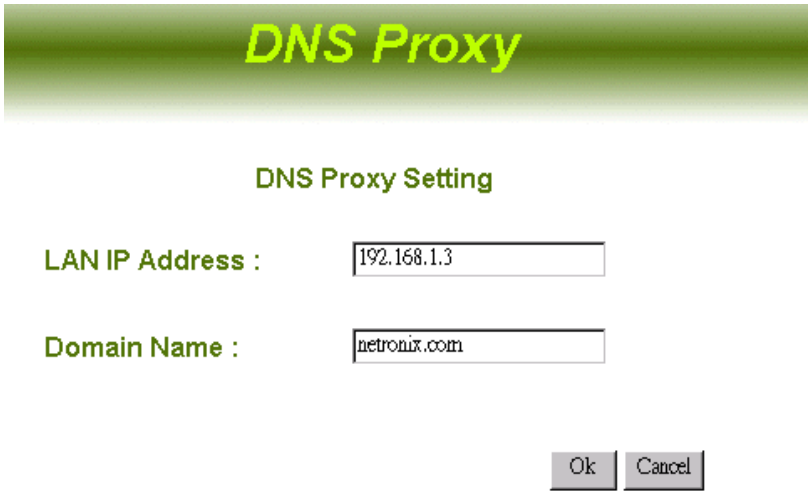
Note: 1. At any time, only one PC can use one Special Application tunnel.
2.You don't need to have a setup here in most of popular applications like "Netmeeting" and the ones comply with H.323 VoIP standard.

3.3.11 DNS Proxy

When you setup a Virtual Server configuration, for example a "WEB Server ", the **DNS Proxy** is recommended to setup at the same time. Because users on the LAN side of the Broadband Gateway will not be able to access the Virtual Server by entering a domain name (Accessing directly by IP address is not limited).

Add a DNS Proxy

Click **DNS Proxy** then click New Entry.
LAN IP address: Enter the IP address of the Virtual Server
Domain Name: The domain name mapping to the Virtual Server



3.3.12 Hacker Alert

When there are extraordinary accesses from Internet to your Broadband Gateway, you might be hacked. To enable the **Hacker Alert,** click the check box and enter your e-mail address, then you will receive a e-mail informing the situation.

SYN Attacks

A SYN attack creates each SYN packet in the flood with a bad source IP address, which under routine procedure identifies the original packet. All responses are sent to the source IP address. But a bad source IP address either does not actually exist or is down; therefore the ACK that should follow a SYN-ACK response will never come back. This creates a backlog queue that's always full, making it nearly impossible for legitimate TCP SYN requests to get into the system.

ICMP Flood

A Smurf hacker floods your router with Internet Control Message Protocol (ICMP) echo request packets (pings). If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up your network--the "intermediary" network--but will also congest the network of the spoofed source IP address--known as the "victim" network. To prevent your network from becoming the intermediary, you can enable the ICMP Flood detection.

UDP Flood

The User Datagram Protocol (UDP) Flood denial-of-service attack also links two unsuspecting systems. By spoofing, the UDP Flood attack hooks up one system's UDP chargen service, which for testing purposes generates a series of characters for each packet it receives, with another system's UDP echo service, which echoes any character it receives in an attempt to test network programs. As a result, a nonstop flood of useless data passes between the two systems.

To prevent a UDP Flood, you can enable UDP Flood detection to filter all incoming UDP service requests.

Ping of Death Attack

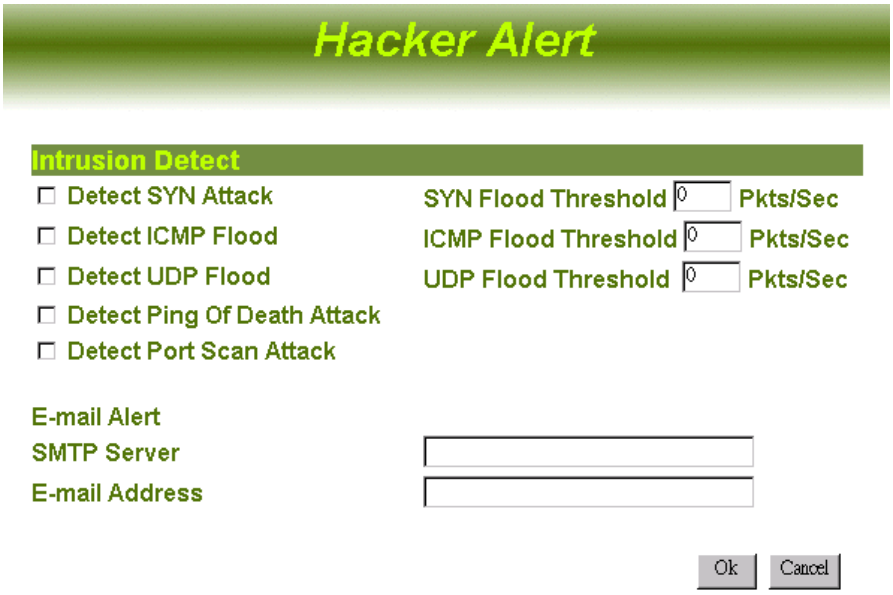
The Ping of Death uses a ping system utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang, or reboot when they receive such a maliciously crafted packet.

Port Scan attack

Readily available port scan applications attempt to connect to a computer by trying all IP ports on that host. Any response that indicates an open connection is put in a log for the initiator of the port scan to investigate. An analogy to a port scan would be a burglar who “cases” a neighborhood by checking all houses for unlocked doors and windows. It is essential that any Internet-connected organization be protected from port scans, which usually appear in the early stages of a sophisticated attack.

SMTP Server: The server name of your e-mail address for outgoing e-mails. Usually the characters after the symbol “@”, like “XXX.com”.

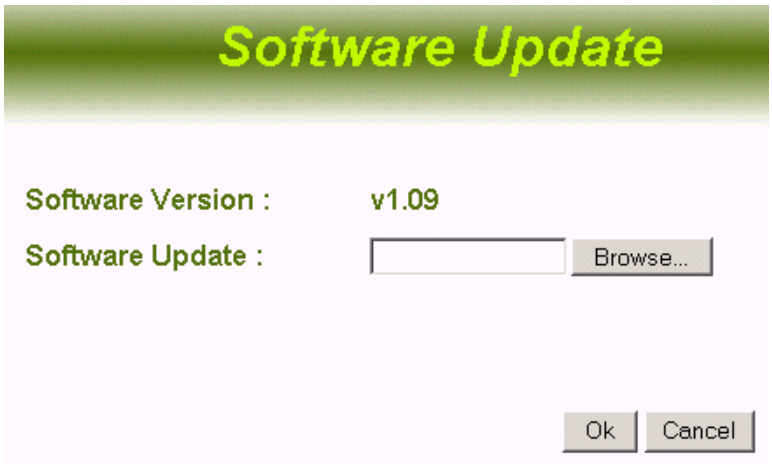
E-mail Address: The e-mail address you want to receive the mail alert.


Hacker Alert
Intrusion Detect
Detect SYN Attack
SYN Flood Threshold 0 Pkts/Sec
Detect ICMP Flood
ICMP Flood Threshold 0 Pkts/Sec
Detect UDP Flood
UDP Flood Threshold 0 Pkts/Sec
Detect Ping Of Death Attack
Detect Port Scan Attack
E-mail Alert
SMTP Server
E-mail Address
Ok
Cancel

3.3.13 Software Update Configuration

You can update the software version by yourself easily. Please follow up the following steps.

1. First you can obtain the version number of current software from **Software Version**.
2. Ask your local distributor to get the newest software's updated version. Download and store the updated program into the server's hard disk.
3. Click Browse button under **Software Update** to enter the Selecting File window and choose the most updated software version.
4. Click Ok on the bottom of the screen to update the software.



NOTE: If the upgrade process has been interrupted by any reason (power off, cable plug out, …) then the IP address of LAN interface of the broadband gate will reset back to the default value 192.168.1.1. Therefore, you need to change the IP address of PC to 192.168.1.xxx for accessing the gateway.

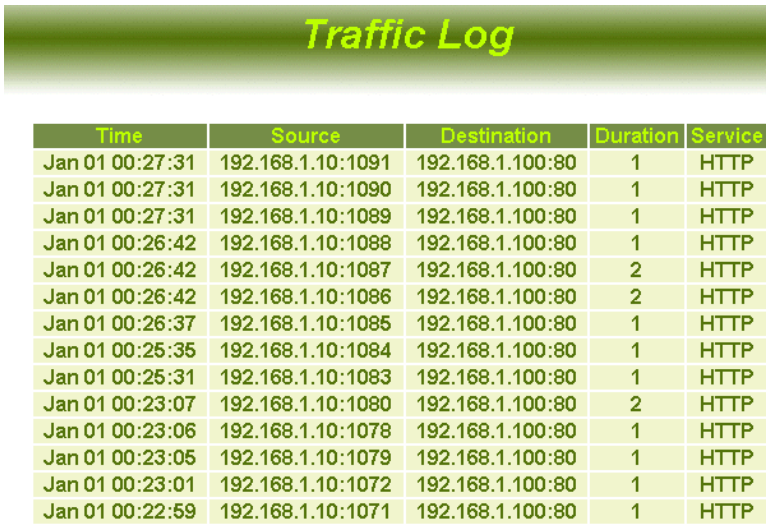
3.3.14 Connection Log

When you use PPPoE protocol to establish connections with your ISP, you can look up the connection log here.

Time	Connection Log
Jan 01 00:00:05	broadcasting DHCP_DISCOVER
Jan 01 00:01:12	sending DHCP_RELEASE for 1.1.1.1 to 0.0.0.0
Jan 01 00:01:13	terminating on signal 1

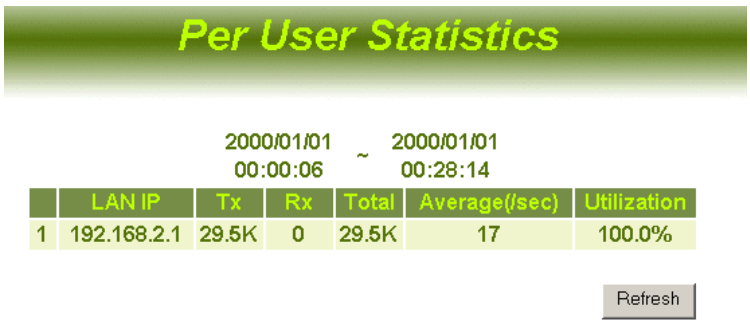
3.3.15 Traffic Log

Time : The log time.
Source : The IP address of the local computer.
Destination : The IP address of destination.
Duration : How much time the service cost.
Service : What kind of services users requested.



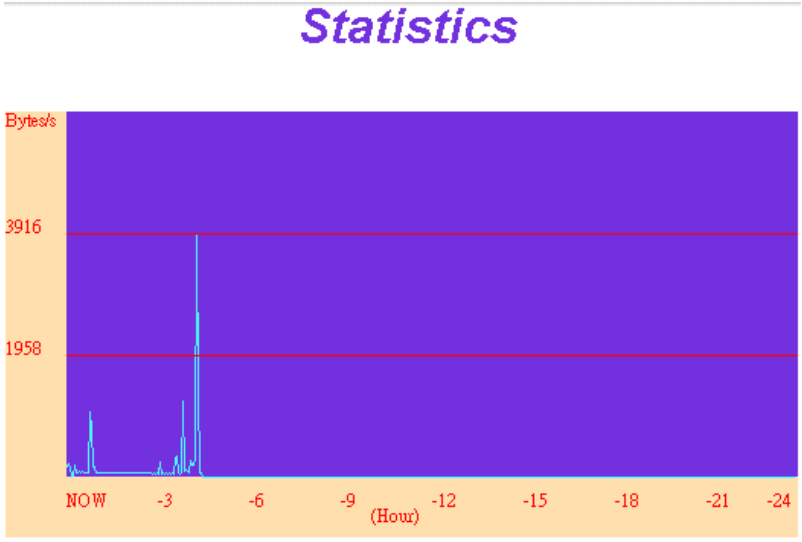
3.3.16 Per user statistics

The statistics of resources users utilized.
LAN IP : IP addresses of local users
Tx : How many data had transmitted.
Rx : How many data had received.
Total : The amount of data users transmitted and received.
Average : The average link speed.
Utilization : The percentage of bandwidth occupied by users.



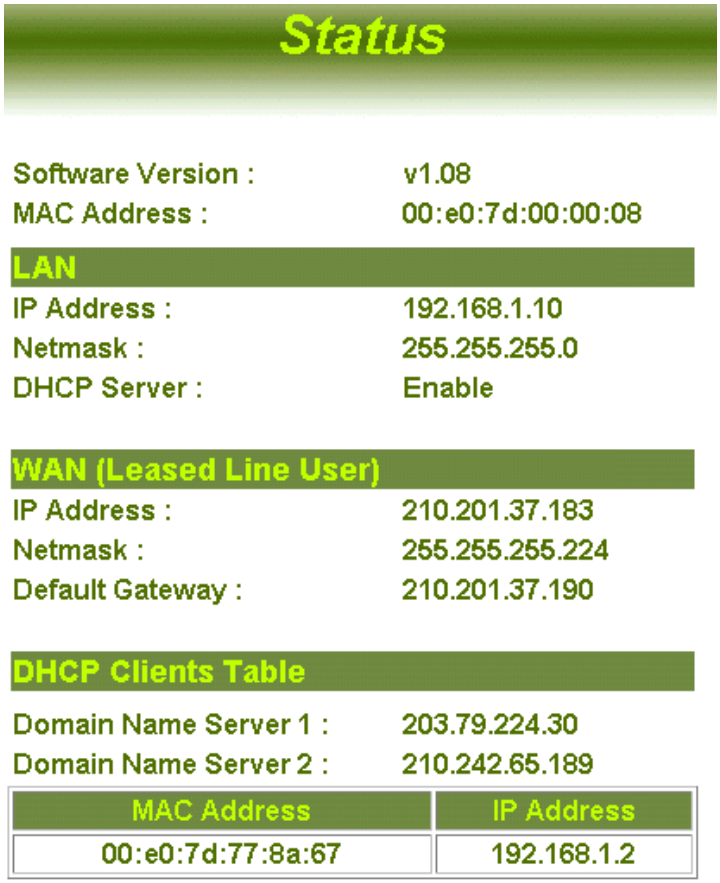
3.3.17 Statistics

The chart shows the utilization of past 24 hours.



3.3.18 Status

You can read basic system information and settings here.



4. Switch Operation

4.1 MAC Address Table and Learning

The LAN switch side is implemented with a MAC address table where is composed of many entries. Each entry is used to store the address information of network nodes on the network, including MAC address, port ID, etc. The information is the most important base to do packet filtering and forwarding.

When one packet comes in from any port, the switch will learn the source address, port ID, and the other related information in address table. Therefore, the content of the MAC table will update dynamically.

4.2 Filtering and Forwarding

When one packet comes in from any port of the switch, it will check the destination address besides the source address learning. The switch will look up the address table for the destination address. If not found, this packet will be forwarded to all the other ports except the port where this packet comes in. If found, and the destination address is located at different port from this packet comes in, the packet will be forwarded to the port where this destination address is located according to the information of address table. But, if the destination address is located at the same port as this packet comes in then this packet will be filtered.

4.3 Store and Forward

Store-and-forward is one kind of packet-forwarding methodology. As a store-and-forward switching hub, it will store the complete packet in the internal buffer and do the complete error checking before transmitting to the network. Therefore, no error packets will disturb the network. It is the best choice when a network needs efficiency and stability.

5. Product Specifications

Standard	IEEE802.3, 10BASE-T IEEE802.3u, 100BASE-TX
Interface	*RJ-45 x 4 10/100 Fast Ethernet switching ports *RJ-45 x 7 10/100 Fast Ethernet switching ports *One 10Mbps Ethernet WAN port
WAN Connection	ADSL/Cable modem
Cable Connections	RJ-45 (10BASE-T) : UTP Category 3,4,5 RJ-45 (100BASE-TX) : UTP Category 5
Network Data Rate	Auto-negotiation (10Mbps, 100Mbps)
Transmission Mode	Auto-negotiation (Full-duplex, Half-duplex)
LED indications	System Power x1, Status x1 Mail x 1(4-port) Http x 1(4-port) Port (LAN) Speed Link/ACT FDX/COL Port (WAN) Link ACT
Software Support	Embedded Web based management interface PPPoE support Static Route DHCP Server and Client Outgoing Policy Incoming Policy Virtual Server Mapped IP Special Application DNS Proxy Hacker Alert Software Update Connection Log Traffic Log Per User Statistics Statistics
Emission	FCC Class A, CE
Operating Temperature	0^0 ~ 50^0C (32^0 ~ 122^0F)
Operating Humidity	10% - 90%
Power Supply	5V,2A

6. Appendix A

Service Name, Protocol and Port number

Service	Protocol	Port	Service	Protocol	Port
ANY	Any	Any	AOL	TCP	5190-5194
BGP	TCP	179	Finger	TCP	79
FTP	TCP	20-21	Gopher	TCP	70
HTTP	TCP	80	HTTPS	TCP	443
IMAP	TCP	143	InterLocator	TCP	389
IRC	TCP	6660-6669	L2TP	TCP	1701
VDOLive	TCP	7000-7010	WAIS	TCP	210
WINFRAME	TCP	1494	X-WIN	TCP	6000-6030
DNS	UDP	53	IKE	UDP	500
NFS	UDP	111	NTP	UDP	123
PC-Anywhere	UDP	123	RIP	UDP	520
SNMP	UDP	161	SYSLOG	UDP	514
TALK	UDP	517-518	TFTP	UDP	69
UDP-Any	UDP	Any	UUCP	UDP	540
PING	ICMP	ANY	TRACEROUTE	ICMP	Any