USER MANUAL

ATU-R140

ADSL2+ SOHO modem

CTC Union Technologies Co., Ltd.

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. CTC Union Technologies assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. CTC Union Technologies reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

CTC Union Technologies makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does CTC Union assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

CTC Union products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a CTC Union product for any such unintended or unauthorized application, the Buyer shall indemnify and hold CTC Union Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that CTC Union Technologies was negligent regarding the design or manufacture of said product.

TRADEMARKS
Microsoft is a registered trademark of Microsoft Corp.
HyperTerminal™ is a registered trademark of Hilgraeve Inc.

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 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 in which case the user will be required to correct the interference at his own expense. NOTICE: (1) The changes or modifications not expressively approved by the party responsible for compliance could void the user's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

CISPR PUB.22 Class A COMPLIANCE:
This device complies with EMC directive of the European Community and meets or exceeds the following technical standard. EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class A.

WARNING:
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

CE NOTICE
Marking by the symbol CE indicates compliance of this equipment to the EMC directive of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards: EN 55022:1994/A1:1995/A2:1997 Class A and EN61000-3-2:1995, EN61000-3-3:1995 and EN50082-1:1997

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Technology Center (Neihu Technology Park)
8F, No. 60, Zhouzi St.
Neihu, Taipei, 114
Taiwan
Phone: +886-2-2659-1021
FAX: +886-2-2799-1355

ATU-R140

ADSL2+ SOHO Modem

User Manual
Version 1.1 Mar 2005 Released for first printing

This manual supports the following models:
ATU-R140

This document is the first official release manual. Please check CTC Union's website for any updated manual or contact us by E-mail at info@ctcu.com. Please address any comments for improving this manual or to point out omissions or errors to marketing@ctcu.com. Thank you.

Table of Contents

1. Introduction

The ATU-R140 ADSL Gateway is the perfect high-speed WAN bridge/router. This full-featured product is specifically designed to connect to the Internet and directly connect to your local area network via high speed 10/100 Mbps Ethernet or 802.11b/g. The gateway also has full NAT firewall and DMZ services to block unwanted users from accessing your network.

1.1 Features

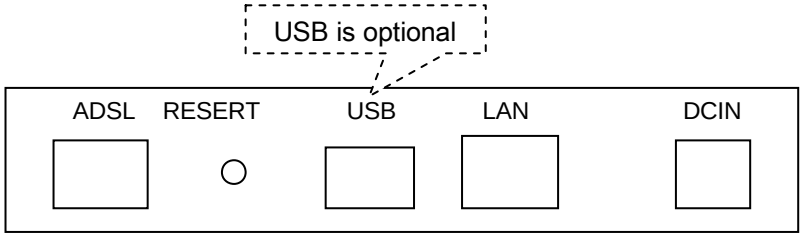
- Equipped with a 1 Port 10/100 Ethernet Switch
- Connects multiple PCs to the Internet with just one WAN IP Address (when configured in router mode with NAT enabled)
- Configurable through user-friendly web pages
- Supports Single-Session IPSec and PPTP Pass-Through for Virtual Private Network (VPN)
- Several popular games are already pre configured. Just enable the game and the port settings are automatically configured.
- Configurable as a DHCP Server on Your Network
- Compatible with virtually all standard Internet applications
- Industry standard and interoperable DSL interface
- Address Filtering, DMZ Hosting, and Much More
- Simple web based status page displays a snapshot of your system configuration, and links to the configuration pages
- Downloadable flash software upgrades
- Support for up to 8 Permanent Virtual Circuits (PVC)
- Support for up to 8 PPPoE sessions
- Supports Classical IP over ATM (CLIP or also referred to as RFC1577)

2. Gateway Overview

Your gateway has many ports, switches and LEDs. Let's take a look at the different options. Depending upon your model of gateway, your gateway may have some or all of the features listed below

2.1 Front View

2.2 Ports and Buttons



ADSL port: This is the WAN interface which connects directly to your phone line.

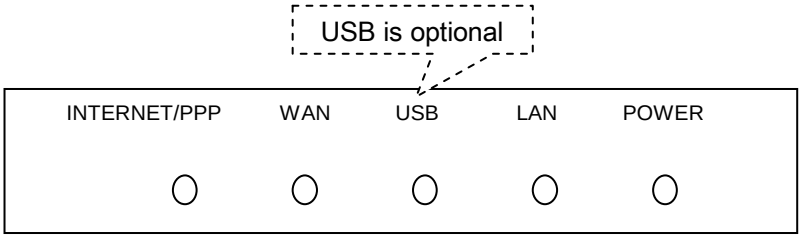
RESET: The RESET button will set the gateway to its factory default setting and reset the gateway. You may need to place the gateway into its factory defaults if the configuration is changed, you loose the ability to enter the gateway via the web interface, or following a software upgrade, and you loose the ability to enter the gateway. To reset the gateway, simply press the reset button for more than 10 seconds. The gateway will be reset to its factory defaults and after about 30 seconds the gateway will become operational again.

POWER: Connect the power adapter that came with the Gateway. Using a power supply with a different voltage rating will damage this product. Make sure to observe the proper power requirements. The power requirement is 9 volts.

LAN (local area network) port: Connect to Ethernet network devices, such as a PC, hub, switch, or router. Some gateways come with a single LAN connection and some come with four LAN connections. Depending on the connection, you may need a cross over cable or a straight through cable.

USB (universal serial port): Connects this port to a PC's USB port. The gateway only supports Window's based PCs via an RNDIS driver (included in the software).

2.3 LED Description



Power LED: The LED stays lighted to indicate the system is power on properly.

WAN LED: This LED is lighted when the WAN connection is established and flashes when the WAN port is sending/receiving data.

INTERNET/PPP LED: This LED is lighted when work under PPPoE / PPPoA mode.

LAN LED: The LED is lighted when a connection is established to LAN port and flashes when LAN port is sending/receiving data.

USB(optional) LED: The LED is lighted when a connection is established to USB port and flashes when USB port is sending/receiving data.

3. Installing Your Gateway

1. Locate an optimum location for the gateway.
2. For connections to the Ethernet and DSL interfaces, refer to the quick start guide.
3. Connect the AC Power Adapter. Depending upon the type of network, you may want to put the power supply on an uninterruptible supply. Only use the power adapter supplied with the gateway. A different adapter may damage the product.

Now that the hardware installation is complete, proceed to **Chapter 4: Setting up your gateway**

4. Setting up Your Gateway

This section will guide you through your gateway's configuration. The gateway is shipped with a standard default bridge configuration; for most users, you may want to change the gateway from a bridge to a router.

4.1 Log into Your Gateway

To configure your gateway, open your web browser. You may get an error message at this point; this is normal. Don't panic. Continue following these directions. Type the default IP address (**192.168.1.1**) Press the **Enter** key and the following screen, shown in Figure 1 will appear. The default user name is **Admin** (case sensitive) and the password is **Admin** (case sensitive).

Note: Before setting up your gateway, make sure you have followed the quick start guide. You should have your computers configured for DHCP mode and have proxies disabled on your browser. Also if you access the Gateway, and instead of getting a login screen, the browser instead displays a login redirection screen, you should check your browser's setting, and verify that JavaScript support is enabled. Also, if you do not get the screen shown in Figure 1, you may need to delete your temporary Internet files (basically flush the cached web pages).

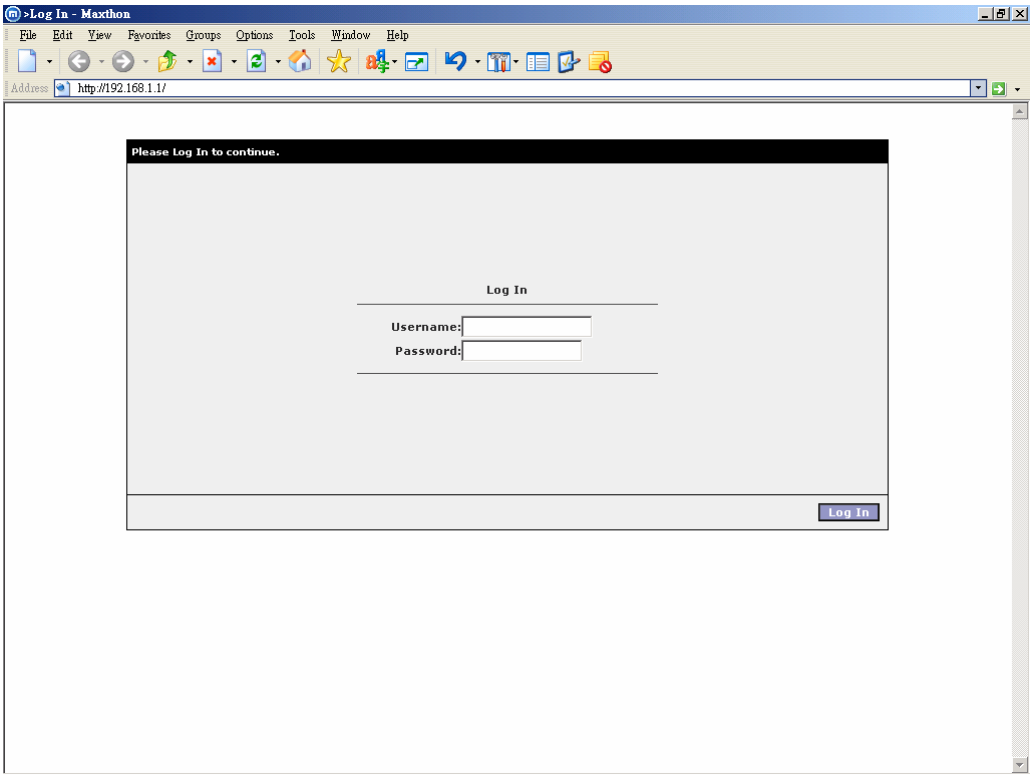


Figure 1 (Log-in screen)

4.2 Home Screen

The first screen (Figure 2) that appears (after the log in screen) is the Home screen. From this screen the user can setup the modem (configure the LAN and WAN connection(s), configure the advanced configuration options within the modem (security, routing, and filtering), access

tools that are helpful for debug purposes, obtain the status of the modem, and view the extensive online help.

The basic layout of the Home page consists of a page selection list across the top of the browser window. The footer displays gateway status, connection information, and other useful information. The center display is where most of the configuration will take place.

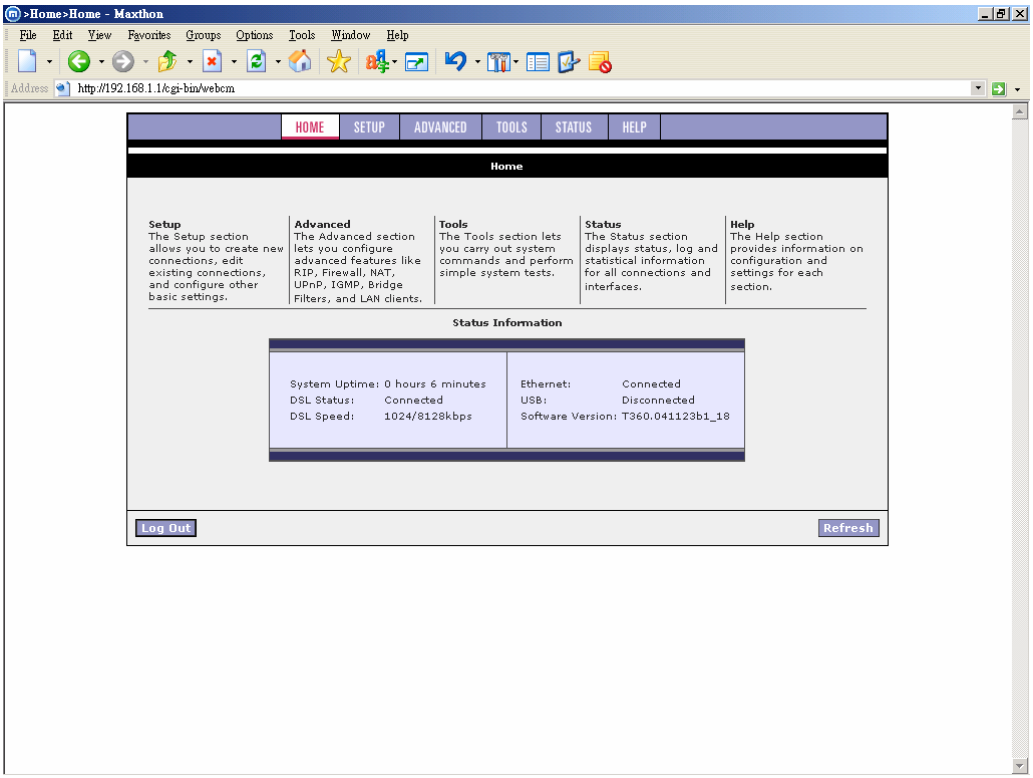


Figure 2 (Home page)

4.3 Setup

To setup your gateway with a basic configuration, from the Home page, select Setup. Figure 3 illustrates the setup page. The page is broken into two subsections the WAN configuration and the LAN configuration.

Before configuring the Gateway, there are several concepts that you should be familiar with on how your new Gateway works. Please take a moment to familiarize yourself with these concepts, as it should make the configuration much easier.

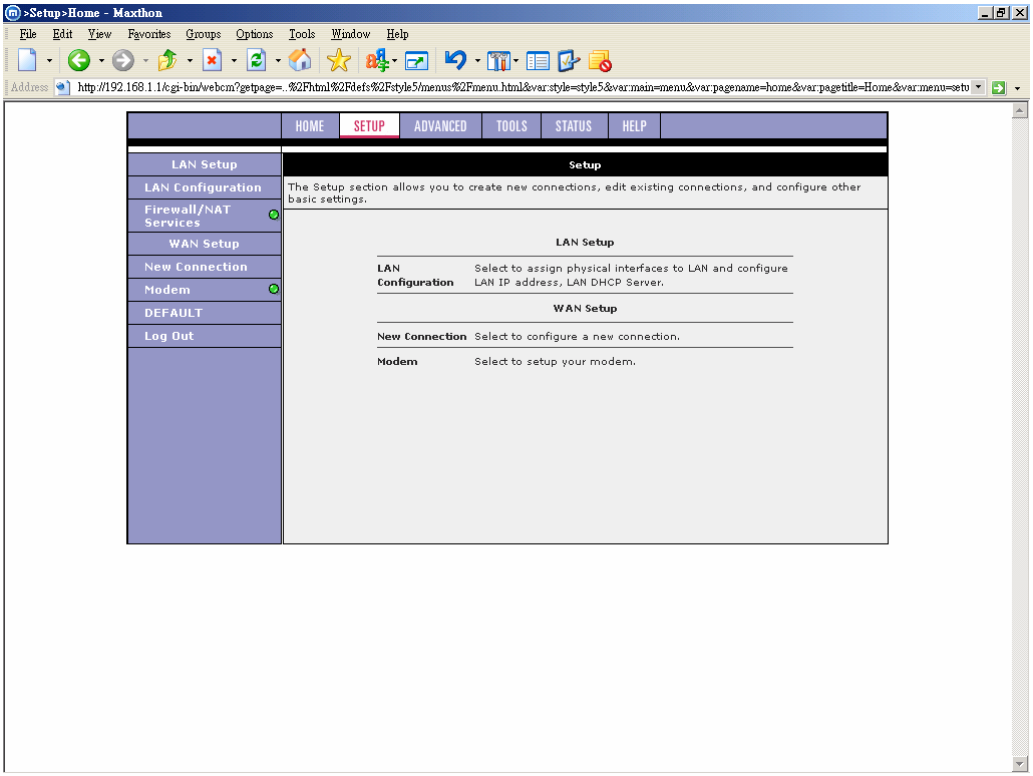


Figure 3 (Setup page)

4.3.1 Wide Area Network Connection

On the other side of the Gateway is where your Wide Area Network (WAN) connection; also referred to as a broadband connection. This WAN connection is different for every WAN supplier. Most of the configuration you will perform will be in this area.

4.3.2 Local Area Network Connection

On one side of your Gateway, you have your own Local Area network (LAN) connections. This is where you plug in your local computers to the Gateway. The Gateway is normally configured to automatically provide all the PC's on your network with Internet addresses.

4.4 Configuring the WAN

Before the gateway will pass any data between the LAN interface(s) and the WAN interface, the WAN side of the modem must be configured. Depending upon your DSL service provider or your ISP, you will need some (or all) of the information outlined below before you can properly configure the WAN:

- Your DSL line VPI and VCI
- Your DSL encapsulation type and multiplexing
- Your DSL training mode (default is MMODE)

For **PPPoA** or **PPPoE** users, you also need these values from your ISP:

- Your username and password

For **RFC 1483** users, you may need these values from your ISP:

- Your DSL fixed Internet IP address
- Your Subnet Mask
- Your Default Gateway
- Your primary DNS IP address

4.4.1 New Connection

A new connection is basically a virtual connection. Your gateway can support up to 8 different (unique) virtual connections. If you have multiple different virtual connections, you may need to utilize the static and dynamic routing capabilities of the modem to pass data correctly.

4.4.1.1 Bridged gateway profile and Connection

A pure bridged connection does not assign an IP address to the WAN interface. NAT and firewall rules are not enabled. This connection method makes the Gateway act as a hub, and just passes packets across the WAN interface to the LAN interface.

To configure the gateway as a bridge, from the Home page, click on Setup and then click on New Connection. The default PPPoE connection setup is displayed. At the Type field select Bridge and the Bridge connection setup page is displayed (see Figure 4). Give your Bridge connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called bridge1. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using 0,35. Also select the quality of service (QOS); leave the default value if you are unsure or the ISP did not provide this information.

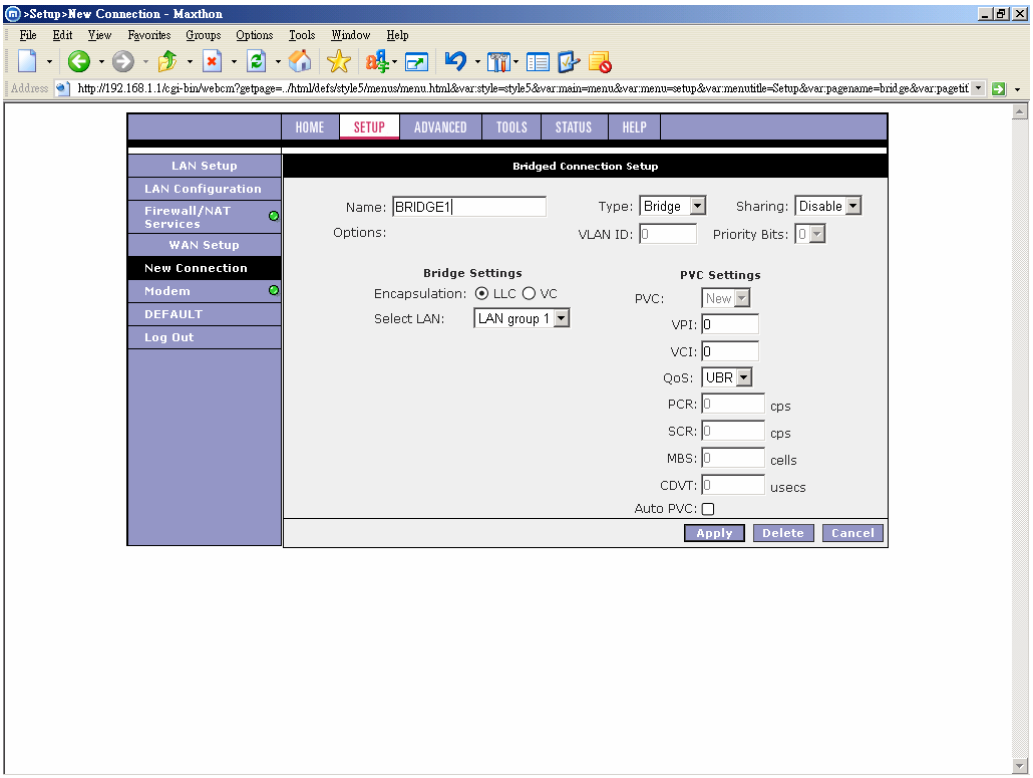


Figure 4 (Bridge Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.4.1.2 PPPoA Connection Setup

PPPoA is also known as RFC 2364. It is a method of encapsulating PPP packets over ATM cells which are carried over the DSL line. PPP or Point-to-Point protocol is a method of establishing a network connection / session between network hosts. It usually provides a mechanism of authenticating users. LLC and VC are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.

By selecting PPPoA, you are forcing your gateway to terminate the PPPoA connection. The advantage is that the PPPoA termination is done within the gateway and not on your PC; this frees up your PC resources and allows multiple users to utilize the PPPoA connection.

To configure the gateway for PPPoA, click on Setup and then click on New Connection. The default PPPoE connection setup is displayed. At the Type field select PPPoA and the PPPoA connection setup page is displayed; figure 5 illustrates a typical PPPoA configuration. Give your PPPoA connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called PPPOA1. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using 0,40. Also select the quality of service (QOS); leave the default value if you are unsure or the ISP did not provide this information.

Following is a description of the different options:

a. Username: The username for the PPPoA access; this is provided by your DSL service provider or your ISP.
b. Password: The password for the PPPoA access; this is provided by your DSL service provider or your ISP.
c. On-Demand: Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.
d. Idle Timeout: Specifies that PPPoA connection should disconnect if the link has no activity detected for n seconds. This field is used in conjunction with the On-Demand feature. To ensure that the link is always active, enter a 0 in this field.
e. Keep Alive: When on-demand option is not enable, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a 0 in this field.
f. Default Gateway: Specify this connection as the default-gateway.
g. MRU: Maximum Receive Unit the DSL connection can receive. It is a negotiated value that asks the provider to send packets of no more than n bytes. The maximum specified value is 1500 although some DSL/ISP providers require a larger value. The minimum MRU value is 128.
h. Debug: Enables PPPoA connection debugging facilities. Debugging is talked about later.
i. PPP Unnumbered: Some ISPs provide unnumbered service for special purpose.

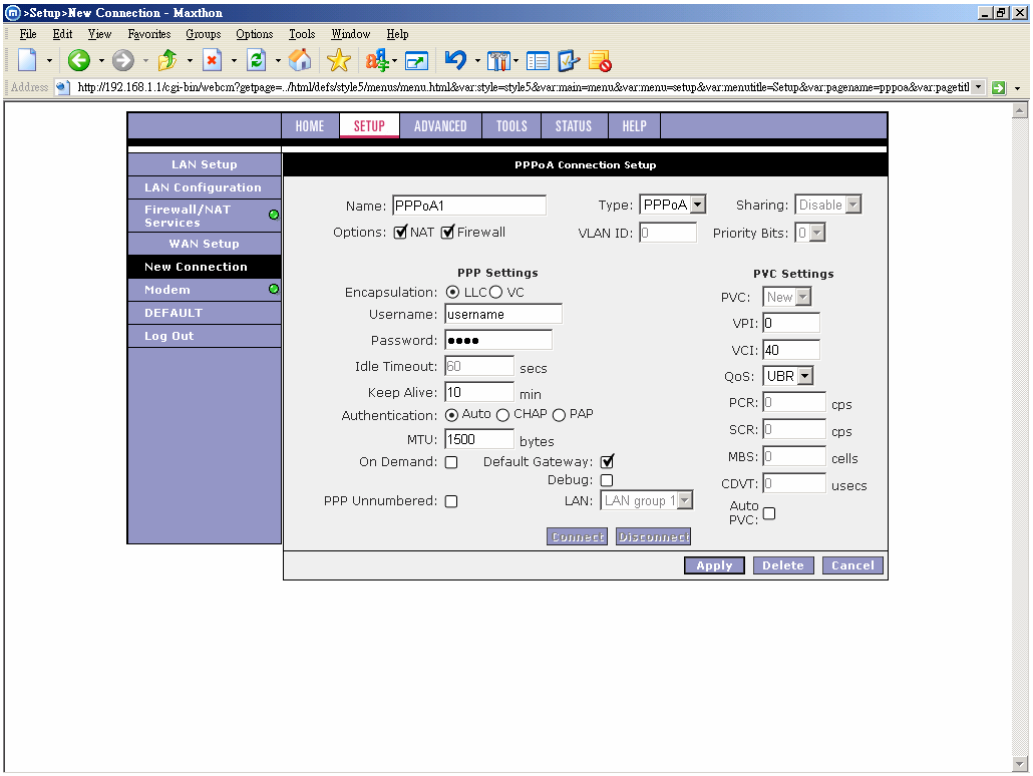


Figure 5 (PPPoA Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.4.1.3 PPPoE Connection Setup

PPPoE is also known as RFC 2516. It is a method of encapsulating PPP packets over Ethernet. PPP or Point-to-Point protocol is a method of establishing a network connection/session between network hosts. It usually provides a mechanism of authenticating users.

To configure the gateway for PPPoE, click on Setup and then click on New Connection. The default PPPoE connection setup is displayed. At the Type field select PPPoE and the PPPoE connection setup page is displayed; figure 6 illustrates a typical PPPoE configuration. Give your PPPoE connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called PPPOE1. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using 0,35. Also select the quality of service (QOS); leave the default value if you are unsure or the ISP did not provide this information.

Following is a description of the different options:

a. Username: The username for the PPPoE access; this is provided by your DSL service provider or your ISP.
b. Password: The password for the PPPoE access; this is provided by your DSL service provider or your ISP.
c. On-Demand: Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.
d. Idle Timeout: Specifies that PPPoE connection should disconnect if the link has no activity detected for n seconds. This field is used in conjunction with the On-Demand feature. To ensure that the link is always active, enter a 0 in this field.

e. Keep Alive: When on-demand option is not enable, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a 0 in this field.
f. Default Gateway: Specify this connection as the default-gateway.
g. MRU: Maximum Receive Unit the DSL connection can receive. It is a negotiated value that asks the provider to send packets of no more than n bytes. The maximum specified value is 1500 although some DSL/ISP providers require a larger value. The minimum MRU value is 128.
h. Enforce MRU: Check this box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MRU by changing TCP Maximum Segment Size to PPP MRU.
i. Debug: Enables PPPoE connection debugging facilities. Debugging is talked about later.
j. PPP Unnumbered: Some ISPs provide unnumbered service for special purpose.

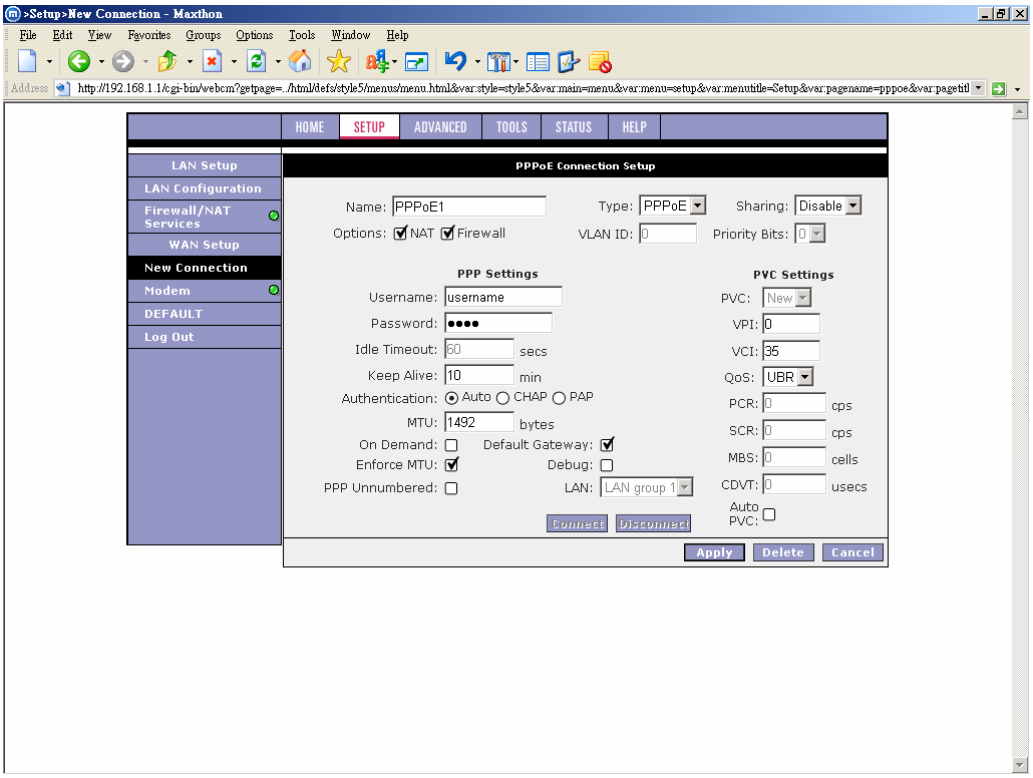


Figure 6 (PPPOE Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.4.1.4 DHCP Connection Setup

Dynamic Host Configuration Protocol (DHCP) allows the gateway to automatically obtain the IP address from the server. This option is commonly used in situations where IP is dynamically assigned and is not known prior to assignment.

To configure the gateway for a DHCP connection, click on Setup and then click on New Connection. The default DHCP connection setup is displayed. At the Type field select DHCP and the DHCP connection setup page is displayed; figure 7 illustrates a typical DHCP configuration. Give your DHCP connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called DHCP1. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using 0,35. Also select the quality of service (QOS); leave the default value if you are unsure or the ISP did not provide this information.

If your DSL line is connected and your DSL/ISP provider is supporting DHCP, you can click the renew button and the gateway will retrieve an IP address, Subnet mask, and Gateway address. At anytime, you can renew the DHCP address by clicking on the renew button; in most cases you will never have to use this button.

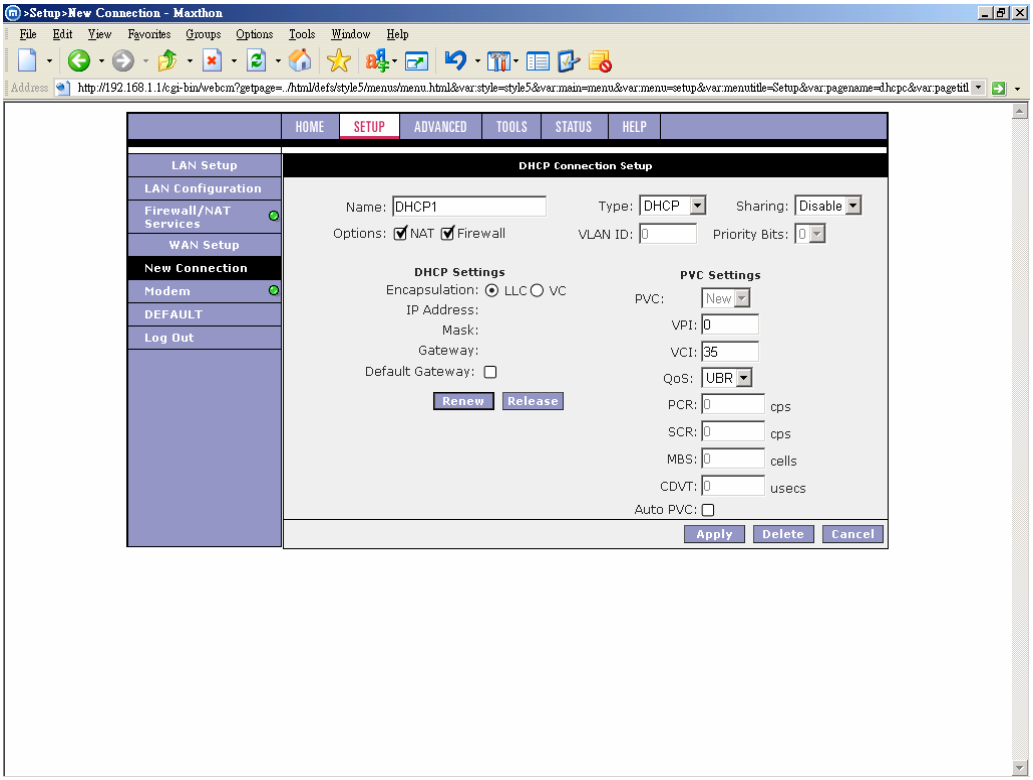


Figure 7 (DHCP Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.4.1.5 Static Connection Setup

Static is used whenever a known static IP is assigned. The accompanying information such as the Subnet mask and the gateway should also be specified. Up to three Domain Name Server (DNS) addresses can also be specified. These servers would enable you to have access to other web servers. Valid IP addresses range is from 0.0.0.0 to 255.255.255.255.

To configure the gateway for a Static connection, click on Setup and then click on New Connection. The default Static connection setup is displayed. At the Type field select Static and the Static connection setup page is displayed; figure 8 illustrates a typical Static configuration. Give your Static connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called STATIC1. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using 0,35. Also select the quality of service (QOS); leave the default value if you are unsure or the ISP did not provide this information. You can also enable Network Address Translation (NAT) and the Firewall options. If you are unsure, leave these in the default mode.

Based upon the information your DSL/ISP provided, enter your assigned IP address, Subnet Mask, Default Gateway (if provided), and Domain Name Services (DNS) values (if provided). For the static configuration, you can also select a bridge connection or a routed connection. Since static IP address is typically used to host WEB servers, you may want to use a bridge connection.

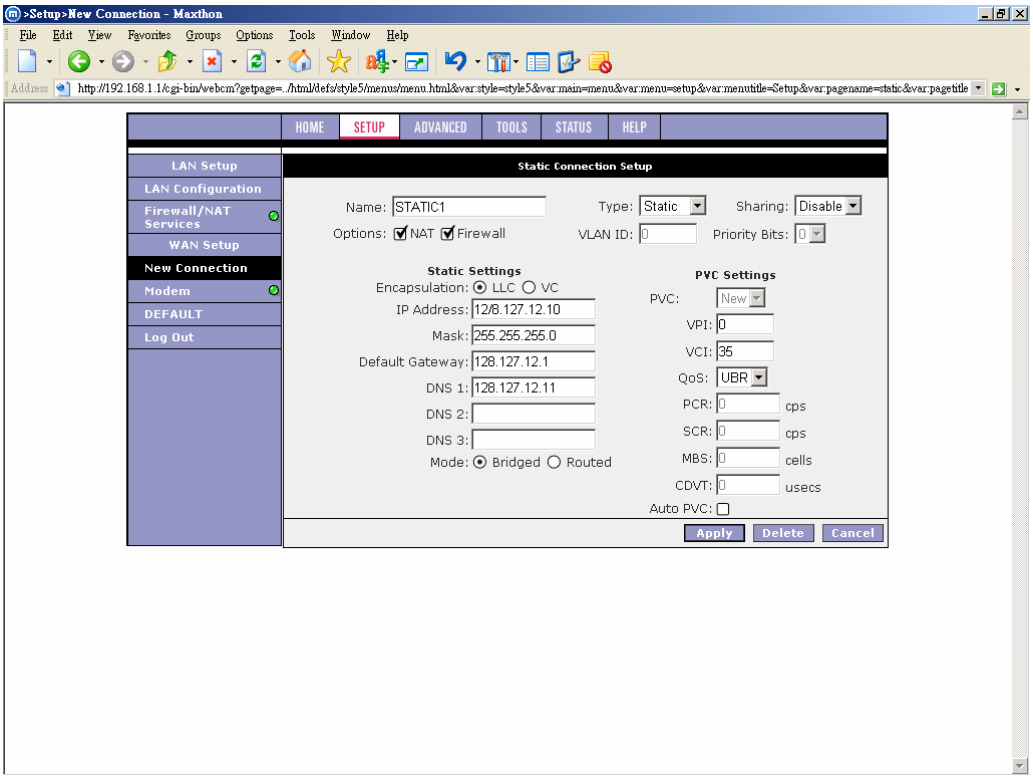


Figure 8 (Static IP Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.4.1.6 Classical IP over ATM Connection Setup

The Classical IP over ATM (CLIP) support provides the ability to transmit IP packets over an ATM network, ATU-R140 ADSL Gateway's CLIP support will encapsulate IP in an AAL5 packet data unit (PDU) frame using RFC1577and it utilizes an ATM aware version of the ARP protocol. (ATMARP. ATU-R140 ADSL Gateway's CLIP support only allows for PVC support; it does not support SVC.)

To configure the gateway for a CLIP connection, click on Setup and then click on New Connection. The default CLIP connection setup is displayed. At the Type field select CLIP and the CLIP connection setup page is displayed; figure 9 illustrates a typical CLIP configuration. Give your CLIP connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called CLIP1. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using 0,35. Also select the quality of service (QOS); leave the default value if you are unsure or the ISP did not provide this information.

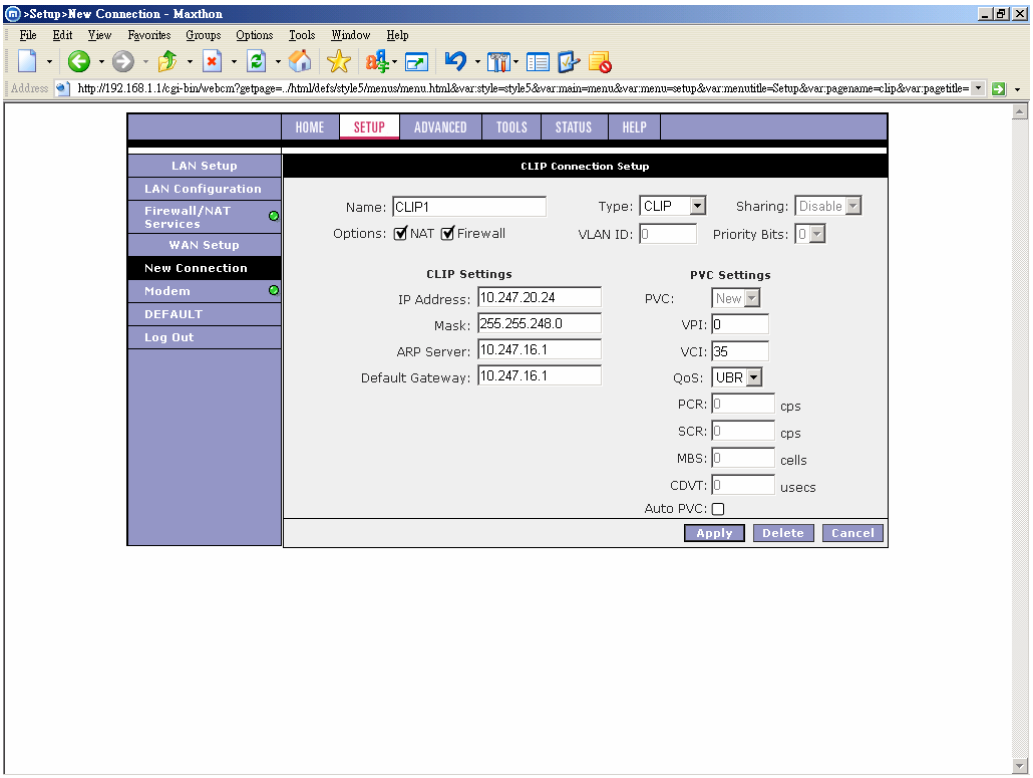


Figure 9 (CLIP Connection Setup)

To complete the connection you must now click the apply button. The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.4.2 Modify an Existing Connection

To modify an existing connection, from the Home screen, click setup and then click the connection you want to modify. The connections are listed as Connection 1 through Connection 8.

As a note, if you delete the connection, to make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.4.3 Modem Setup

To configure the DSL modulation type, go to the Home screen, Click setup. Under WAN Setup, select Modem Setup. This will bring up the modem setup screen. Leave the default value if you are unsure or the DSL/ISP did not provide this information. For most all cases, this screen should not be modified.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.5 Configuring the LAN

By default, your gateway has DHCP server (LAN side) enabled. If you already have a DHCP server running on your network, you *must* disable one of the two DHCP servers; if you plug a second DHCP server into the network, you will experience network errors and the network will not function normally. Click setup. Under LAN Setup, select LAN Configuration. This will bring up the screen shown in Figure 10.

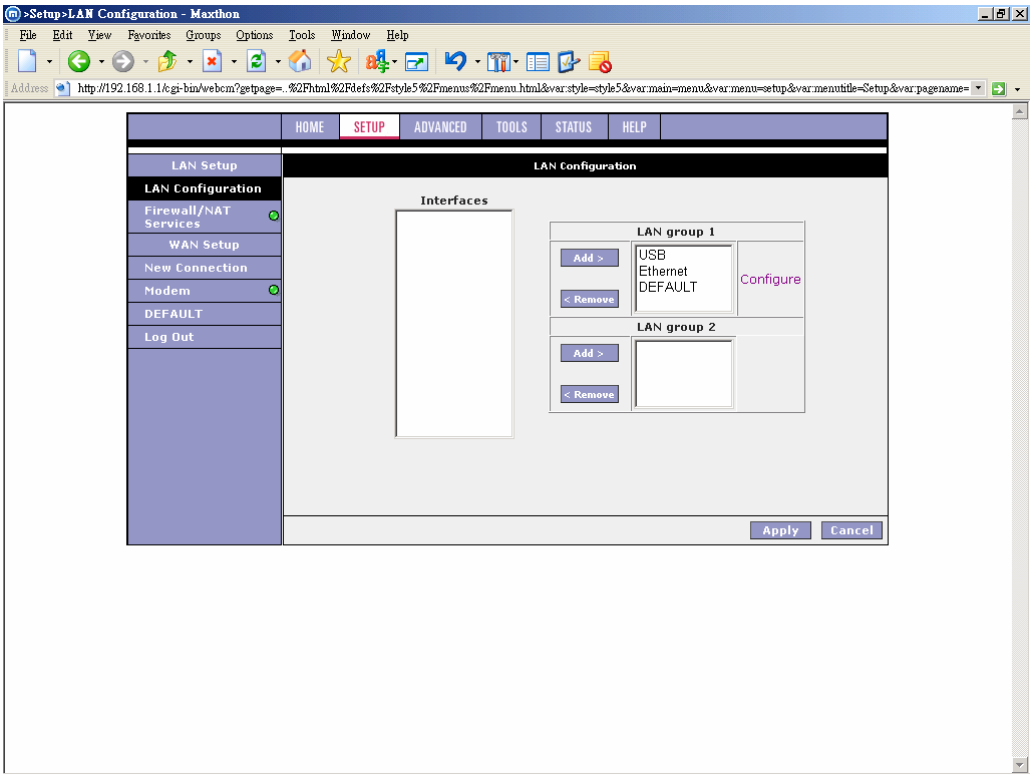


Figure 10 (LAN configuration)

4.5.1 Enable/Disable DHCP

To enable or disable DHCP go to the Home screen. Click setup and under LAN Setup, select LAN Configuration, press Configure. This will bring up the screen shown in Figure 12.

The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the gateways IP address value. For example if the gateways IP address is 192.168.1.1 (default) than the starting IP address must be 192.168.1. 2 (or higher).

The End IP Address is where the DHCP server stops issuing IP addresses. The ending address cannot exceed a subnet limit of 254. Hence the max value for our default gateway is 192.168.1.254. If the DHCP server runs out of DHCP addresses, users will not get access to network resources. If this happens you can increase the Ending IP address (to the limit of 255) or reduce the lease time.

The Lease Time is the amount of time a network user will be allowed connection to the Gateway with their current dynamic IP address. The amount of time is in units of seconds; the default value is 3600 seconds (1 hour).

Note: If you change the start or end values, make sure the values are still within the same subnet as the gateways IP address. In other words, if the gateways IP address is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.128.1.2/192.128.1.100, you will not be able to communicate to the gateway if your PC has DHCP enabled.

In addition to the DHCP server feature, the gateway supports the DHCP relay function. When the gateway is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the gateway is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server. See figure 11.

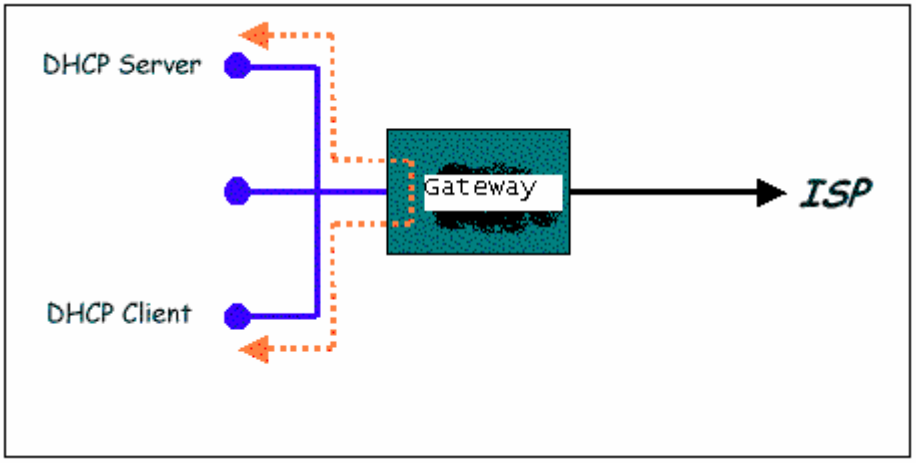


Figure 11 (Example of a DHCP Relay configuration)

By turning off the DHCP server and relay the network administrator must carefully configure the IP address, Subnet Mask and DNS settings of every computer on your network. Do not assign the same IP address to more than one computer and your Gateway must be on the same subnet as all the other computers.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.5.2 Changing the gateways IP address

You can change the gateway's IP address by going to the Home screen, click setup and under LAN Setup, select LAN Configuration, press Configure. This will bring up the screen shown in Figure 12.

4.5.2.1 Static IP address assignment

Your gateway's default IP address and subnet mask are 192.168.1.1/255.255.255.0; this subnet mask will allow the gateway to support 254 users. If you want to support a larger number of users you can change the subnet mask; but remember. The DHCP server is defaulted to only give out 255 IP addresses. Further remember that if you change your gateways' IP address and you have DHCP enabled, the DHCP configuration must reside within the same subnet.

The hostname can be any alphanumeric word that does not contain spaces. The domain name is used to in conjunction with the host name to uniquely identify the gateway. To access the gateway's web pages the user can type 192.168.1.1 (the gateway's default IP address) or type mygateway1.ar7.

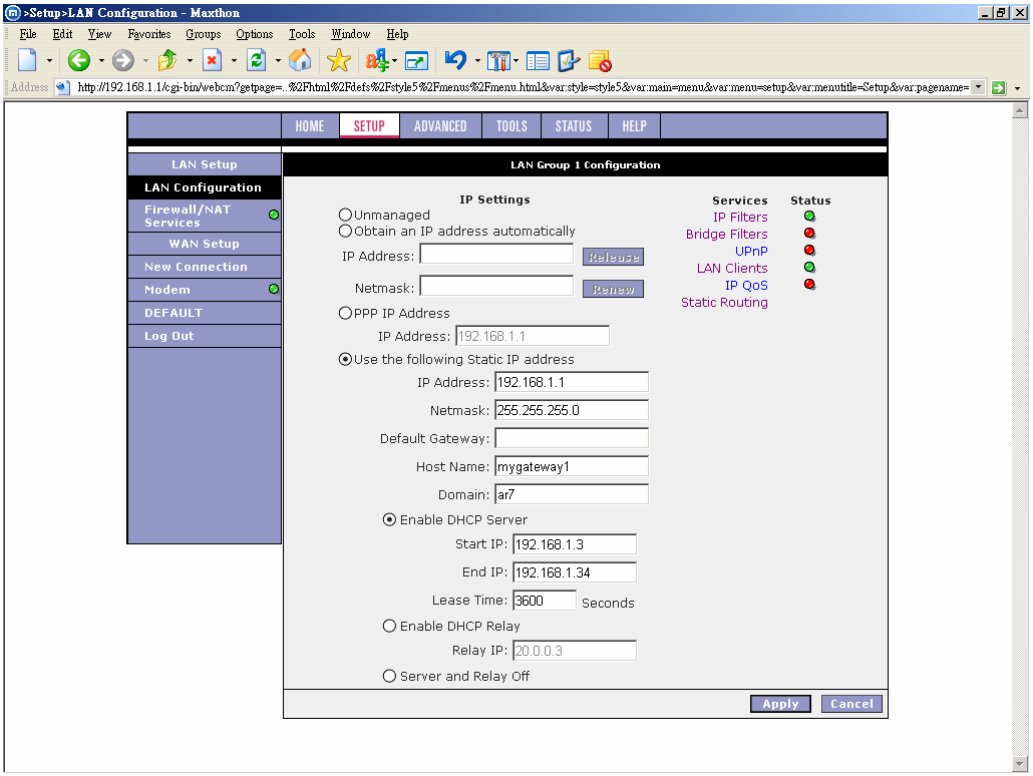


Figure 12 (LAN IP address)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.5.3 Firewall/NAT Services

You can enable or disable Firewall and NAT by going to the Home screen, click setup and under LAN Setup, select Firewall/NAT Services. By unselecting the "Enable Firewall and NAT Services" button the firewall and NAT services is disabled for all WAN connections.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.6 Advanced

The gateway supports a host of advanced features. For basic Gateway functionality, the user does not need to utilize these advanced features. The features help with routing, security, port configuration, and plug and play capability.

4.6.1 UPnP

UPnP NAT and Firewall Traversal allow traffic to pass-thru the Gateway for applications using the UPnP protocol. This feature requires one active DSL connection. In presence of multiple DSL connections, select the one over which the incoming traffic will be present, for example the default Internet connection.

To enable UPnP, you must first have a WAN connection configured. Once a WAN connection is configured, from the Home screen, click Advanced and under Advanced, select UPnP. This will bring up the screen shown in Figure 13. You must enable UPnP and then select which connection will utilize UPnP.

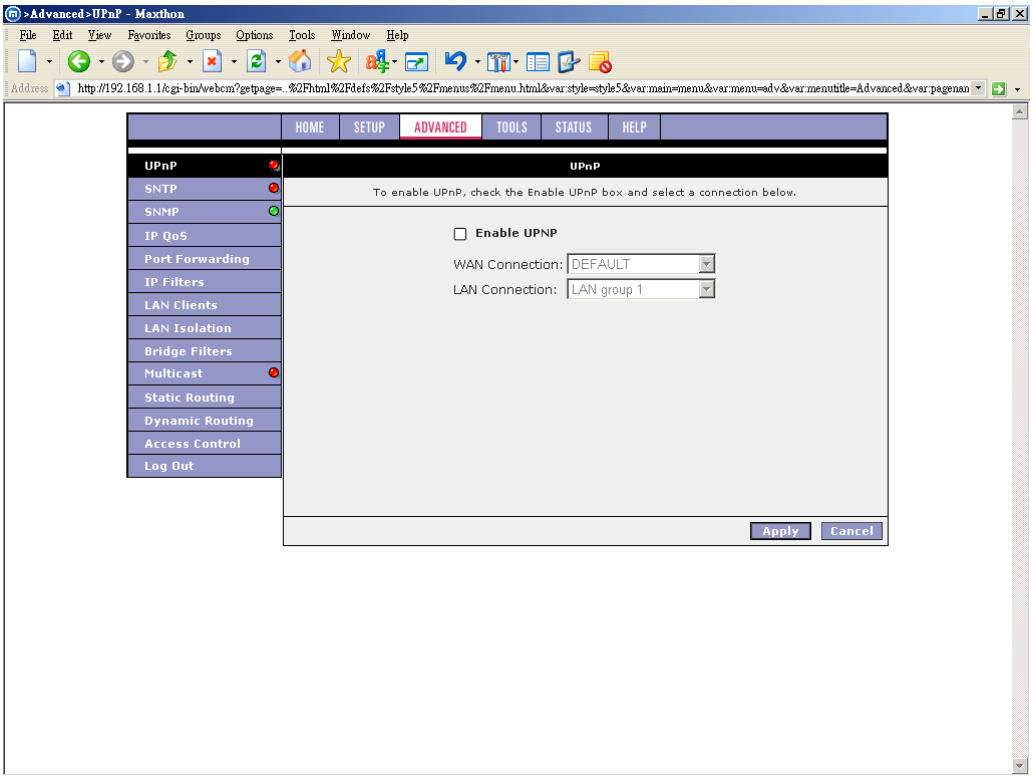


Figure 13 (UPnP)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.6.2 SNTP

Simple Network Time Protocol(SNTP) which is an adaptation of the Network Time Protocol (NTP) used to synchronize clocks in the Internet.

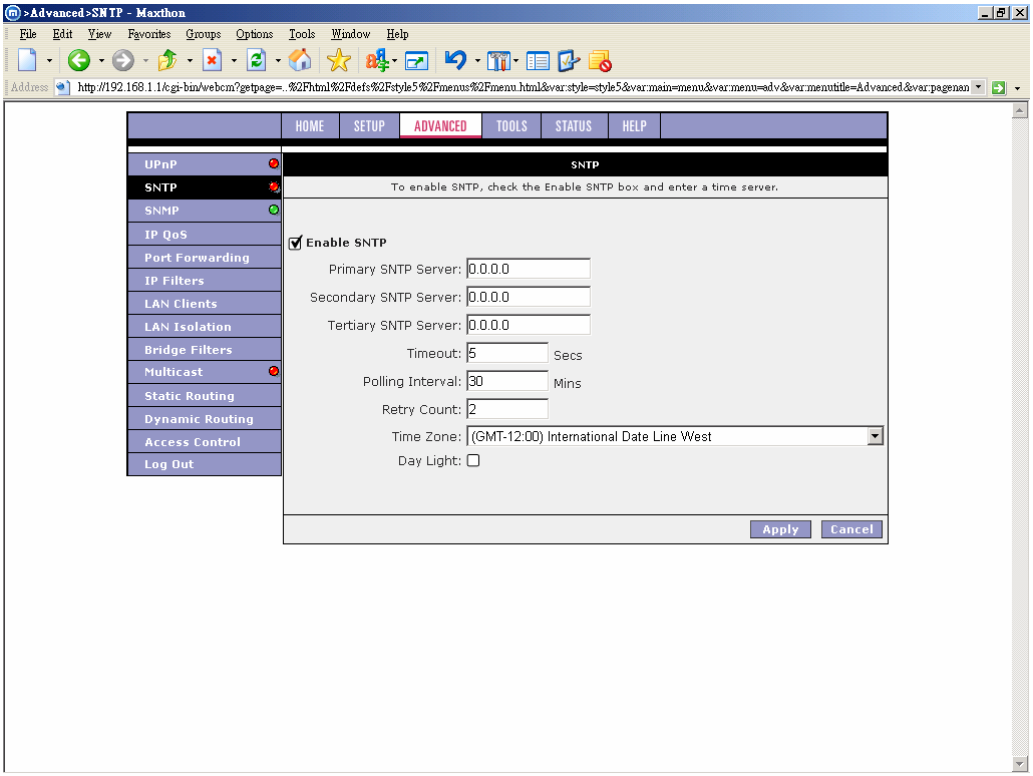


Figure 14 (SNTP)

4.6.3 SNMP

SNMP management feature comes with SNMP agent built. The agent provides management information to the Network Management Station by keeping track of various operational aspects of gateway.

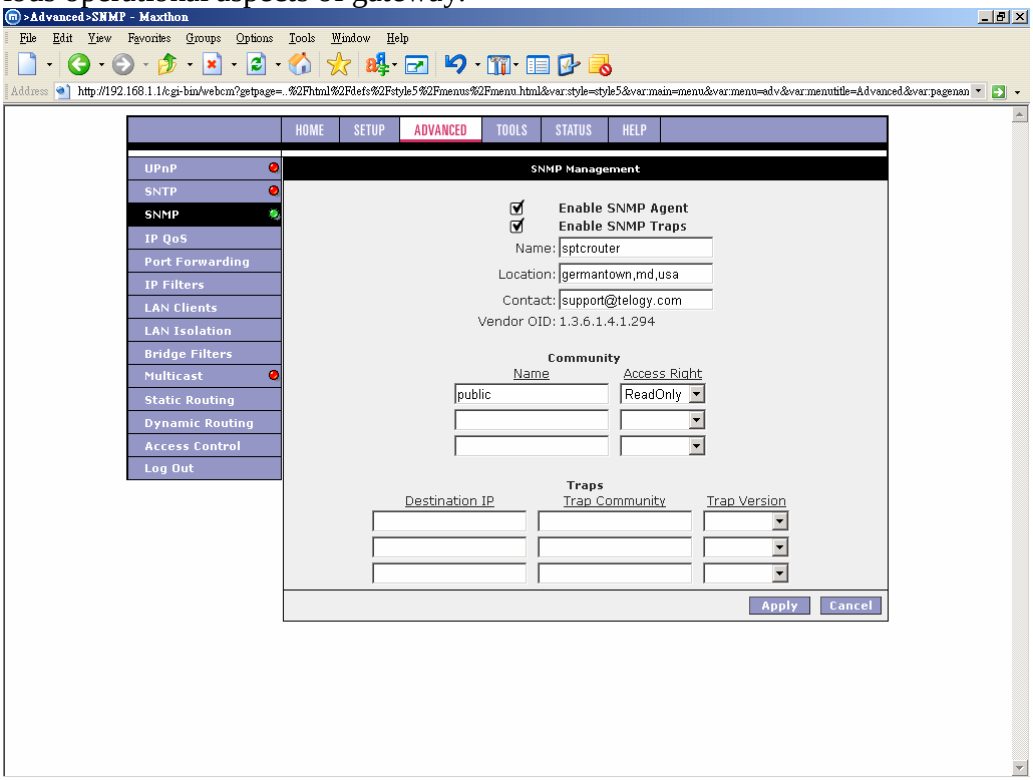


Figure 15 (SNMP)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.6.4 IP QoS

IP QoS services in the NSP is applicable to the output device (Egress side). Meaning the IP QoS traffic shaping is associated with any transmitted traffic from the perspective of the NSP. Each output device has 3 priority queues associated with transmit data. The High priority queue has strict priority over medium and low priority queues. The Medium and Low priority queues are serviced on a Round Robin priority basis according to the configured weights (WRR), after the High priority queue has been completely serviced.
The "IP QoS" section under "Advanced section" allows you to setup IP QoS for a connection. The "IP QoS" section has two sub-sections - QoS Setup Page and Rule Setup Page.

4.6.4.1 QoS Setup

The QoS setup page allows you to configure IP QoS for a connection, to view the configured QoS rules and to add/delete a QoS rule.
Choose a connection: This field allows you choose a connection from the list of available connections. For e.g. Choose a WAN connection to enable IP QoS for the Upstream traffic of the Modem. On the other hand choose the LAN connection (Ethernet and USB Bridged) for the downstream traffic.
Low/Medium priority weights: These 2 fields will allow you to select the weights of the Medium and Low priority queues in increments of 10 percent, so that that the sum of the weights of these 2 queues is equal to 100 percent.
Enable IP QoS: This field allows you to enable/disable IP QoS for the chosen connection.
Trusted Mode: The NSP has two primary modes of operation with regard to queue traffic prioritization - Trusted and Un-trusted. This field allows you to choose the mode - Trusted (checked) and Un-trusted (Unchecked).
In "Trusted mode" all the rules will be applied first, regardless of the setting of the TOS bits. After the rules have been exhausted the existing TOS bit settings will be honored. The "Un-trusted" mode will match first against all rules as in "Trusted" mode. The difference is that if there is no match then a default rule will be used. The default rule will have an associated queuing priority - Low.
Rules section: This section displays a list of configured rules, allows you to add a new rule and allows you to delete an existing rule.
Each rule is a Matching criteria that identifies an Application traffic to be transmitted by the NSP using one of the 3 Priority Queues - High, Medium and Low.

Note: If IP QoS is enabled and no rules are defined, a Default Rule is added which is hidden. The Default Rule puts all the Traffic to be transmitted in the Low Priority Queue.

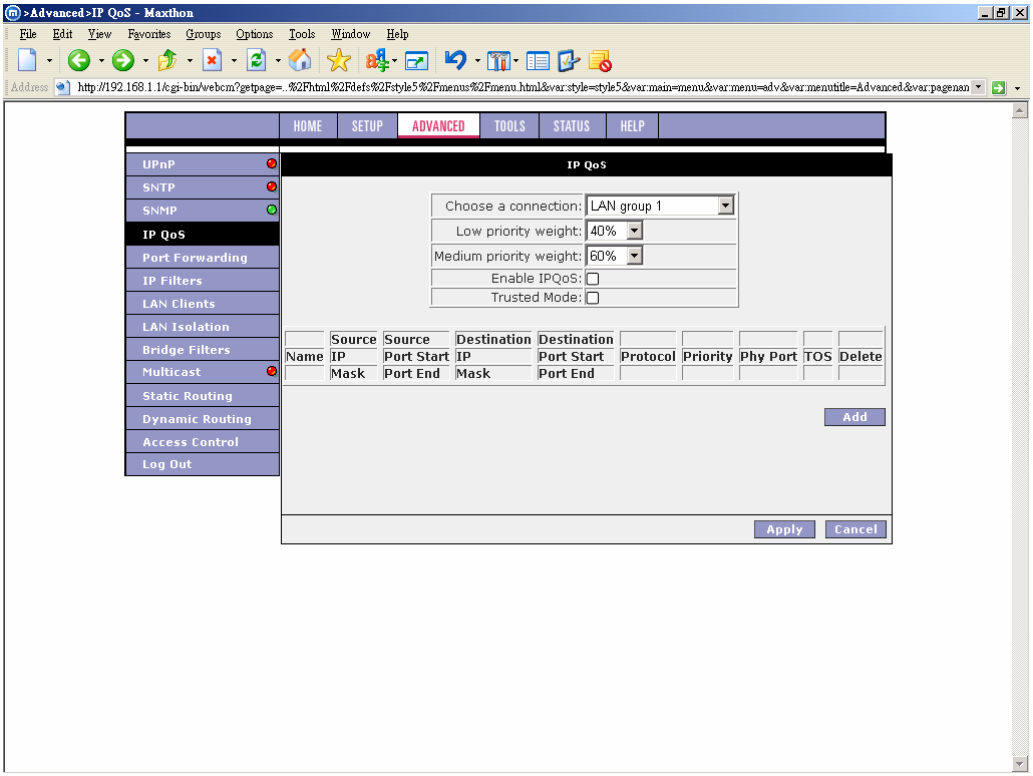


Figure 16 (IP QoS)

4.6.4.2 Rule Setup

This page is invoked when you click on the "Add" button of "QoS Setup Page". This page allows you add a Rule or Matching criteria that identifies an Application traffic. The Application traffic can be identified by Rule Name, Source/Destination IP Address and Netmask, Source/Destination Port range, Protocol and Traffic Priority.
The Traffic Priority field corresponds to the Priority Queue (High/Medium/Low) for for this traffic. The possible options for Protocol are - ANY, ICMP, TCP and UDP. Wildcard(*) entries are allowed for IP Address/Netmask and Port range fields.
The additional TOS marking field allows you to assign a TOS value to this traffic. The values for the TOS marking can be - No Change, Normal Service, Minimize monetary cost, Maximize reliability, Maximize throughput and Minimize delay.

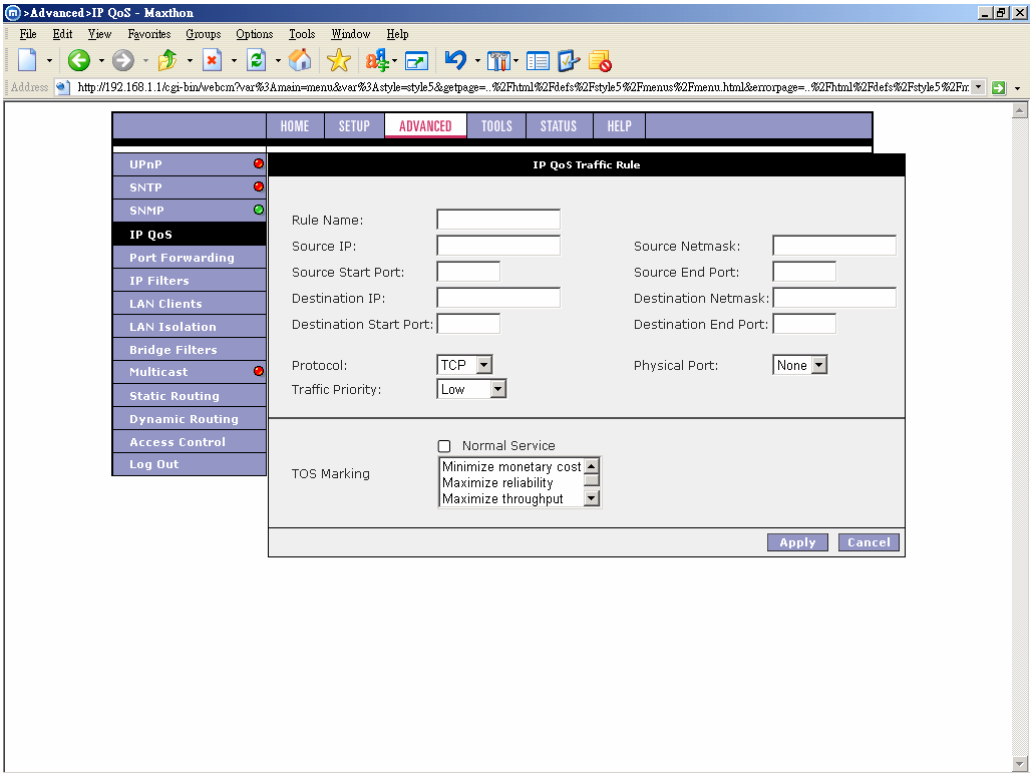


Figure 17 (IP QoS Traffic Rule)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.6.5 Port Forwarding

Using the Port Forwarding page, you can provide local services (for example web hosting) for people on the Internet or play Internet games. When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate PC. Port forwarding can be used with DHCP assigned addresses but remember that a DHCP address is dynamic (not static). For example, if you were configuring a netmeeting server, you would want to assign this server a static IP address so that the IP address is not reassigned. Also remember that if an Internet user is trying to access an Internet application, they must use the WAN IP address. The port forwarding will translate the WAN IP address into a LAN IP address.

To configure a service, game, or other application select the external connection (for example the Internet connection), from the Home screen, click Advanced and under Advanced, select Port Forwarding. Next select the computer hosting the service and add the corresponding firewall rule. If you want to add a custom application, select the User category, click New and fill in the port, protocols and description for your application.

For example, if you want to host a Netmeeting session, from the Home screen, click Advanced and under Advanced, select Port Forwarding. First select the IP address for your Netmeeting server. Next select the Audio/Video category and add Netmeeting to the applied rules box. To view the management rules, highlight Netmeeting and select view; this will display the pre configured protocols and ports that Netmeeting will use. Now assuming that your WAN connection is correct, you can run Netmeeting from your server and call users that are on the Internet. If you know your WAN IP address, users can call you. Figure 18 illustrates a typical Port Forwarding configuration.

4.6.5.1 DMZ configuration

Setting a computer (on your local network) as a DMZ forwards any network traffic that is not redirected to another computer via the port-forwarding feature to the computer's IP address. This opens the access to the DMZ computer from the Internet.

4.6.5.2 Enable Incoming ICMP Ping

Enabling the Incoming Internet Control Message Protocol (ICMP) Ping will allow Echo requests to come into the gateway. The gateway will respond with an ICMP Echo response message. The option allows the DSL provider or ISP to determine the following:

a. The status of the network.
b. Tracking and isolating hardware and software problems.
c. Testing, measuring, and managing networks.

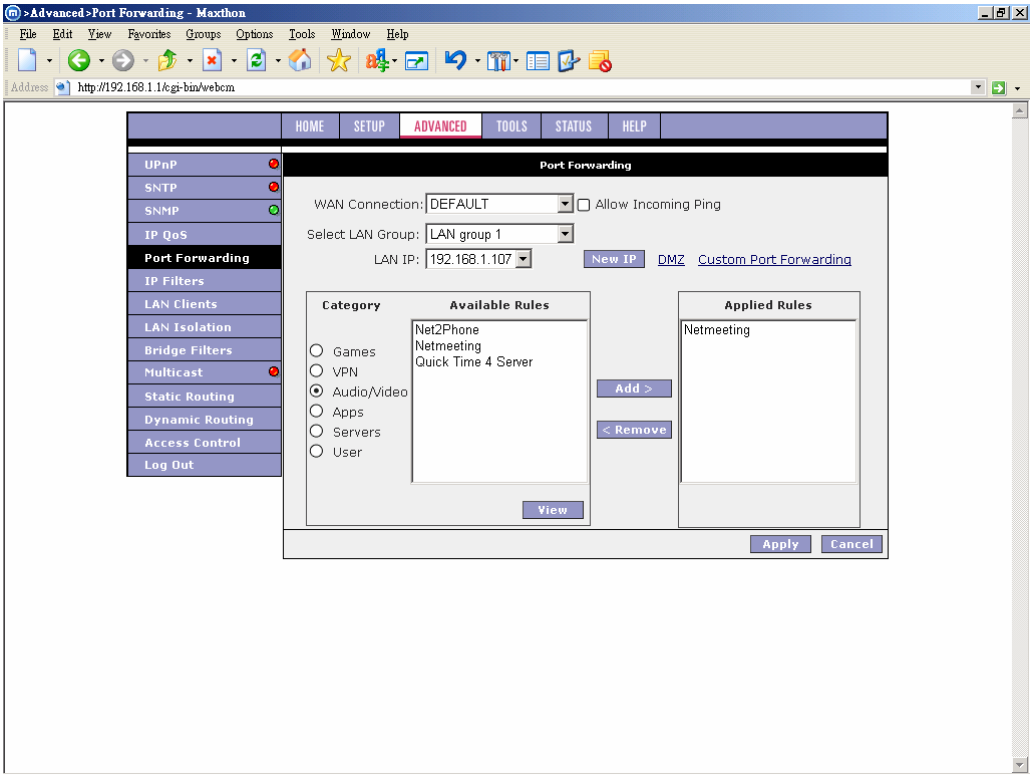


Figure 18 (Port Forwarding: Netmeeting)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.6.6 IP Filters

IP Filters can also be called port blocking. Specific types of traffic that is destined can be blocked. To enable any of the IP Filters features, from the Home screen, click Advanced and under Advanced, select IP Filters. A page similar to the port-forwarding page appears. Similar to the port-forwarding page, an IP address can be added to a rule. All IP Filters rules have precedence over rules that were added via the port-forwarding page. In the presence of the firewall, anonymous Internet traffic is blocked. The Gateway's firewall and NAT services (port forwarding, IP filters) can be disabled for all interfaces by un-checking the "Enable Firewall and NAT Service"

To enable any of the advanced security features, from the Home screen, click Advanced and under Advanced, select IP Filters. Figure 19 illustrates the typical IP Filters configuration.

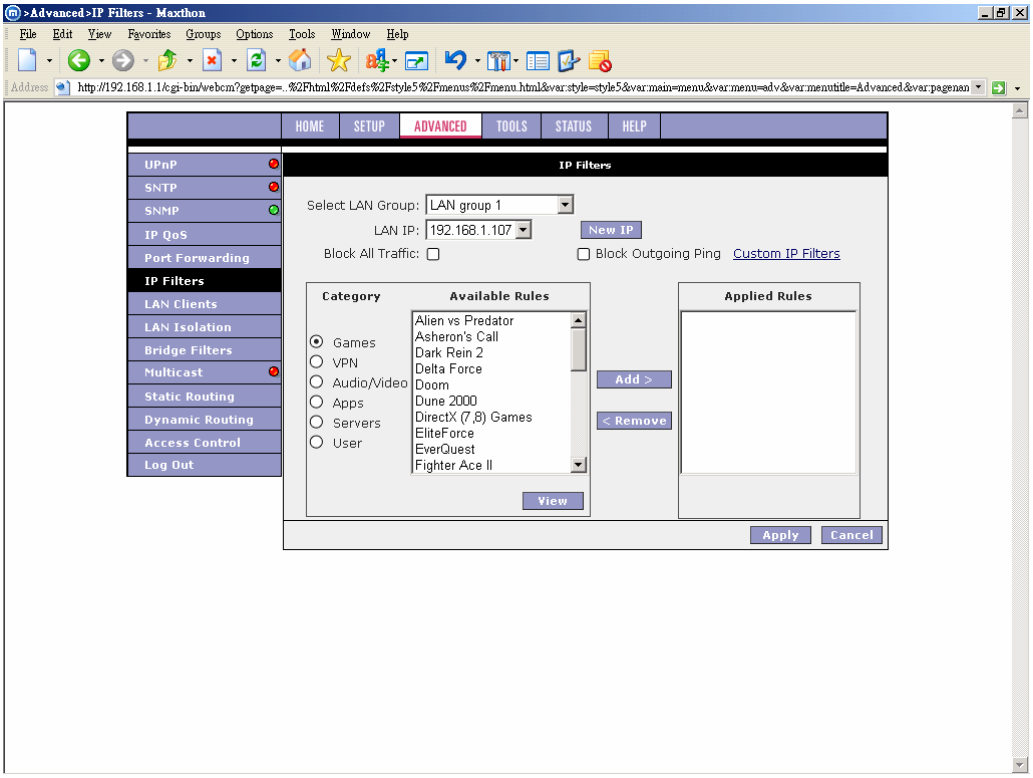


Figure 19 (IP Filters)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.6.7 LAN clients

To add a LAN client, from the Home screen, click Advanced and under Advanced, select LAN Clients. If DHCP is used, all DHCP clients are automatically assigned. If a fixed IP address server is on the LAN and you want this server to be visible via the WAN, you must add its IP address. Once the IP address has been added to you can apply Port Forwarding and Access Control rules to this IP address.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

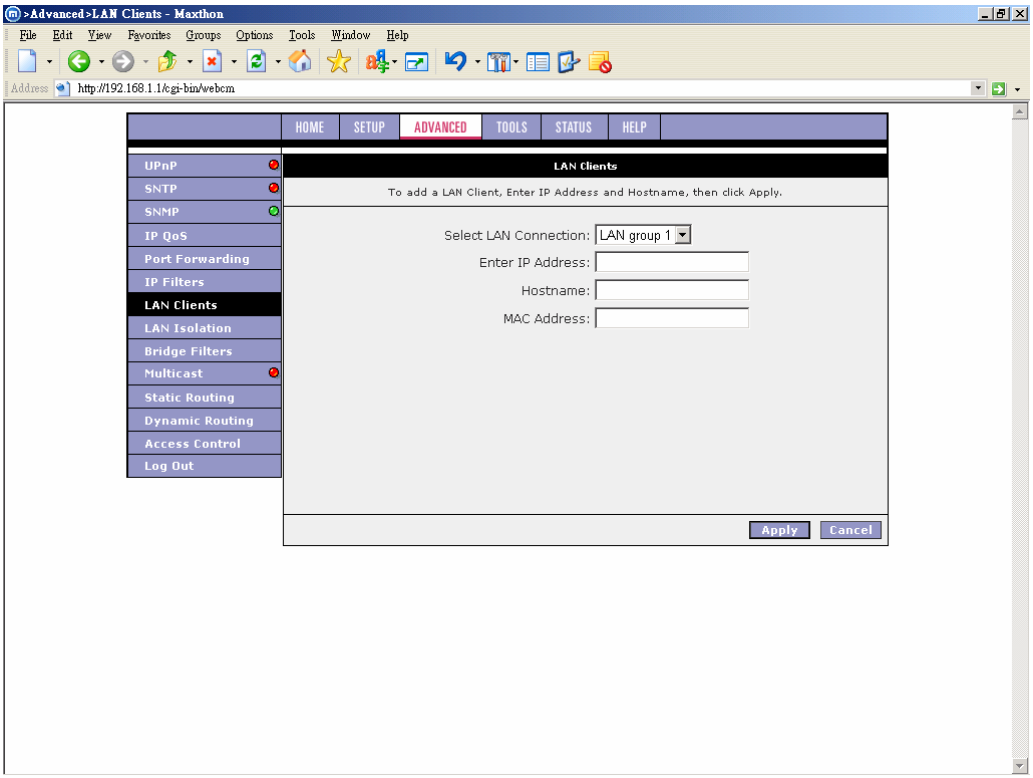


Figure 20 (LAN Client)

4.6.8 LAN Isolation

The LAN Isolation feature allows user to disable traffic between different LAN groups.

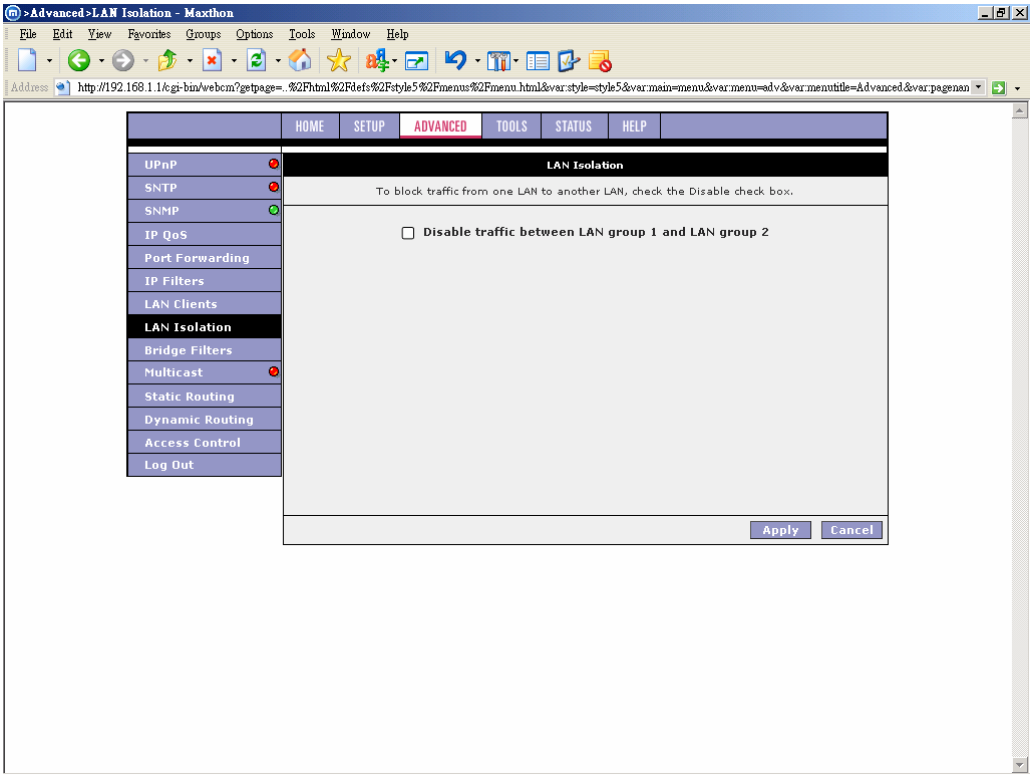


Figure 21 (LAN Isolation)

4.6.9 Bridge Filters

The bridge filtering mechanism provides a way for the users to define rules to allow/deny frames through the bridge based on source MAC address, destination MAC address and/or frame type. When bridge filtering is enabled, each frame is examined against the defined filter rules sequentially, and when a matched is determined, the appropriate filtering action (determined by the access type selected ... i.e. allow or deny) is performed. The user should note that the bridge filter will only examined frames from interfaces which are part of the bridge itself. Twenty filter rules are supported with bridge filtering. To enable Bridge Filters, from the Home screen, click Advanced and under Advanced, select Bridge Filters. Figure 22 illustrates a typical Bridge filter configuration.

The User Interface for Bridge Filter allows the user to add/edit/delete, as well as, enables the filter rules. To add rules, simply define the source MAC address, destination MAC address and frame type with desired filtering type (i.e. allow/deny), and press the "Add" button. The MAC address must be in a xx-xx-xx-xx-xx-xx format, with 00-00-00-00-00-00 as "don't care". Blanks can be used in the MAC address space, and would be considered also as "don't care".

To edit/modify an existing filter rule, select the desired rule created previously from "Add" in the "Edit" select box. The selected filter rule will appear on top section, as with the "Add" filter rule. Make the desired change to the MAC address, frame type and/or access type, and press "Apply".

To delete filter rule(s), select the filter rule entry to delete in the "Delete" selection box. Note that multiple deletions are possible. Once all the desired filter rule(s) is/are selected for deletion, press the "Apply" button. The "Select All" select box can also be used to delete the entire filter rule. It provides a quick method of selecting all filter rules for deletion.

The "Enable Bridge Filters" button allows the user to enable or disable bridge filtering. It can be set/unset during any add/edit/delete operation. It can also be set/unset independently by just pressing the "Apply" button.

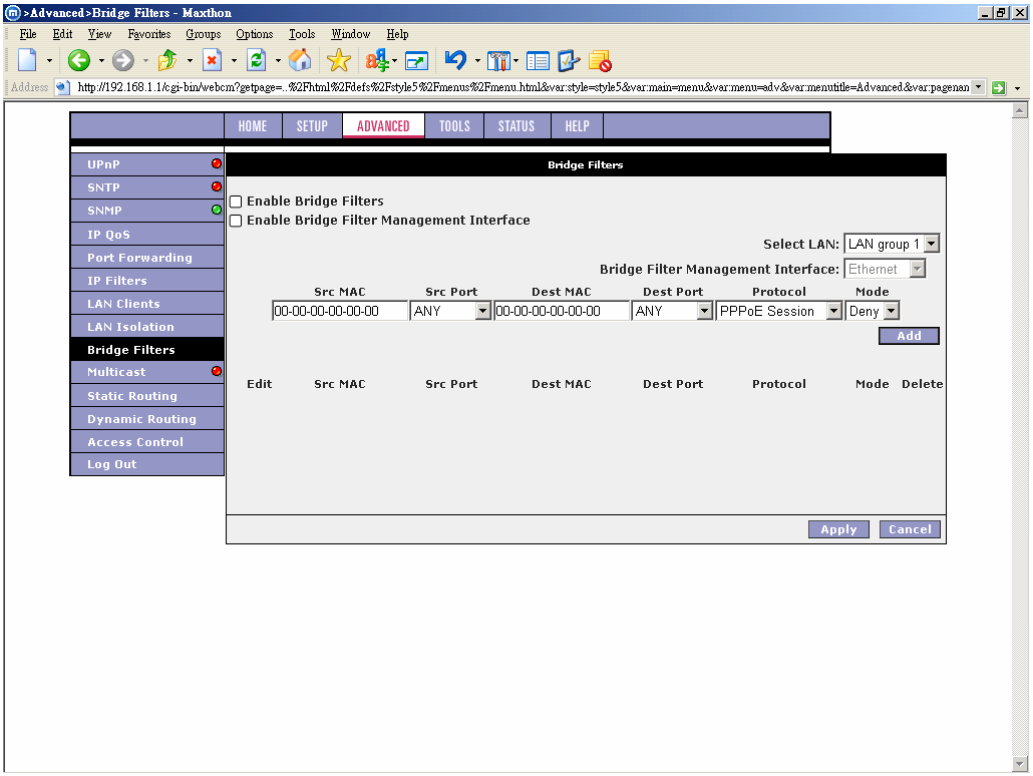


Figure 22 (Bridge Filters)

Note: The bridge filter table contains 3 hidden rules. These rules are entered automatically by the system to ensure the user does not "lock" them out of the system. The first rule allows any and all ARP frames through the system. The second rule allows all IPv4 frames with the destination MAC address of the bridge to go through. The third rule allows all IPv4 frames with the source MAC address of the bridge to go through.

Tip: On a windows based machine, to find a MAC address, at a DOS prompt type **ipconfig /all**.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.6.10 Multicast

Multicasting is a form of limited broadcast. UDP is used to send datagrams to all hosts that belong to what is called a "host group." A host group is a set of zero or more hosts identified by the same destination IP address. The following statements apply to host groups.

a. Anyone can join or leave a host group at will.
b. There are no restrictions on a host's location.
c. There are no restrictions on the number of members that may belong to a host group.
d. A host may belong to multiple host groups.
e. Non-group members may send UDP datagrams to the host group.

Multicasting is useful when data needs to be sent to more than one other device. For instance, if one device is responsible for acquiring data that many other devices need, then multicasting is a natural fit. Note that using multicasting as opposed to sending the same data to individual devices uses less network bandwidth.

To enable Multicasting, from the Home screen, click Advanced and under Advanced, select Muliticast. Figure 23 illustrates a typical Multicast configuration.

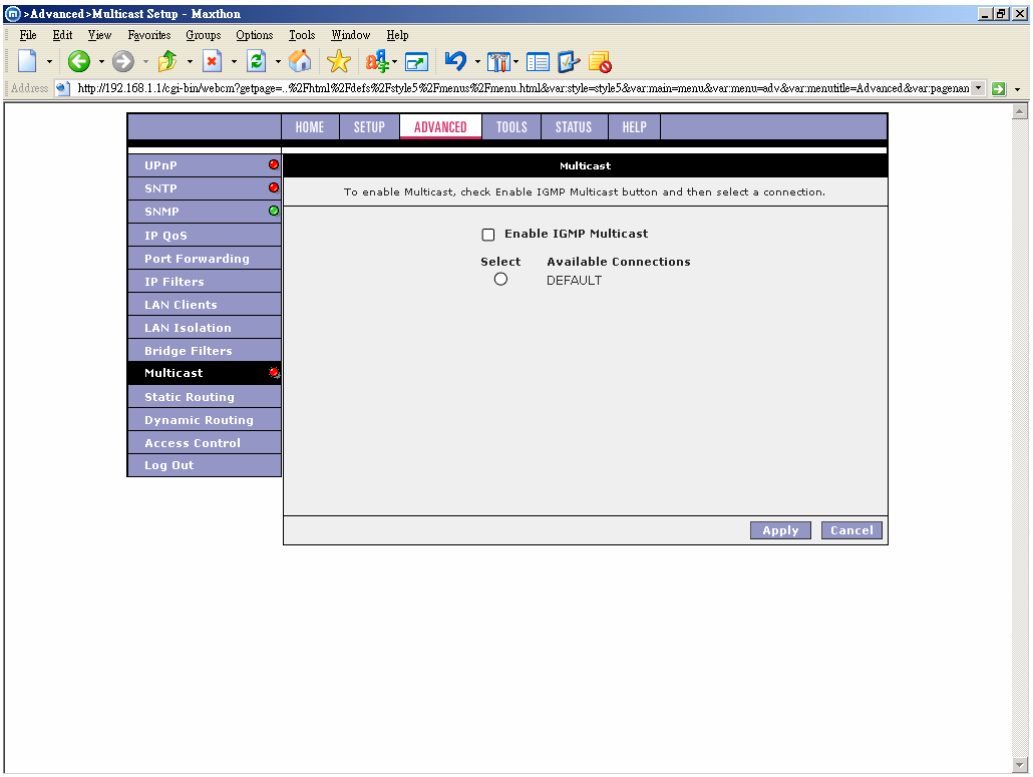


Figure 23 (Multicast)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.6.11 Static Routing

If the Gateway is connected to more than one network, you may need to set up a static route between them. A static route is a pre-defined pathway that network information must travel to reach a specific host or network. You can use static routing to allow different IP domain users to access the Internet through the Gateway.

The New Destination IP is the address of the remote LAN network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route here. For a standard Class C IP domain, the network address is the first three fields of the New Destination IP, while the last field should be 0. The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0. The Gateway IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host. The Hop Count determines the maximum number of steps between network nodes that data packets will travel. A node is any device on the network (such as a router or switch).

To enable Static Routing, from the Home screen, click Advanced and under Advanced, select Static Routing. Figure 24 illustrates a typical Static Route.

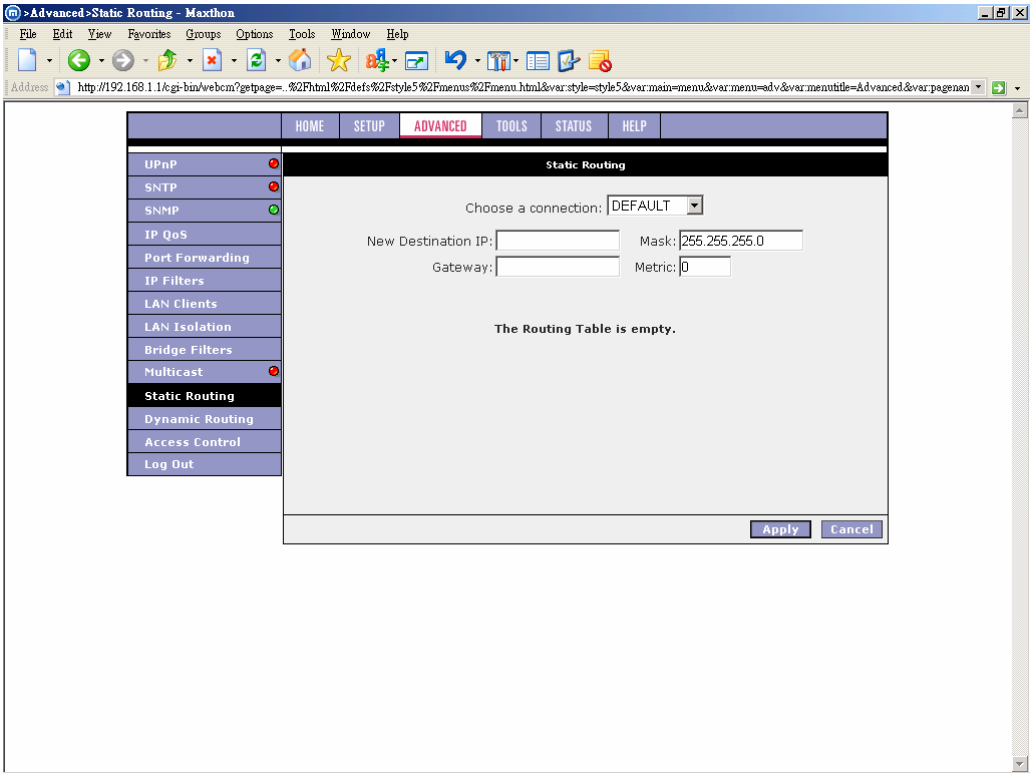


Figure 24 (Static Routing)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.6.12 Dynamic Routing

Dynamic Routing allows the Gateway to automatically adjust to physical changes in the network. The Gateway, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.

The Direction determines the direction that RIP routes will be updated. Selecting In means that the Gateway will only incorporate received RIP information. Selecting Out means that the Gateway will only send out RIP information. Selecting both means that the Gateway will incorporate received RIP information and send out updated RIP information.

The protocol is dependent upon the entire network. Most networks support Rip v1. If RIP v1 is selected, routing data will be sent in RIP v1 format. If Rip V2 is selected, routing data will be sent in RIP v2 format using subnet broadcasting. If Rip V1 Compatible is selected, routing data will be sent in RIP v2 format using multicasting.

To enable Dynamic Routing, from the Home screen, click Advanced and under Advanced, select Dynamic Routing. Figure 25 illustrates a typical Dynamic Route.

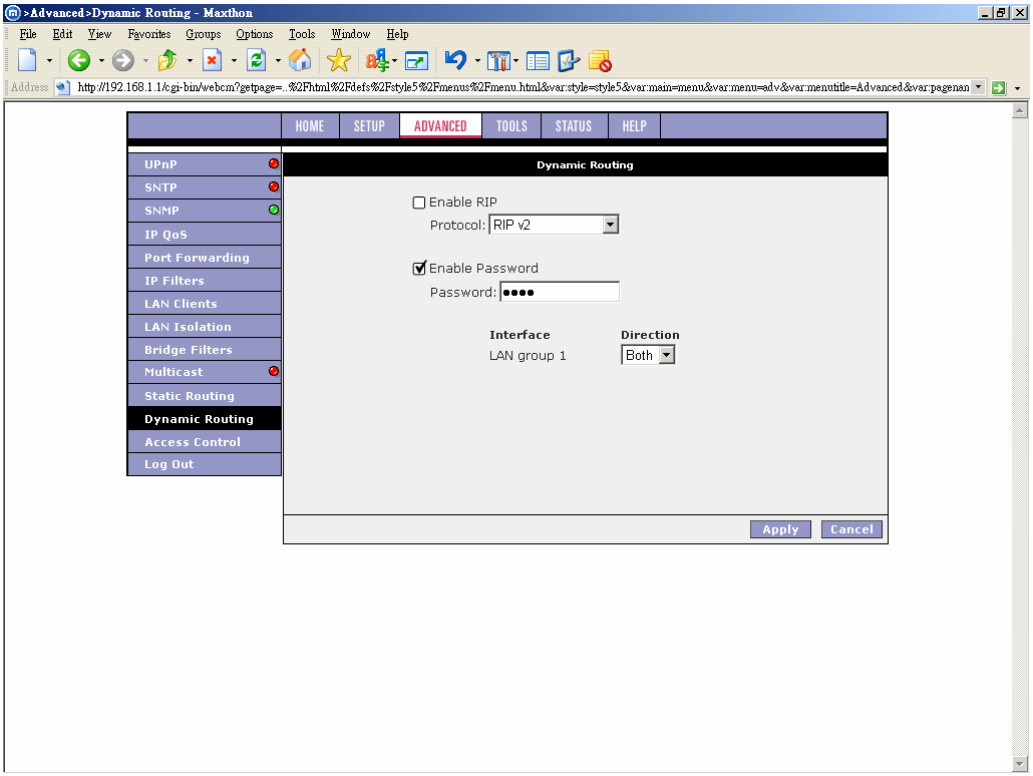


Figure 25 (Dynamic Routing)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.6.13 Access Control

Open the access from the Internet to the Gateway's management ports (web, telnet).

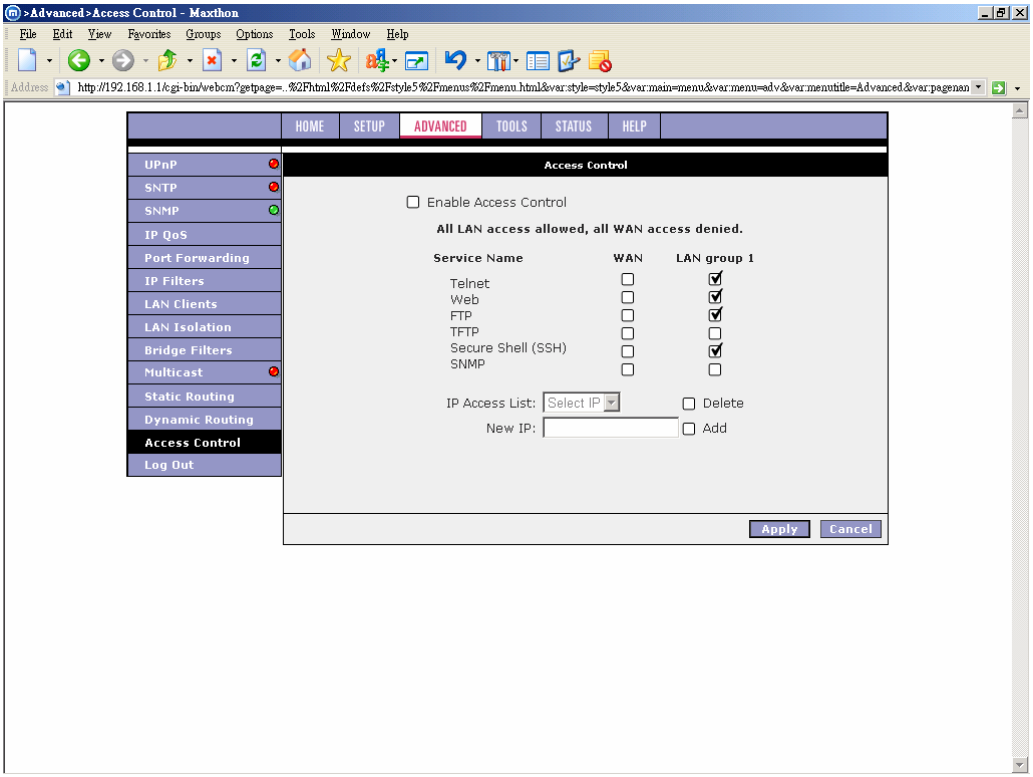


Figure 26(Access Control)

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.7 Tools

The gateway supports a host of tools which will allow you to customize and debug your gateway.

4.7.1 System Commands

To make the changes permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. The following commands are used to configure the gateway:

a. Save all: Press this button in order to permanently save the current configuration of the Gateway. If you do re-start the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
b. Restart: Use this button to re-start the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon re-starting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
c. Restore Defaults: Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

4.7.2 Remote Log

The remote log feature is used in conjunction with the PC tool (software provided with your gateway). For PPPoE and PPPoA connections, you can select debug if you want to log the connection information. This is helpful when trying to debug connection problems.

The remote log feature will forward all logged information to the remote PC. The type of information forwarded to the remote PC depends upon the Log level. Each log message is assigned a severity level, which indicates how seriously the triggering event affects Gateway functions. When you configure logging, you must specify a severity level for each facility; messages that belong to the facility and are rated at that level or higher are logged to the destination.

Table 1 defines the different severity levels.

To forward logging information, you need to click on **Tools** (at the top of the page) and select **Remote Log**.

Severity Level	Description
panic	System panic or other condition that causes the router to stop functioning.
alert	Conditions that require immediate correction, such as a corrupted system database.
critical	Critical conditions, such as hard drive errors.
error	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
warning	Conditions that warrant monitoring.
notice	Conditions that are not errors but might warrant special handling.
info	Events or non-error conditions of interest.
debug	Software debugging messages. Specify this level only when so directed by a technical support representative.

Table 1 (Severity Level)

4.7.3 User Management

You can change your gateway's username and password by going to the Home screen, under the tools menu, click User Management. From here you can change the login name and password. You can also change the idle timeout; you will need to log back onto the gateway once the timeout expires.

If you forget your password, you can press and hold the reset to factory defaults button for 10 seconds (or more). The gateway will reset to its factory default configuration and all custom configurations will be lost.

The apply button will temporarily save this connection. To make the change permanent you need to click on **Tools** (at the top of the page) and select **System Commands**. At the system commands page, click on **Save All**.

4.7.4 Update Gateway

You can remotely upgrade the gateway's firmware by going to the Home screen, under the tools title, click Update Gateway. This will bring up the screen shown in Figure 27. ATU-R140 ADSL Gateway will provide two different images; one image is the kernel (operating system) and the other image is the file system.

To upgrade the firmware, click browse, find the firmware file to download. Make sure this is the correct file. Click on upgrade firmware (as shown in Figure 27). Once the upgrade is complete the gateway will reboot. You will need to log back onto the gateway after the firmware upgrade is complete.

The firmware upgrade should take less that 5 minutes to complete. If it takes longer than 5 minutes, something has gone wrong.

Note: Do not remove power from the gateway during the firmware upgrade procedure.

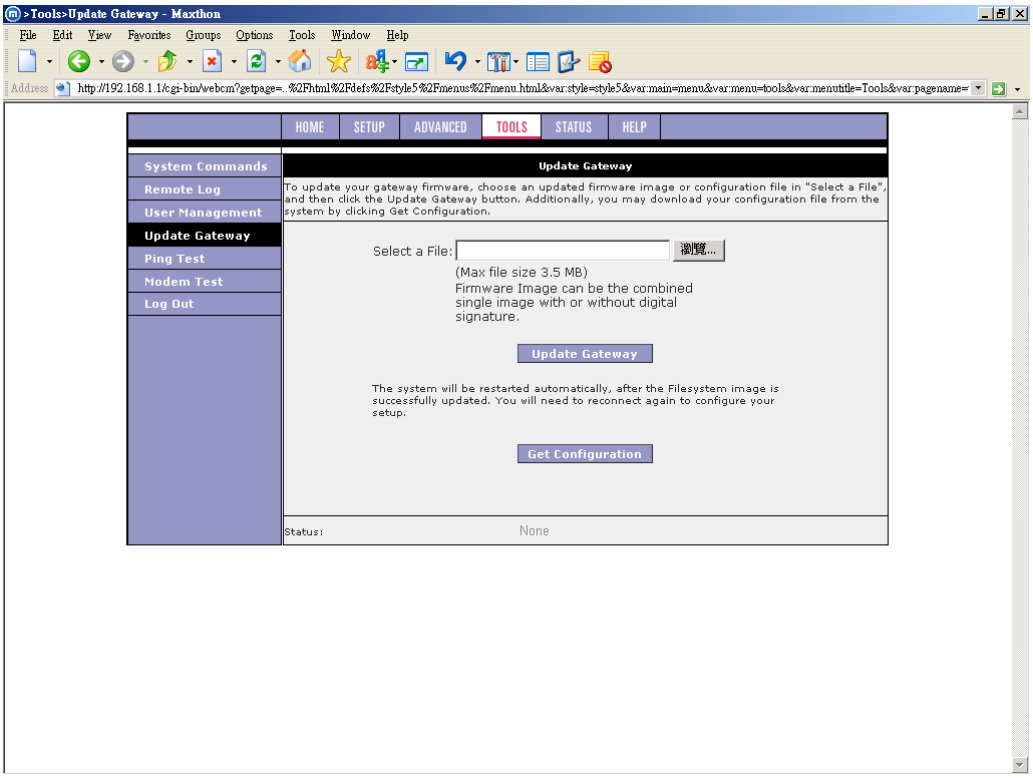


Figure 27 (Update Gateway)

4.7.5 Ping Test

Once you have your gateway configured, it is a good idea to make sure you can Ping the network. You can get to the Ping web page by going to the Home screen, under the Tools title, click Ping Test. Type the target address that you want to pin. If you have your PC connected to the gateway via the default DHCP configuration, you should be able to Ping the network address 192.168.1.1. If your ISP has provided their server address you can try to ping the address. If the pings for both the WAN and the LAN side complete, and you have the proper protocols configured, you should be able to surf the Internet.

By default when you select ping test, the gateway will ping itself 3 times. As shown in Figure 28, the gateway passed the Ping test; this basically means that the TCP/IP protocol is up and running. If this first Ping test does not pass, the TCP/IP protocol is not loaded for some reason; you should restart the modem.

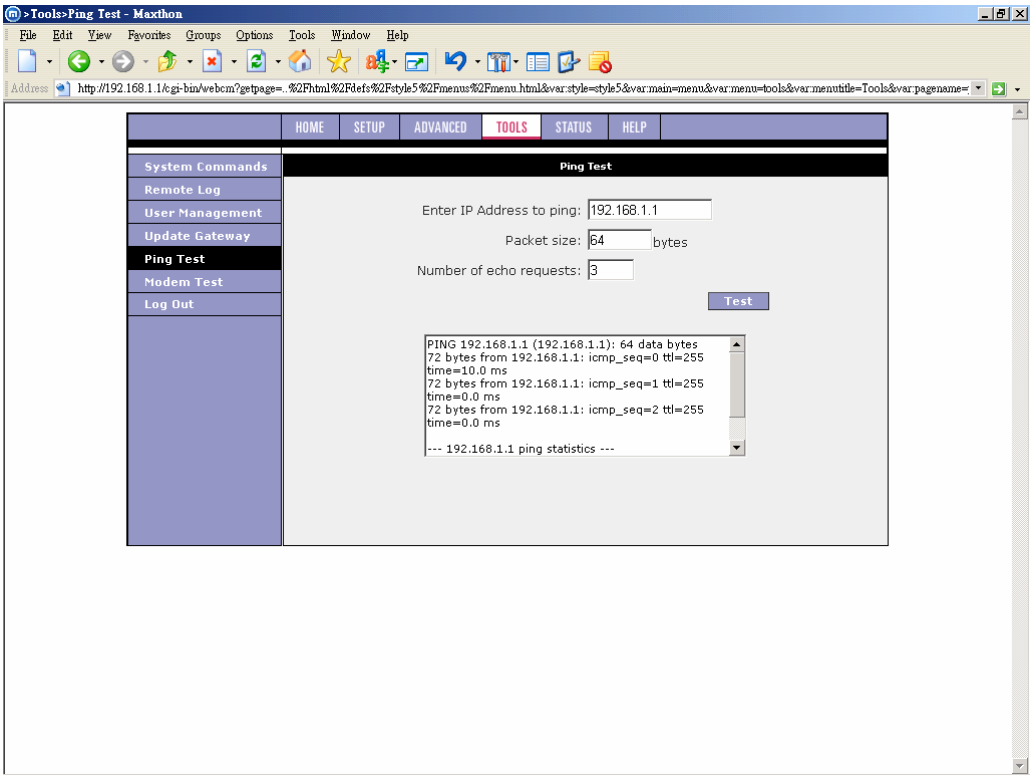


Figure 28 (Ping test)

4.7.6 Modem Test

The Modem Test is used to check whether your Modem is properly connected to the WAN Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button. Before running this test, make sure you have a valid DSL link; if the DSL link is not connected, this test will always fail.

Also the DSLAM must support this feature; not all DSLAMs have F4 and F5 support.

4.8 Status

The Status section allows you to view the Status/Statistics of different connections and interfaces.

4.8.1 Network Statistics

Select to view the Statistics of different interfaces - Ethernet/USB/DSL.

4.8.2 Connection Status

Select to view the Status of different connections.

4.8.3 DHCP Clients

Select to view the list of DHCP clients.

4.8.4 Modem Status

Select to view the Status and Statistics of your broadband (DSL) connection.

4.8.5 Product Information

You can display the gateway's driver and run-time information by going to the Home screen, under the Status title, click Product Information. Figure 29 illustrates the typical product information, which is provided.

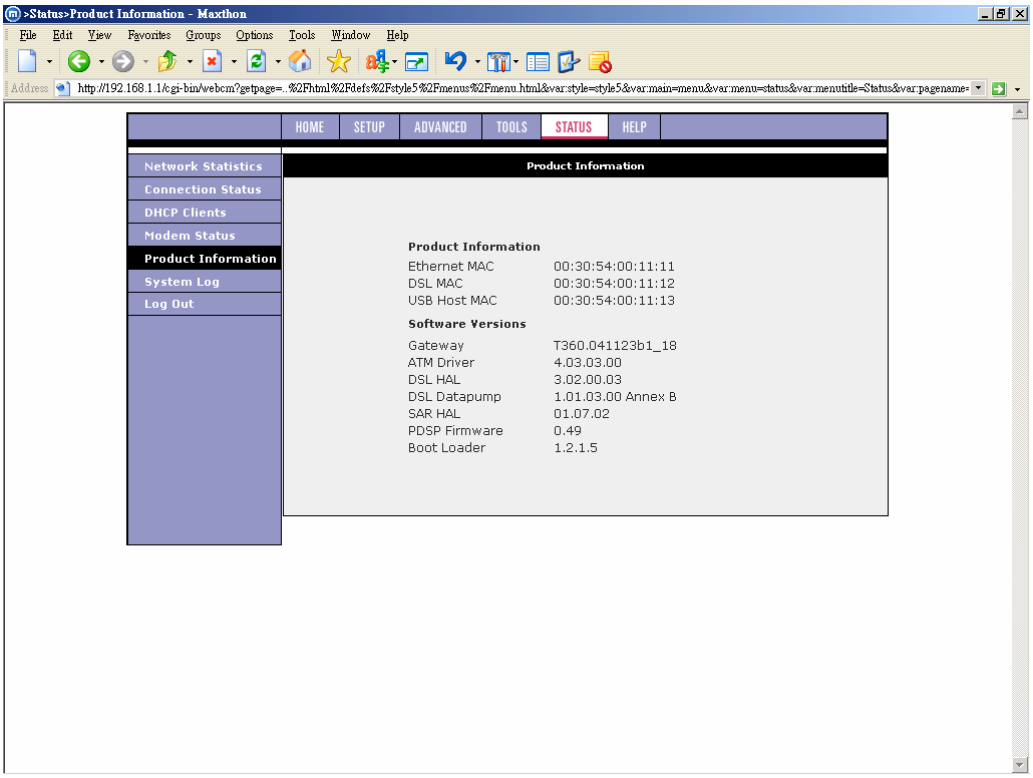


Figure 29 (Product Information)

4.8.6 System Log

You can display the Gateway's log by going to the Home screen, under the Status title, click System log. From here you can view all logged information. Depending upon the severity level, this logged info will generate log reports to a remote host (if remote logging is enabled).

5. Appendix A: Troubleshooting

Below is a list of commonly asked questions. Before calling technical support, please look through these issues to see if they help solve your problem.

5.1 The gateway is not functional.

1. Check to see that the power LED is green and than the network cables are installed correctly. Refer to the quick start guide for more details.
2. Check to see that the LAN and WAN LEDs are green.
3. Check to see that the DSL LED is green
4. Make sure you are not connecting the USB and the Ethernet port at the same time. You must only use 1 interface at a time.
5. Check the settings on your PC. Again, refer to the quick start guide for more details
6. Check the gateway's settings.
7. From your PC, can you PING the gateway? Assuming that the gateway has DHCP enabled and your PC is on the same subnet as the gateway, you should be able to PING the gateway.
8. Can you PING the WAN? Your ISP should have provided the IP address of their server. If you can ping the gateway and your protocols are configured correctly, you should be able to ping the ISPs network. If you cannot PING the ISPs network, make sure your using the correct protocols with the correct VPI/VCI values.
9. Make sure NAT is enabled for your connection. If NAT is disabled you the gateway will not route frames correctly.

5.2 I can't connect to the gateway.

1. Check to see that the power LED is green and that the network cables are installed correctly; see the quick start guide for more details.
2. Make sure you are not connecting the USB and the Ethernet port at the same time. You must only use 1 interface at a time.
3. Make sure that your PC and the gateway is on the same network segment. The gateway's default IP address is 192.168.1.1. If you are running a Windows based PC, you can open a DOS window and type IPCONFIG; make sure that the network adapter that is connected to the gateway is within the same 192.168.1.x subnet.
4. Also, your PC's Subnet Mask should match the gateways subnet mask. The gateway has a default subnet mask of 255.255.255.0.
5. If this still does not work, press the reset button for 10 seconds. This will place the gateway into its factory default state. Go through the above procedures again.
6. Make sure NAT is enabled for your connection. If NAT is disabled you the gateway will not route frames correctly.

5.3 The LEDs blink in a sequential pattern.

This typically means that either the kernel or flash file system is corrupted. The only way to recover from this type of failure is via the PC tool. You need to install the PC tool that was provided with ATU-R140 ADSL Gateway and perform the following steps:

1. In windows disable all network adapters except the one, which is connected to the gateway.
2. Disable zone alarm or any IP blocking software that is running of the PC.
3. Run the PC tool application. At the IP address prompt, type 192.168.1.1 and retrieve/assign IP address. The PC application should come back with information about the gateway. You then need to load the kernel image, flash file system, and config.xml file to the flash.
4. Once all three codes have been loaded into the gateway, the gateway will automatically reboot. As long as there is no problem with the Flash

memory, the gateway should be functional and the LEDs should light correctly.

5.4 The DSL Link LED continues to blink but does not go solid.

1. This means that the DSL line is trying to train but for some reason it cannot establish a valid connection. The main cause of this is that you are too far away from the central office. Contact your DSL service provider for further assistance.

5.5 The DSL Link LED is always off.

1. Make sure you have DSL service. You should get some kind of information from your ISP which states that DSL service is installed. You can usually tell if the service is installed by listening to the phone line; you will hear some high-pitched noise. If you do not hear high-pitched noise, contact your ISP.
2. Verify that the phone line is connected directly to the wall and to the line input on the gateway. If the phone line is connected to the phone side of the gateway or you have a splitter installed on the phone line, the DSL light will not come on.

6. Gateway terms

What is a firewall?
A firewall is protection between the Internet and your local network. It acts similarly to the firewall in your car, protecting the interior of the car from the engine. Your car's firewall has very small opening that allow desired connections from the engine into the cabin (gas pedal connection, etc), but if something happens to your engine, you are protected.
The firewall in the Gateway is very similar. Only the desired connections that you allow are passed through the firewall. These connections are normally originating from the local network; such as web browsing, checking your email, downloading a file, and playing a game. However, in some cases, you can allow incoming connections so that you can run programs like a web server.

What is NAT?
NAT stands for Network Address Translation. Another name for it is Connection Sharing. What does this mean? Your ISP provides you with a single network address for you to access the Internet through. However, you may have several machines on your local network that want to access the Internet at the same time. The Gateway provides NAT functionality that converts your local network addresses to the single network address provided by your ISP. It keeps track of all these connections and makes sure that the correct information gets to the correct local machine.
Occasionally, there are certain programs that don't work well through NAT. Some games, and some specialty applications have a bit of trouble. The Gateway contains special functionality to handle the vast majority of these troublesome programs and games. NAT does cause problems when you want to run a SERVER though. When running a server, please see the DMZ section below.

What is a DMZ?
DMZ really stands for Demilitarized Zone. It is a way of separating out part of your local network so that is more open to the Internet. Suppose that you want to run a web-server, or a game server. Normal servers like these are blocked from working by the NAT functionality. The solution is to "isolate" the single local computer into a DMZ. This makes the single computer look like it is directly on the Internet, and others can access this machine.
Your machine isn't really directly connected to the Internet, and it really has an internal local network address. When you provide the servers network address to others, you must provide the address of the Gateway. The Gateway "fakes" the connection to your machine.
You should use the DMZ when you want to run a server that others will access from the Internet. Internal programs and servers (like print servers, etc) should NOT be connected to the DMZ

What is a Gateway?
The Internet is so large that a single network cannot handle all of the traffic and still deliver a reasonable level of service. To overcome this limitation, the network is broken down into smaller segments or subnets that can deliver good performance for the stations attached to that segment. This segmentation solves the problem of supporting a large number of stations, but introduces the problem of getting traffic from one subnet to another.

To accomplish this, devices called routers or gateways are placed between segments. If a machine wishes to contact another device on the same segment, it transmits to that station directly using a simple discovery technique. If the target station does not exist on the same segment as the source station, then the source actually has no idea how to get to the target.

One of the configuration parameters transmitted to each network device is its default gateway. This address is configured by the network administrators and it informs each personal computer or other network device where to send data if the target station does not reside on the same subnet as the source. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside of this area, it is usually because of an incorrectly configured default gateway.

Transmission Series

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Technology Center
(Neihu Technology Park)
8F, No.60, Zhouzi Street
Neihu, Taipei, Taiwan
Phone:(886) 2.2659.1021 Fax:(886) 2.2799.1355
E-mail: info@ctcu.com
http://www.ctcu.com