DSL-2140/2140W Series
ADSL2PLUS 4-port Router

User Guide

Revision 1.0

Jan/2008

Contents

Chapter 1- Getting to Know the DSL-2140/2140W

Your DSL-2140/2140W integrates high-speed 10/100Mbps auto-negotiating LAN interface(s) and a high-speed ADSL port. The DSL-2140/2140W is perfect for making LAN-to-LAN connections to remote networks and for high-speed Internet browsing. The DSL-2140/2140W provides lightning-fast Internet access to multiple users by combining Direct Subscriber Line (DSL) and Network Address Translation (NAT).

The Web-based Graphical User Interface (GUI) allows easy management and is not dependent on any single operating system to use.

1.1 Features of the DSL-2140/2140W

- **High Speed Internet Access**

The DSL-2140/2140W ADSL 2/2+ router support downstream transmission rates of up to 24Mbps and upstream transmission rates of 1Mbps.

- **PPPoE Support (RFC2516)**

Point-to-Point Protocol over Ethernet (PPPoE) emulates a dial-up connection. It allows your Internet Service Provider (ISP) to use its existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the DSL-2140/2140W is transparent to the computers on the LAN. Computers see only Ethernet and are not aware of PPPoE; you don't have to manage PPPoE clients on individual computers.

- **Network Address Translation (NAT)**

Network Address Translation (NAT) allows the conversion of an Internet protocol (IP) address used within one network, such as a private IP address used in a LAN, to a different IP address known within another network, such as a public IP address used on the Internet.

- **Universal Plug and Play (UPnP)**

Using the standard TCP/IP protocol, the DSL-2140/2140W and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

- **10/100M Auto-negotiation Ethernet/Fast Ethernet Interface**

Auto-negotiation allows the DSL-2140/2140W to detect incoming transmissions' speeds and make necessary adjustments without manual intervention. It also allows data transfer rates of either 10 Mbps or 100 Mbps, in either half-duplex or full-duplex mode, depending on your Ethernet network.

- **Dynamic DNS Support**

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessed from other locations on the Internet.

You must register for this service with a Dynamic DNS client.

- **Multiple PVC (Permanent Virtual Circuit) Support**

  Your DSL-2140/2140W supports up to 8 PVCs.

- **ADSL Standards**

  - Compliant to ITU-T G.992.1 (G.dmt), G.992.3 (ADSL2), G.992.4, and G.992.5 (ADSL2+) Annex A, B, I, J, L, and M
  - Supports Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.994.1 and G.996.1 (for ISDN only); G.991.1; G.lite (G992.2))
  - Supports OAM F4/F5 loop-back, AIS and RDI OAM cells
  - ATM Forum UNI 3.1/4.0 PVC
  - Supports up to 8 PVCs (UBR, CBR, VBR)
  - Multiple Protocols over AAL5 (RFC 1483)
  - PPP over AAL5 (RFC 2364)
  - PPP over Ethernet (RFC 2516)

- **DHCP Support**

Dynamic Host Configuration Protocol (DHCP) allows individual clients (computers) to get TCP/IP configuration information at start-up from a DHCP server. The DSL-2140/2140W has its built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The DSL-2140/2140W can also act as a substitute DHCP server (DHCP Relay), relaying IP address assignment from the actual DHCP server to the clients.

- **IP Alias**

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The DSL-2140/2140W can support up to 3 logical LAN interfaces through its physical Ethernet interface with the DSL-2140/2140W acting as the gateway for each network.

- **IP Policy Routing (IPPR)**

Normally, routing is based only on the destination address; the router forwards the packet along the shortest path. IP Policy Routing (IPPR) is a method to override this routing behavior and change the forwarding path based on policies defined by the network administrator.

- **Protocol Support**

  - Point-to-Point Protocol (PPP) link layer protocol
    - PPP over PAP (RFC 1334)
    - PPP over CHAP (RFC 1994)
  - RIP I/RIP II
  - IGMP Proxy
  - ICMP support
  - MIB II support (RFC 1213)

- PPPoE feature
  - PPPoE idle time out
  - PPPoE dial on demand

➢ **Networking Compatibility**

The DSL-2140/2140W is compatible with major ADSL Digital Subscriber Line Access Multiplexer (DSLAM) providers.

➢ **Multiplexing**

The DSL-2140/2140W supports VC-based and LLC-based multiplexing.

➢ **Encapsulation**

The DSL-2140/2140W supports PPP over ATM Adaptation Layer 5 (PPPoA, RFC 2364), RFC 1483 encapsulation over ATM, MAC encapsulated routing (ENET Encapsulation) as well as PPP over Ethernet (RFC 2516).

➢ **Network Management**

- Embedded Web Configurator
- Command Line Interpreter (CLI)
- Simple Network Management Protocol (SNMP) manageable
- DHCP Server/Client
- Built-in Diagnostic Tools
- Syslog
- TFTP/FTP server, firmware upgrade and configuration backup/support supported

➢ **Diagnostics Capabilities**

The DSL-2140/2140W can run self-diagnostic tests. These tests check the status of the following:

- LAN port
- ADSL circuitry
- RAM
- FLASH memory

➢ **Filters**

The DSL-2140/2140W's packet filtering abilities gives added network security and management.

➢ **Ease of Installation**

The DSL-2140/2140W is designed for fast, simple installation.

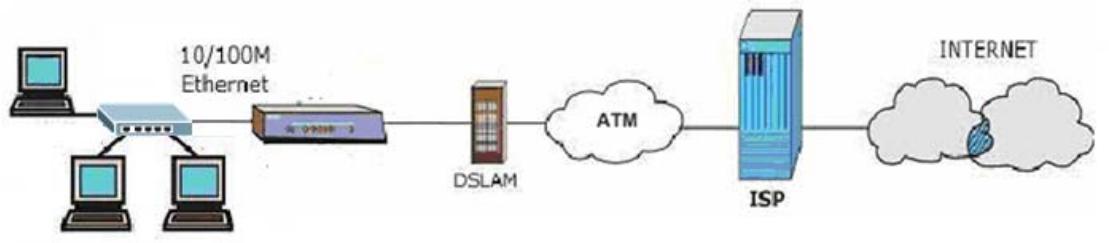
1.2 Applications for the DSL-2140/2140W

Here are some uses that the DSL-2140/2140W is suitable for.

1.2.1 Accessing the Internet

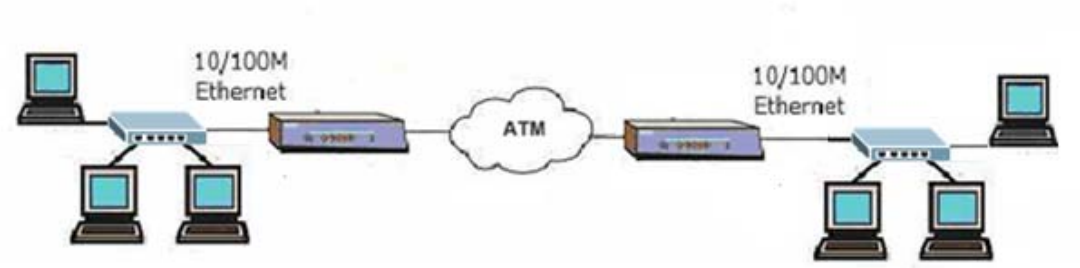
The DSL-2140/2140W is an ideal high-speed Internet access solution. It supports the TCP/IP protocol, which the Internet uses exclusively. The DSL-2140/2140W is compatible with all major ADSL DSLAM providers. A DSLAM is a group of ADSL line cards with data multiplexed into a network interface/connection, such as T1, OC3, DS3, ATM or Frame Relay. It is similar to an ADSL modem rack.

An example Internet access application is shown below.



1.2.2 Making LAN to LAN Connections

The DSL-2140/2140W can be used to connect two physically distant networks through the ADSL line. An example LAN-to-LAN connection is shown below.



Chapter 2 - Introducing the Web Configurator

Your DSL-2140/2140W can be managed from anywhere with the embedded Web configurator using a Web browser, such as Microsoft Internet Explorer or Netscape Navigator. Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled should be used. A screen resolution of 1024 by 768 pixels is recommended.

2.1 Accessing the DSL-2140/2140W Web Configurator

Step 1. Ensure that the DSL-2140/2140W is properly connected.

Step 2. Prepare your computer/computer network to connect to the DSL-2140/2140W.

Step 3. Launch your Web browser.

Step 4. Enter "192.168.1.1" as the URL.

Step 5. The Connect to 192.168.1.1 window will open. Enter your User name (“admin” is the default) and Password (“1234” is the default), and then click on OK.

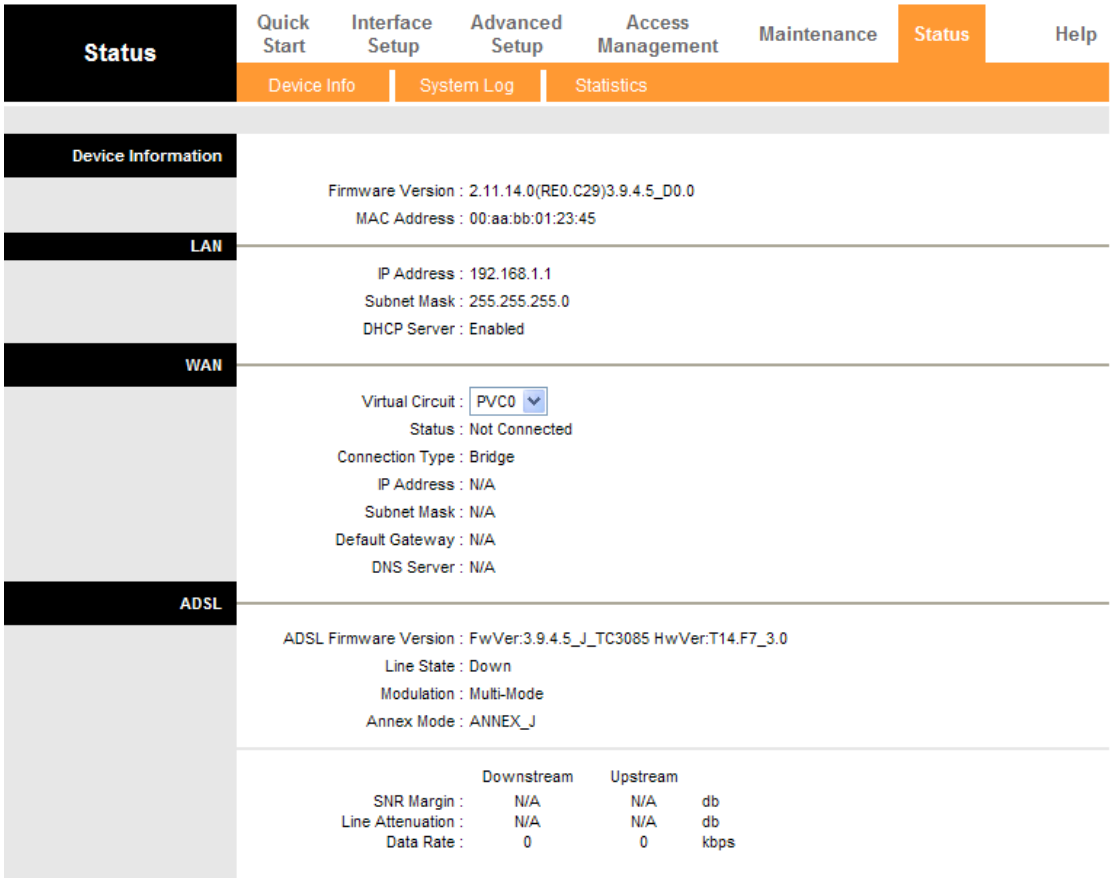
Step 6. You should now see the Web configurator.

2.2 Navigating the DSL-2140/2140W Web Configurator

Steps to navigate the Web Configurator from the Site Map are summarized below.

- Click on Quick Start to begin a wizard that helps to configure your DSL-2140/2140W.
- Click on Interface Setup to configure Internet and LAN DSL-2140/2140W functions.

- Click on Advanced Setup to configure advanced DSL-2140/2140W features.
- Click on Access Management to manage Internet access options.
- Click on Maintenance to set a new password, to set the time zone, to upgrade or reload firmware and to run diagnostic tests on the DSL-2140/2140W.
- Click on Status to see DSL-2140/2140W device information, system logs and performance statistics.
- Click on Help to see available help topics.



2.3 Resetting the DSL-2140/2140W

If you should forget your password, or if you can't gain access to the DSL-2140/2140W, you will have to reload the factory-default configuration file or use the RESET button on the back of the DSL-2140/2140W device to regain access. Uploading the default configuration file replaces the current configuration file. You will lose all your previously-saved configurations. The password will also be reset to "1234".

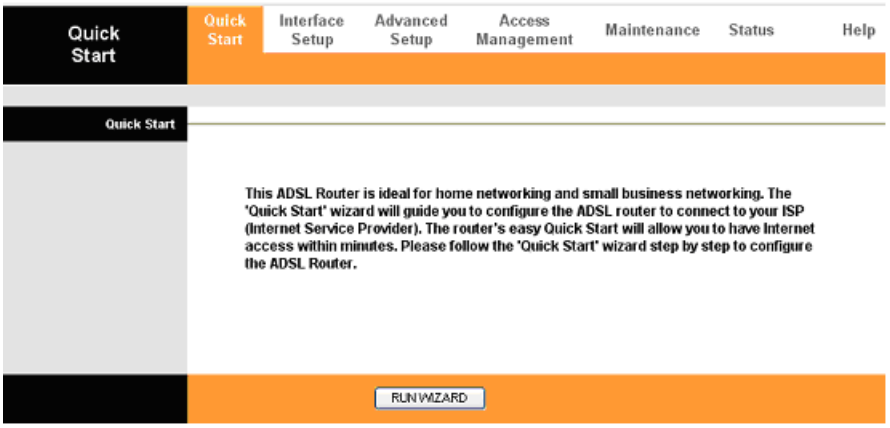
2.3.1 Using the Reset Button

Step 1. Make sure the SYS LED is on and not blinking.

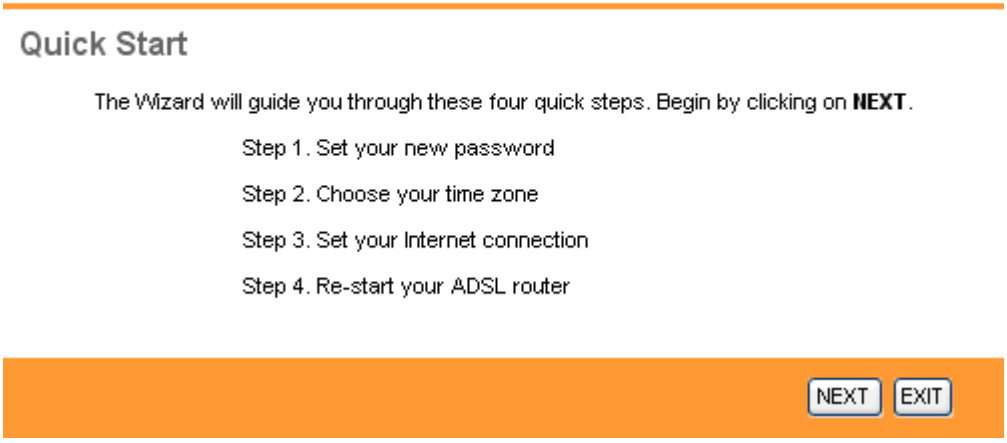
Step 2. Press and hold the RESET button for five seconds, and then release it. When the SYS LED begins to blink, the default configurations have been restored and the DSL-2140/2140W will then restart.

Chapter 3 - The Quick Start Wizard

Use the Quick Start wizard to configure your system settings. Your ISP may have configured some of the fields in the wizard for you.



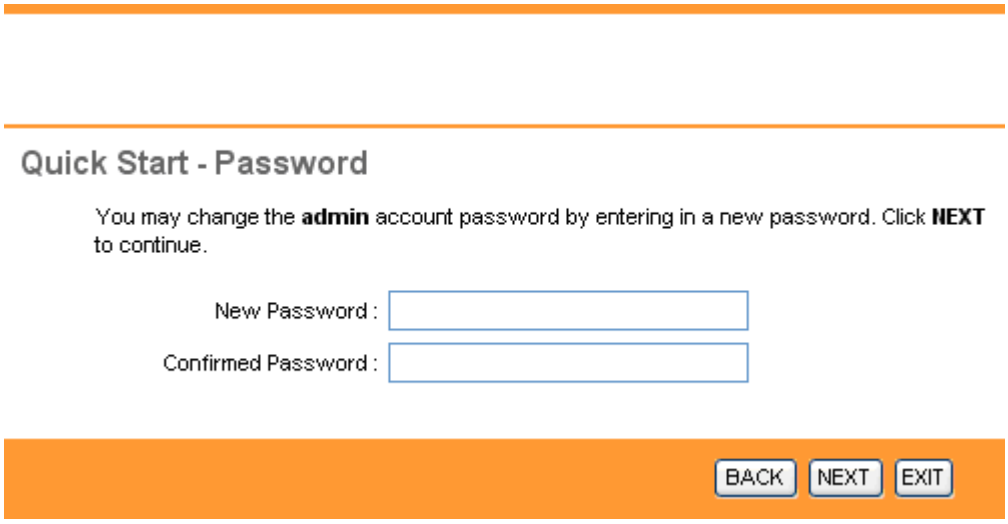
Click on the RUN WIZARD button to start the Quick Start wizard. The Quick Start wizard will open a new browser window with the following screen.



Click on NEXT to continue, or on EXIT to exit the wizard without saving.

3.1 Setting a New Password

This screen helps you set a new password, replacing the default password.



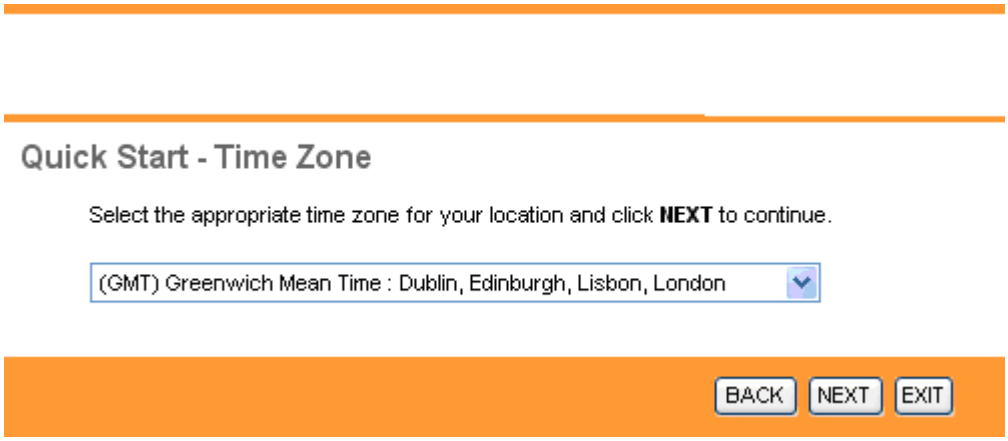
The following table describes the labels in this screen.

LABEL	DESCRIPTION
New Password	Enter the password you wish to use here
Confirmed Password	Enter the password again to confirm

Click on BACK to return to the previous screen, on NEXT to continue, or on EXIT to exit the wizard without saving.

3.2 Choosing the Time Zone

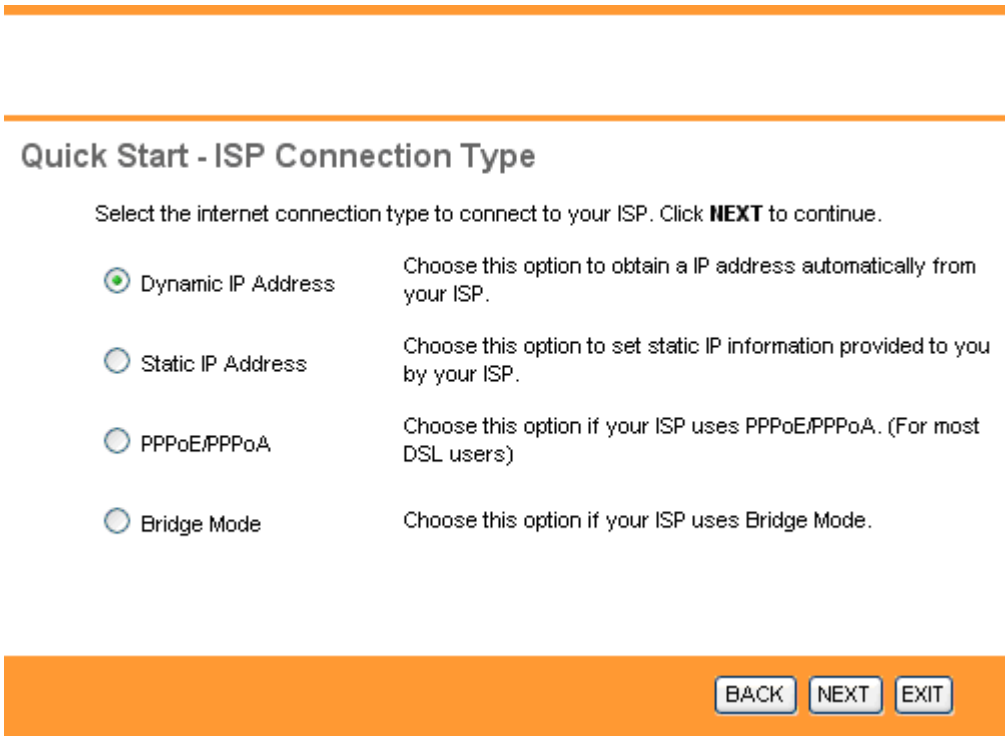
This screen helps you set the time zone for your DSL-2140/2140W.



Select the appropriate time zone for your location from the dropdown list. Click on BACK to return to the previous screen, on NEXT to continue, or on EXIT to exit the wizard without saving.

3.3 Setting the ISP Connection Type

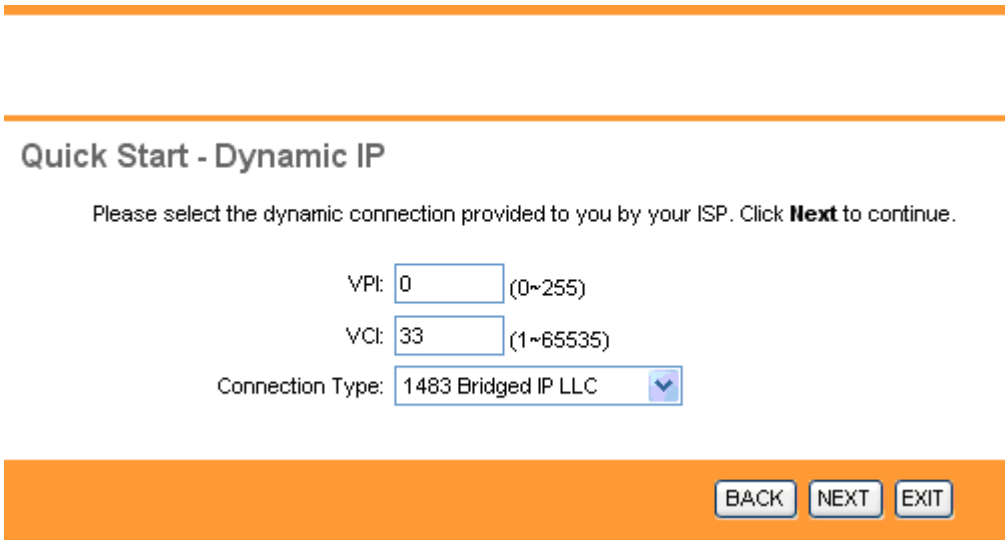
This screen helps you select, then configure, your ISP connection type.



Select the Internet connection type you use to connect to your ISP. Click on BACK to return to the previous screen, on NEXT to continue, or on EXIT to exit the wizard. The following screen will vary depending on which connection type you chose. Each screen is explained below.

3.3.1 Configuring Dynamic IP Address

A dynamic IP address connection requests a new IP address from your ISP each time you connect to it.



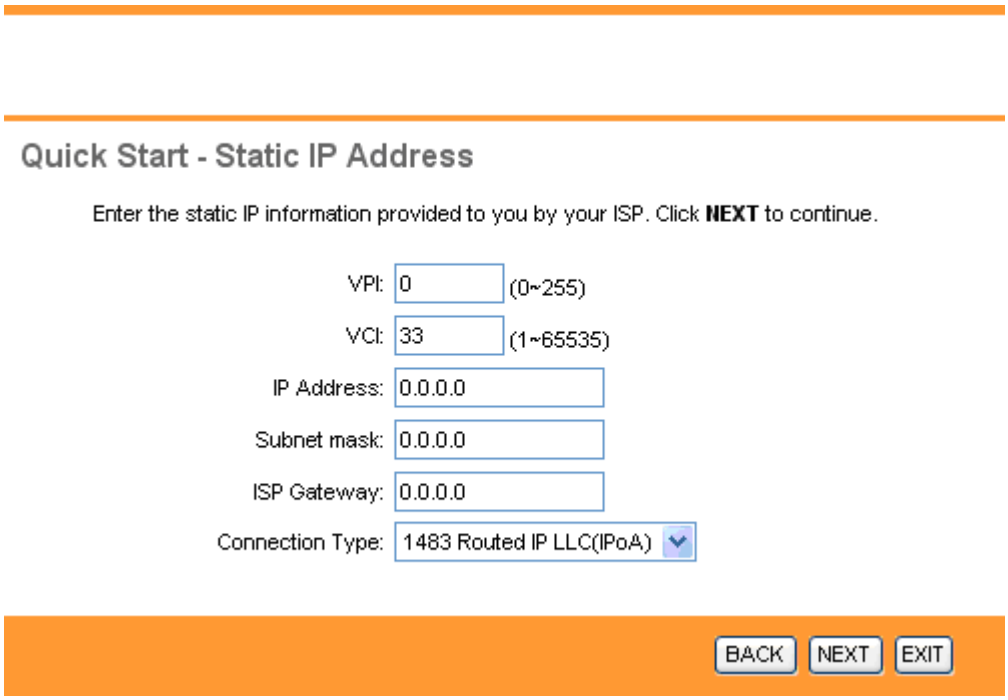
The following table describes the labels in this screen.

LABEL	DESCRIPTION
VPI	Enter the VPI here. VPI can range from 0 to 255.
VCI	Enter the VCI here. VCI can range from 1 to 65535.
Connection Type	Select your connection type from the dropdown list.

Your ISP should provide the above information. Click on BACK to return to the previous screen, on NEXT to continue, or on EXIT to exit the wizard without saving.

3.3.2 Configuring Static IP Address

A static IP address connection uses the same IP each time you connect to your ISP.



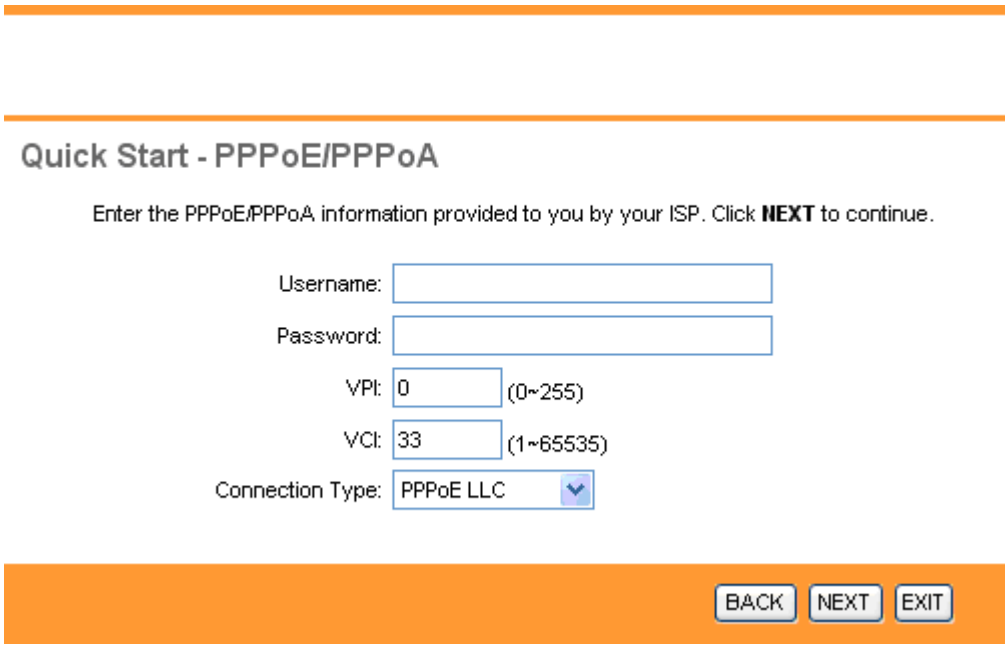
The following table describes the labels in this screen.

LABEL	DESCRIPTION
VPI	Enter the VPI here. VPI can range from 0 to 255.
VCI	Enter the VCI here. VCI can range from 1 to 65535.
IP Address	Enter the IP address here.
Subnet Mask	Enter the Subnet Mask here.
ISP Gateway	Enter the ISP Gateway here.
Connection Type	Select your connection type from the dropdown list.

Your ISP should provide this information. Click on BACK to return to the previous screen, on NEXT to continue, or on EXIT to exit the wizard without saving.

3.3.3 Configuring PPPoE

PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The DSL-2140/2140W bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM Permanent Virtual Circuit (PVC) that connects to the ADSL Access Concentrator, where the PPP session terminates. A single PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the appendix.



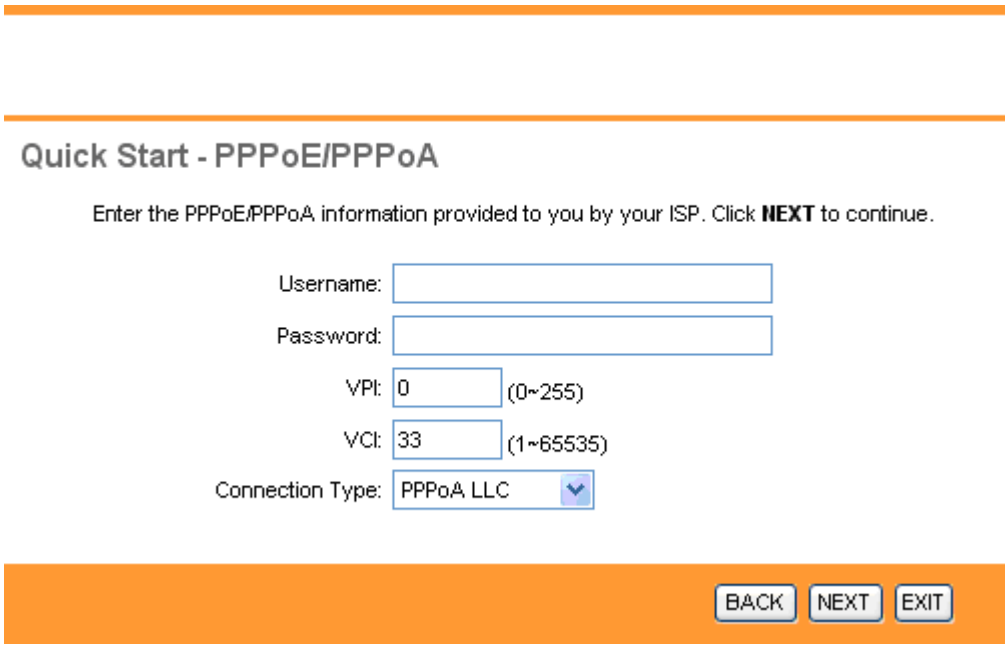
The following table describes the labels in this screen.

LABEL	DESCRIPTION
Username	Enter your username here.
Password	Enter your password here.
VPI	Enter the VPI here. VPI can range from 0 to 255.
VCI	Enter the VCI here. VCI can range from 1 to 65535.
Connection Type	Select your connection type from the dropdown list.

Your ISP should provide the above information. Note that you must enter the user name exactly as your ISP assigned it. If the assigned name is in the form of user@domain where domain identifies a service name, enter it exactly as given. Click on BACK to return to the previous screen, on NEXT to continue, or on EXIT to exit the wizard without saving.

3.3.4 Configuring PPPoA

Point-to-Point Protocol over ATM Adaptation Layer 5 (AAL5) (PPPoA) provides access control and billing functionality in a manner similar to dial-up services using PPP. The DSL-2100 encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC to the ISP's DSLAM. Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.



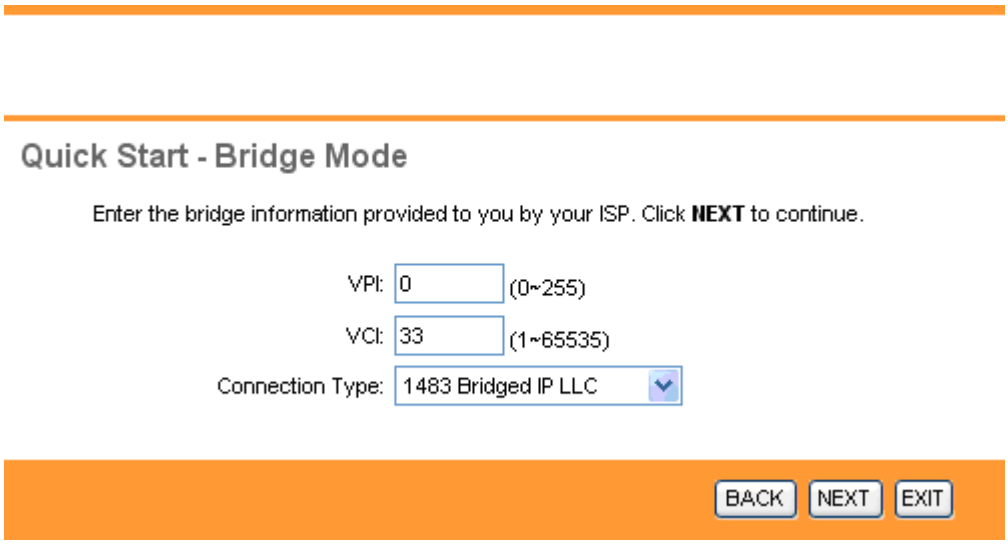
The following table describes the labels in this screen.

LABEL	DESCRIPTION
Username	Enter your username here.
Password	Enter your password here.
VPI	Enter the VPI here. VPI can range from 0 to 255.
VCI	Enter the VCI here. VCI can range from 1 to 65535.
Connection Type	Select your connection type from the dropdown list.

Your ISP should provide the above information. Note that you must enter the user name exactly as your ISP assigned it. If the assigned name is in the form of user@domain where domain identifies a service name, enter it exactly as given. Click on BACK to return to the previous screen, on NEXT to continue, or on EXIT to exit the wizard without saving.

3.3.5 Configuring Bridge Mode

RFC 1483 explains two methods for Multiprotocol Encapsulation over AAL5. The first method allows multiplexing of multiple protocols over just one ATM virtual circuit (LLC-based multiplexing). The second method assumes that each individual protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more information.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
VPI	Enter the VPI here. VPI can range from 0 to 255.
VCI	Enter the VCI here. VCI can range from 32 to 65535.
Connection Type	Select your connection type from the dropdown list.

Your ISP should provide the above information. Click on BACK to return to the previous screen, on NEXT to continue, or on EXIT to exit the wizard without saving.

3.3.6 Multiplexing

Two conventions identify what protocols a virtual circuit (VC) is carrying. Be sure to use the multiplexing method your ISP requires.

3.3.6.1 VC-based Multiplexing

In VC-based multiplexing, by prior mutual agreement, each protocol is assigned to a specific virtual circuit. For example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

3.3.6.2 LLC-based Multiplexing

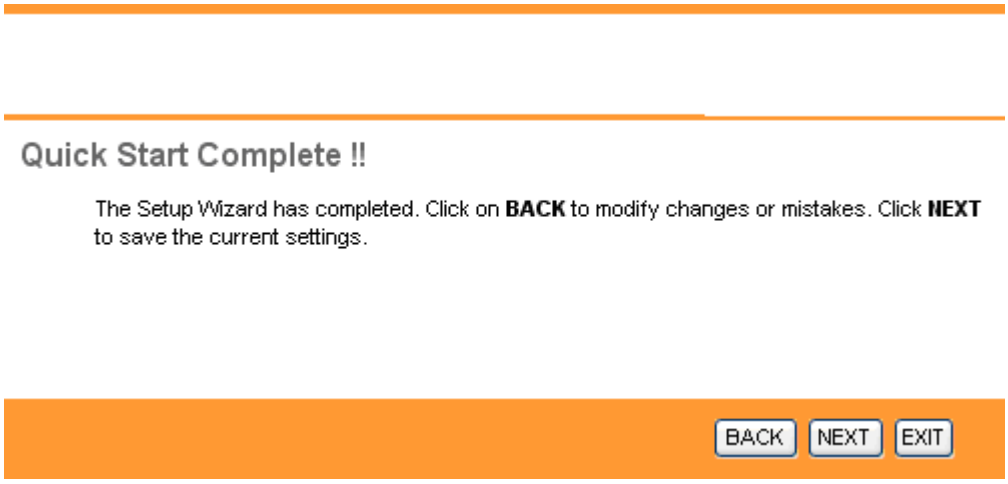
In LLC-based multiplexing, one VC carries multiple protocols with protocol-identifying information contained in each packet header. While this method requires extra bandwidth and

processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol; for example, if charging heavily depends on the number of simultaneous VCs.

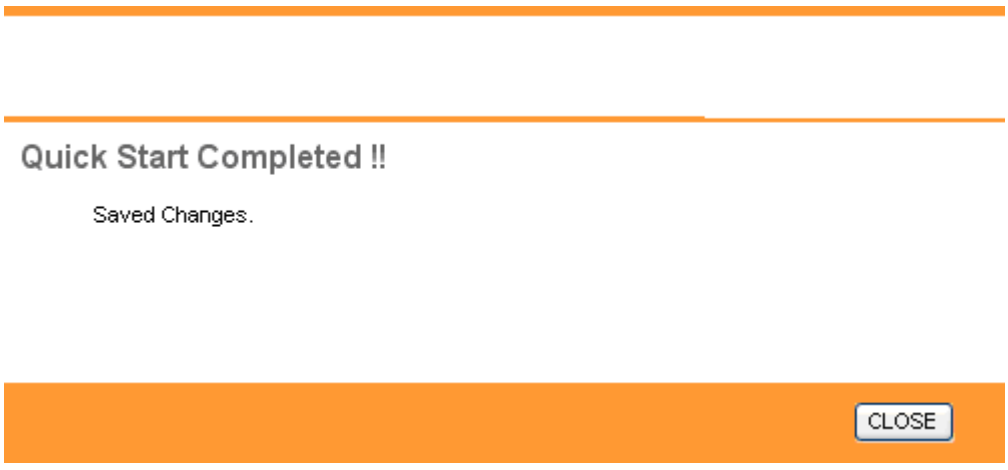
3.3.7 VPI and VCI

Be sure to use the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255. The valid range for the VCI is 32 to 65535. 0 to 31 is reserved for local management of ATM traffic.

3.4 Finishing the Wizard



The Quick Start wizard now has all the information it needs. Click on BACK to make changes or correct mistakes. Click on NEXT to save the current settings. Click on EXIT to exit the wizard without saving.



Your changes have been saved. Click on CLOSE. The Quick Start wizard window will close.

Chapter 4 - The Interface Setup Screens

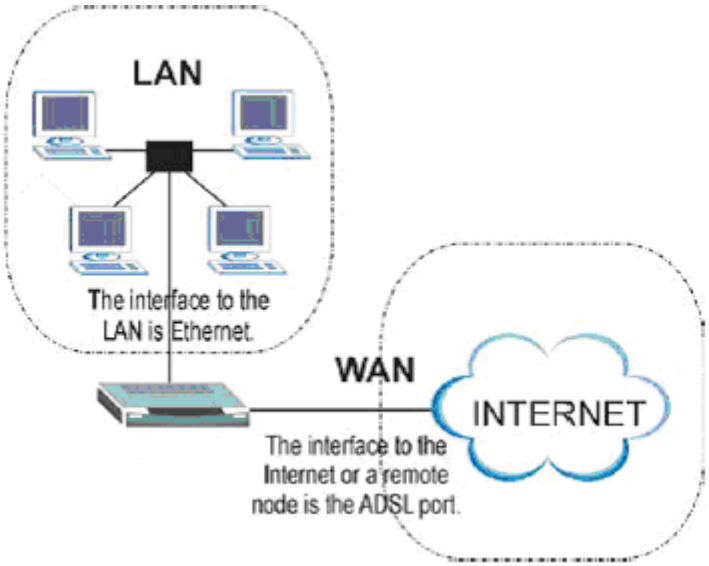
The Interface Setup screens help you connect your DSL-2140/2140W to the Internet and to your local network.

4.1 Interface Setup Overview

The physical connections determine whether the DSL-2140/2140W ports are local area network (LAN) ports or wide area network (WAN) ports. There are two kinds of IP networks. The local, private kind is the LAN network; the global, public kind is the WAN network. The following illustration shows the relationship between the DSL-2140/2140W and the two different networks.

A LAN is a shared communication system to which many computers are attached. A LAN is generally limited to the immediate area, usually the same building or floor of a building.

A WAN is an outside connection to another network or to the Internet.

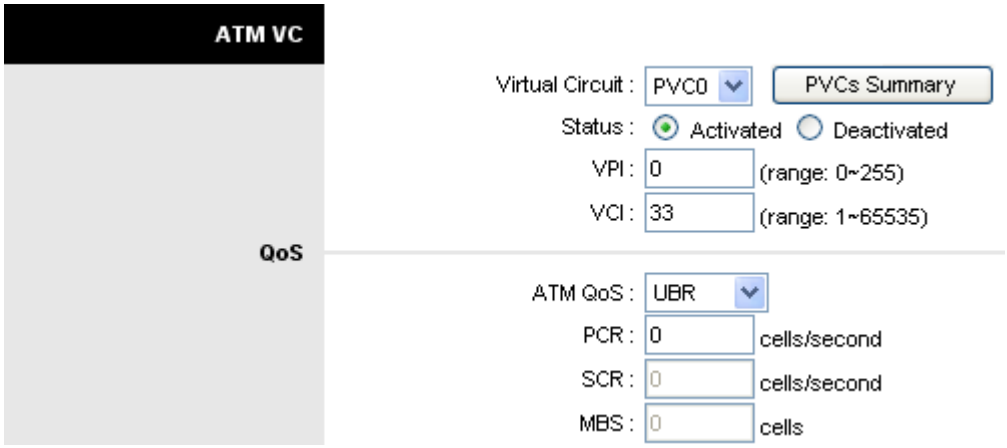


4.2 The Internet Screen

The Internet screen allows you to set up how your DSL-2140/2140W connects to the Internet. If you already ran the Quick Start wizard, the information you provided to the wizard should be entered into the fields already. When you are done making changes, click on the SAVE button to save your changes.

4.2.1 ATM VC & QoS

Asynchronous transfer mode (ATM) is a protocol that arranges data into small, uniform-sized cells with VCI data, as opposed to variable-sized data packets. ATM settings are used to connect to your ISP. Your ISP provides your VPI and VCI setting information. You can configure up to 8 virtual circuits (VC), each using different encapsulations, if you apply for 8 different VCs from your ISP. You must activate each VC for it to take effect. For permanent virtual circuit (PVC) management, you can use ATM Quality of Service (QoS) to set up each PVC traffic line's priority.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Virtual Circuit	Select the PVC you wish to modify.
Status	Each PCV can be toggled Activated or Deactivate.
VPI	Enter your VPI number here.
VCI	Enter your VCI number here.
ATM QoS	Select the QoS type for the PVC in question from the dropdown list.
PCR	Enter the PCR here. For all QoS types.
SCR	Enter the SCR here. Only for rtVBR and nrtVBR.
MBS	Enter the MBS here. Only for rtVBR and nrtVBR.

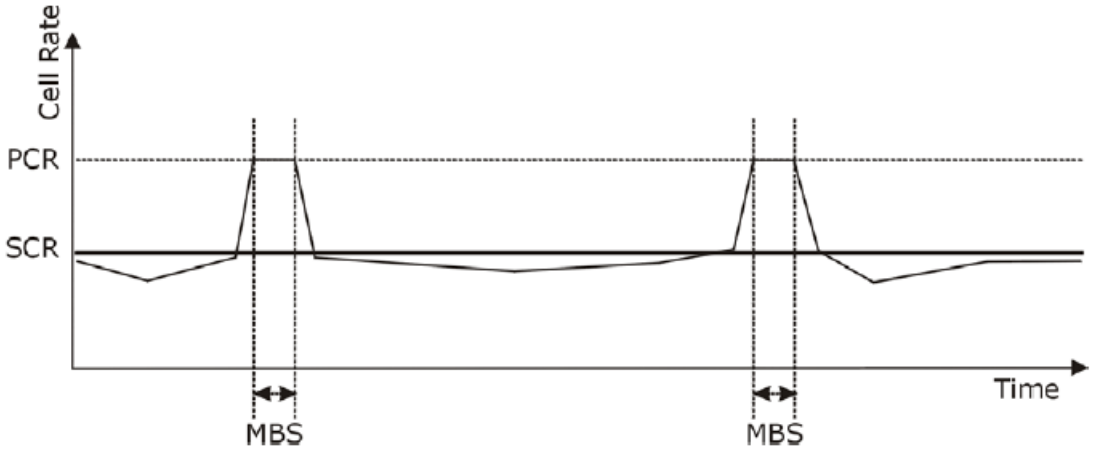
The PVCs Summary button opens a new window that displays the current PVC settings.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832 Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

Sustained Cell Rate (SCR) is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. SCR may not be greater than the PCR; the system default is 0 cells/sec.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

The following figure illustrates the relationship between PCR, SCR and MBS.



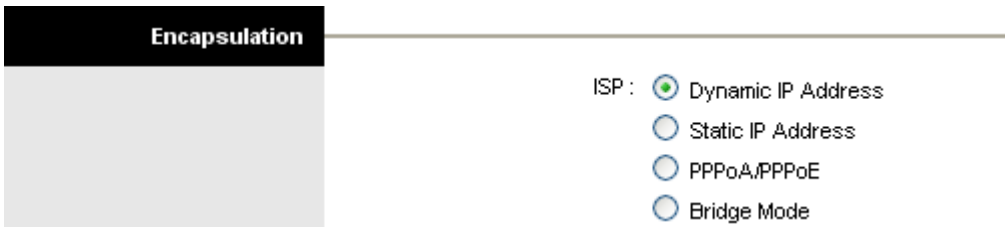
CBR is for connections that support constant rates of data transfer. The only parameter you need to worry about in CBR is PCR.

UBR is for connections that have variable traffic. The only parameter you need to worry about in UBR is PCR.

rtVBR is for connections that, while having variable traffic, require precise timing between traffic source and destination. PCR, SCR and MBS must all be set for rtVBR.

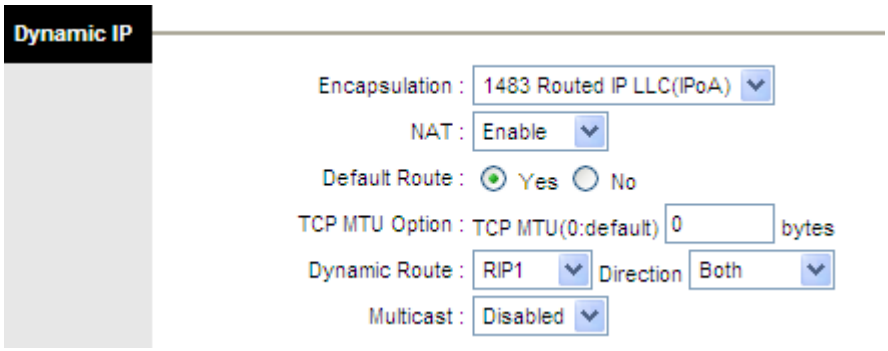
nrtVBR is for connections that have variable traffic, do not require precise timing, but still require a set bandwidth availability. PCR, SCR and MBS must all be set for nrtVBR.

4.2.2 Encapsulation



Select the encapsulation protocol your ISP uses. The following section will vary depending on which encapsulation protocol you select.

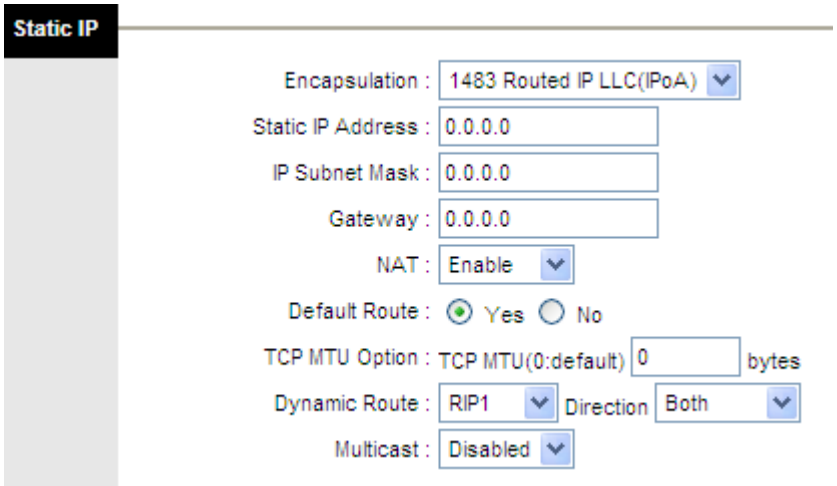
4.2.2.1 Dynamic IP Address



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Encapsulation	Select your encapsulation type from the dropdown list.
Bridge interface	Select whether Bridge interface is activated or deactivated.
NAT	Select whether NAT is Enabled or Disabled.
Default Route	Select whether this PVC will be the default route for Internet data.
TCP MTU Option	Enter you TCP MTU bytes here. (Default is 0 bytes)
Dynamic Route	Select the RIP type and direction from the dropdown lists.
Multicast	Select the multicast protocol you wish to use from the dropdown list.

4.2.2.2 Static IP Address

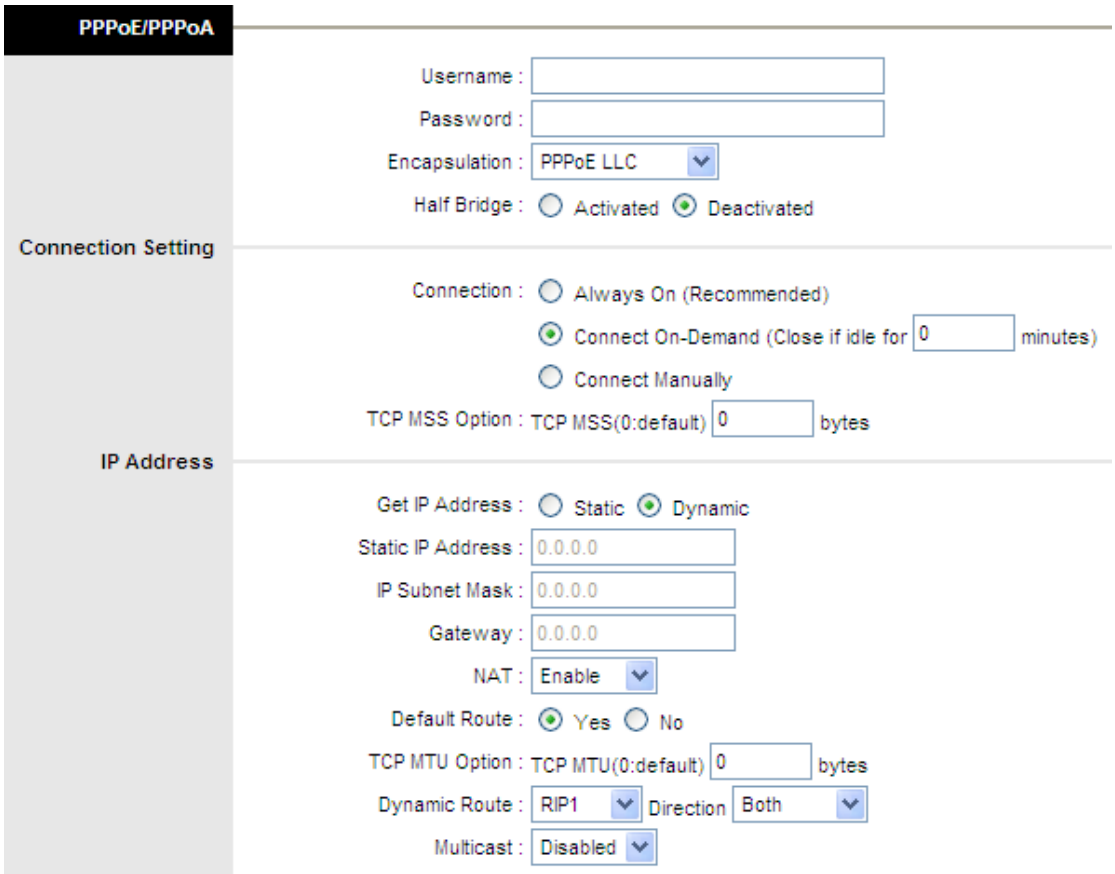


The following table describes the labels in this screen.

LABEL	DESCRIPTION
Encapsulation	Select your encapsulation type from the dropdown list.
Static IP Address	Enter the static IP Address here.
IP Subnet Mask	Enter the IP Subnet Mask here.
Gateway	Enter the Gateway address here.
NAT	Select whether NAT is Enabled or Disabled.
Default Route	Select whether this PVC will be the default route for Internet data.
TCP MTU Option	Enter you TCP MTU bytes here. (Default is 0 bytes)
Dynamic Route	Select the RIP type and direction from the dropdown lists.
Multicast	Select the multicast protocol you wish to use from the dropdown list.

Your ISP should provide the above information.

4.2.2.3 PPPoE/PPPoA



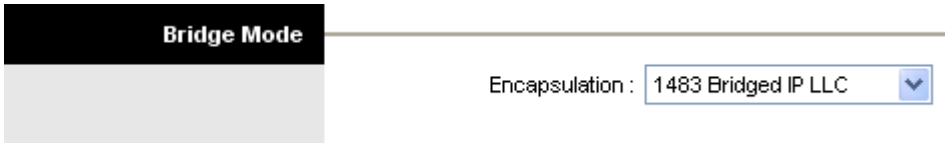
The following table describes the labels in this screen.

LABEL	DESCRIPTION
Username	Enter your username here.

Password	Enter your password here.
Encapsulation	Select your encapsulation type from the dropdown list.
Bridge interface	Select whether Bridge interface is activated or deactivated.
Connection	Select whether your connection is always on or if it connects on demand. If on demand, specify how many minutes the connection may be idle before it disconnects.
TCP MSS Option	Enter the TCP MSS you wish to use here.
Get IP Address	Choose whether the TC3162 EVM obtains the IP address statically or dynamically.
Static IP Address	Enter the static IP address here. Only if you chose Static above.
IP Subnet Mask	Enter the IP subnet mask here. Only if you chose Static above.
Gateway	Enter the gateway here. Only if you chose Static above.
NAT	Select whether NAT is Enabled or Disabled.
Default Route	Select whether this PVC will be the default route for Internet data.
TCP MTU Option	Enter you TCP MTU bytes here. (Default is 0 bytes)
Dynamic Route	Select the RIP type and direction from the dropdown lists.
Multicast	Select the multicast protocol you wish to use from the dropdown list.

Your ISP should provide the above information. Note that you must enter the user name exactly as your ISP assigned it. If the assigned name is in the form of user@domain where domain identifies a service name, enter it exactly as given.

4.2.2.4 Bridge Mode

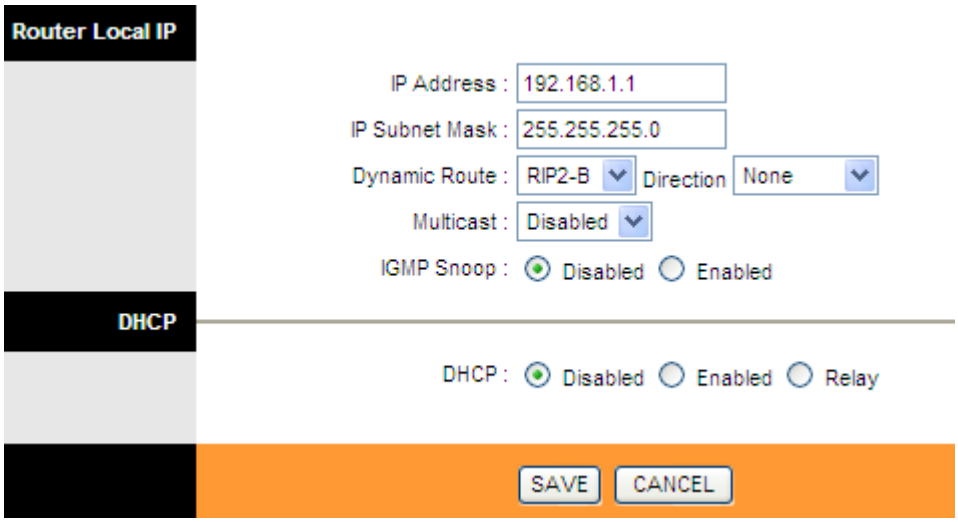


The following table describes the labels in this screen.

LABEL	DESCRIPTION
Encapsulation	Select your encapsulation type from the dropdown list.

4.3 The LAN Screen

The LAN screen allows you to set up how your DSL-2140/2140W connects to your LAN. When you are done making changes, click on SAVE to save your changes or CANCEL to reset the fields to their original states.



4.3.1 Router Local IP

The following table describes the labels in this screen.

LABEL	DESCRIPTION
IP Address	Enter the IP address you wish to use with your LAN here.
IP Subnet Mask	Enter the IP subnet mask you wish to use with your LAN here.
Dynamic Route	Select the Routing Information Protocol (RIP) you wish to use from the dropdown list and the direction you want from the dropdown list. The RIP and direction options are described below.
Multicast	Select the multicast protocol you wish to use from the dropdown list.

4.3.1.1 Explaining RIP Setup

Routing Information Protocol (RIP) allows a router to exchange routing information with other routers. The RIP Direction field controls how RIP packets are allowed to enter and leave the router. Selecting Both means the DSL-2140/2140W will broadcast its routing table and incorporate the RIP information that it receives. Selecting “In Only” means the DSL-2140/2140W will only accept RIP packets received, not send RIP packets. Selecting “Out

Only" means the DSL-2140/2140W will only send RIP packets, not accept any RIP packets received. Selecting "None" means the DSL-2140/2140W will not send any RIP packets nor will it accept any RIP packets received.

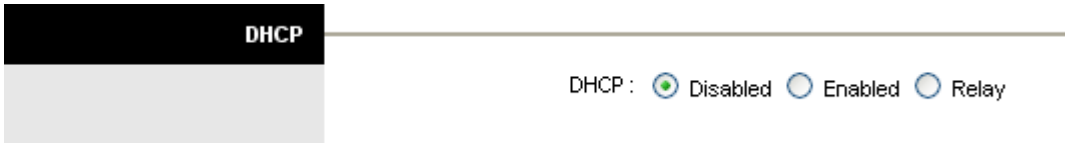
The Dynamic Route field controls the format and the broadcasting method of RIP packets that the DSL-2140/2140W sends. It recognizes both formats when receiving packets.

RIP-1 is universally supported, but RIP-2 carries more information. RIP-1 is adequate for most networks. Only consider RIP-2 if your network has unusual topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format. RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.

4.3.2 Introducing DHCP

Dynamic Host Control Protocol (DHCP), when enabled, gives out IP addresses to a device that requests an IP address to be logged on to the network as it boots up. A device must be configured as a DHCP client to obtain the IP address automatically. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.



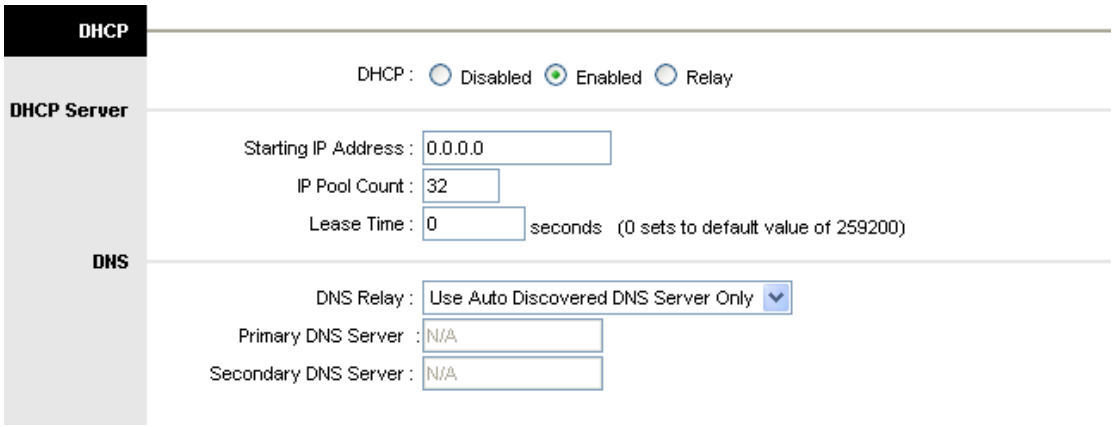
The following table describes the labels in this screen.

LABEL	DESCRIPTION
DHCP	Select whether DHCP is Disabled, Enabled or Relay.

The next screen will vary depending on the DHCP option you selected.

4.3.3 Enabled DHCP

The following screen will appear if you selected Enabled in the DHCP Server field.



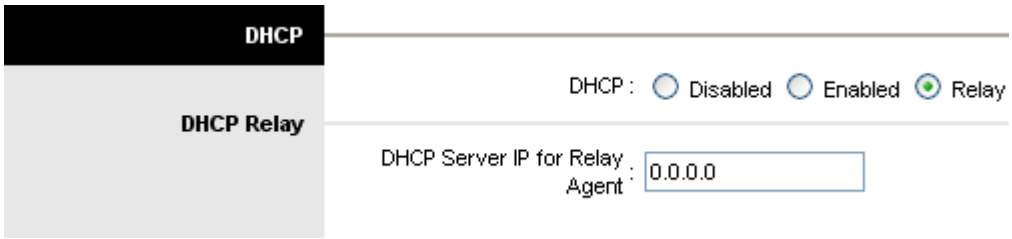
The following table describes the labels in this screen.

LABEL	DESCRIPTION
Starting IP Address	Enter the starting IP address you wish to use as the DHCP server's IP assignment.
IP Pool Count	Enter the maximum user pool size you wish to allow.
Lease Time	Enter the amount of time you wish to lease out a given IP address.
DNS Relay	Select the DNS relay option you wish to use from the dropdown list.
Primary DNS Server	Enter the primary DNS server IP address you wish to use. For user discovered DNS only.
Secondary DNS Server	Enter the secondary DNS server IP address you wish to use. For user discovered DNS only.

If you don't want to use the DNS Relay option, set the DNS relay to "Use User Discovered DNS Server Only" and set both Primary and Secondary DNS Servers to "0.0.0.0".

4.3.4 Relay DHCP

The following screen will appear if you selected Relay in the DHCP Server field.



The following table describes the labels in this screen.

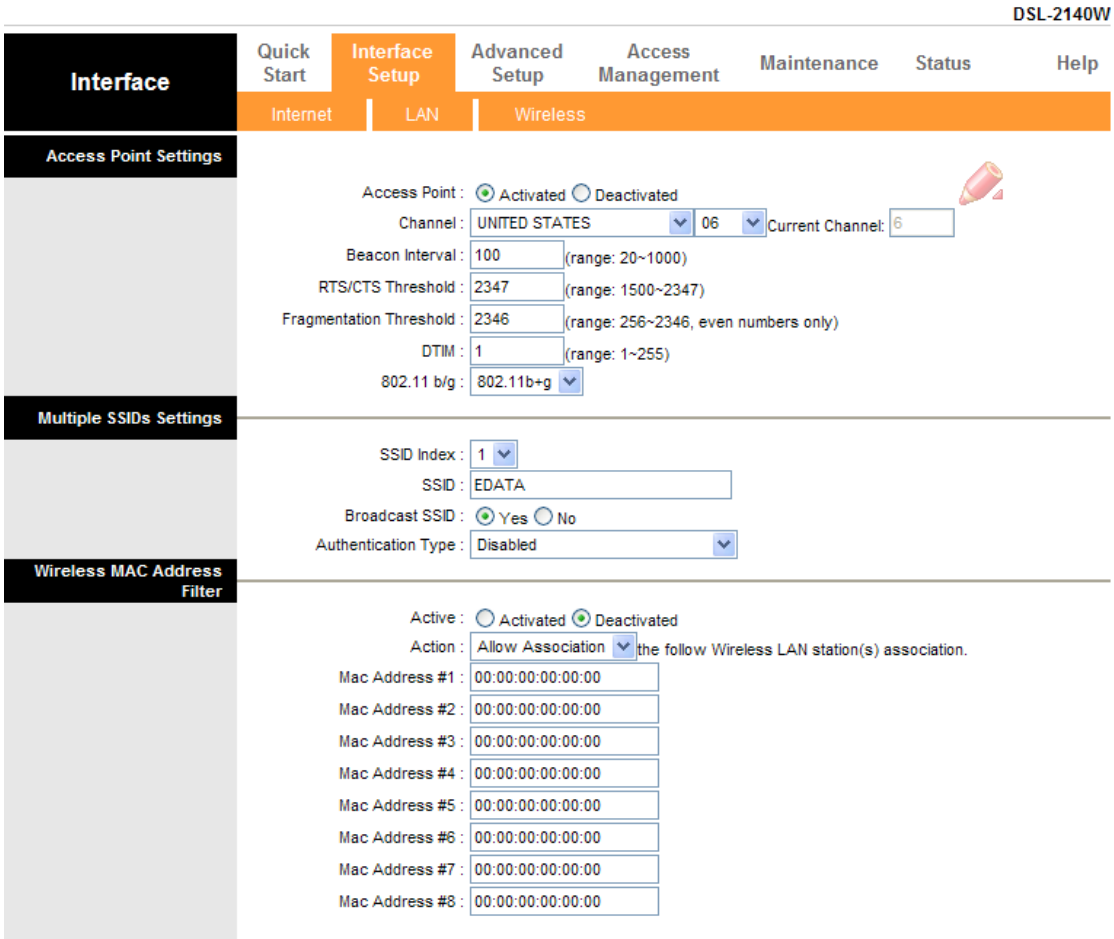
LABEL	DESCRIPTION
DCHP Server IP for Relay Agent	Enter the IP address for the DHCP relay agent.

A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the IP addresses. If the DHCP Relay option is enabled, DHCP requests from local PCs will be forwarded to the DHCP server that runs on WAN side. For this function working properly, you must run it on router mode only; disable the DHCP server on the LAN port and make sure the routing table has the correct routing entry.

4.4 The Wireless LAN Screen (for DSL-2140W only)

The wireless LAN Screen includes some basic configurations. The complexity of wireless LAN depends on the network environment. That is, wireless LANs are simple while two computers with wireless LAN cards communicate in a peer-to-peer network, though they still need more complicated setting as

there are a number of computers with wireless LAN card communicating through access points which bridge network traffic to the wired LAN.



4.4.1 Access Point Settings

The following table describes the labels in this screen.

LEBAL	DESCRIPTION
Access Point	Default setting is set to **Activated**. If you do not have any wireless, both 802.11g and 802.11b, device in your network, select **Deactived.**
Channel	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel from the drop-down list box.
Beacon interval	The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network.
RTS/CTS Threshold	The RTS (Request To Send) threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake Enter a value between 1500 and 2347.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
DMIT	This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).
802.11b/g	The default setting is **802.11b+g** (Mixed mode). If you do not know or have both 11g and 11b devices in your network, then keep the default in **mixed mode**. From the drop-down manual, you can select **802.11g** if you have only 11g card. If you have only 11b card, then select **802.11b**.

4.4.2 Multiple SSIDs Settings

The following table describes the labels in this screen.

LEBAL	DESCRIPTION
SSID Index, SSID	The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change the default name to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.
Broadcast SSID	Select **Yes** to hide the SSID in so a station cannot obtain the SSID through passive scanning. Select **No** to make the SSID visible so a station can obtain the SSID through passive scanning.
Authentication Type	To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP.&WPA. If you require high security for transmissions, there are two alternatives to select from: **64-bit WEP and 128-bit WEP**. WEP 128 will offer increased security over WEP 64. You can disable or enable with WPA or WEP for protecting wireless network. The default type of wireless is **disabled** and to allow all wireless computers to communicate with the access points without any data encryption

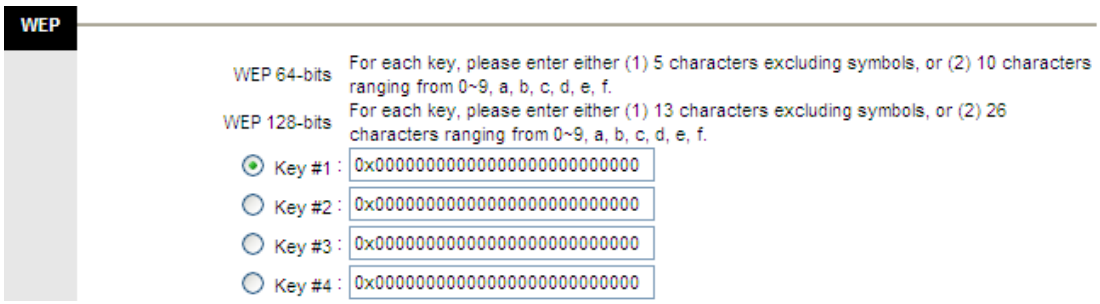
4.4.3 Wireless MAC Address Filter

Users are able to configure the router to give exclusive access to up to 8 devices or exclude up to 8 devices from accessing the router through the MAC filter screen . MAC (Media Access Control) address is a number that acts like a

name for a particular network adapter; the network cards (or built-in network adapters) in two different computers will have different names. However, it is possible to change the MAC address on most of today's hardware. You need to know the MAC address of the devices to configure this screen. To change your router's MAC filter settings, click Wireless LAN, MAC Filter to open the MAC Filter screen. The screen appears as shown.

LEBAL	DESCRIPTION
Active	Select **Actived** to enable MAC address filtering.
Action	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the router.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the router in these address fields.

4.4.3.1 WEP

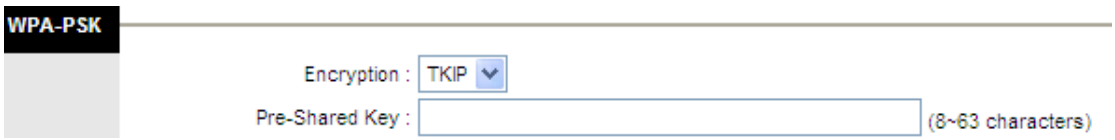


Key 1 to Key 4: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for 64-bitWEP and 128-bitWEP respectively.

If you chose **WEP 64-bits**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "a,b,c,d,e,f").

If you chose **WEP 128-bits**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "a,b,c,d,e,f"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.

4.4.3.2 WPA-PSK



Encryption: TKIP (Temporal Key Integrity Protocol) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

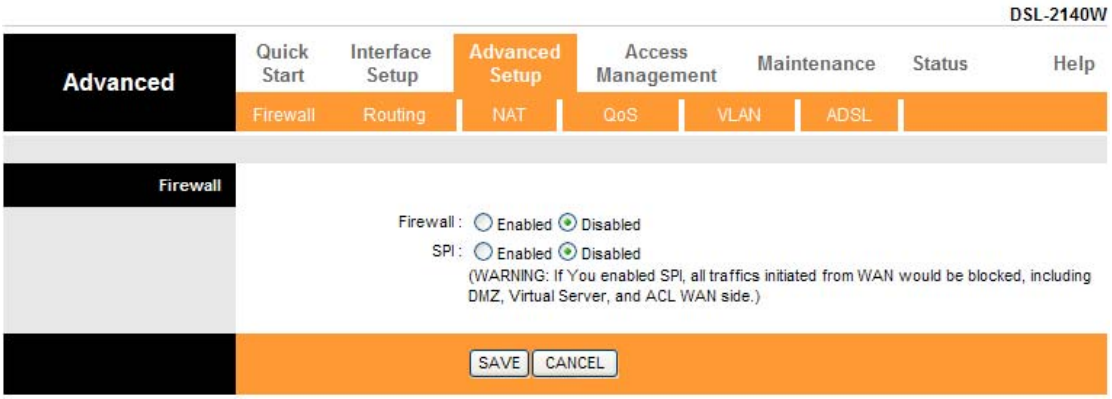
Pre-Shared key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Chapter 5 - The Advanced Setup Screens

The advanced setup screens help you manage how data enters and exits your DSL-2140/2140W.

5.1 The Firewall Screen

In the Firewall Screen, users are able to change the statue of Firewall and SPI.



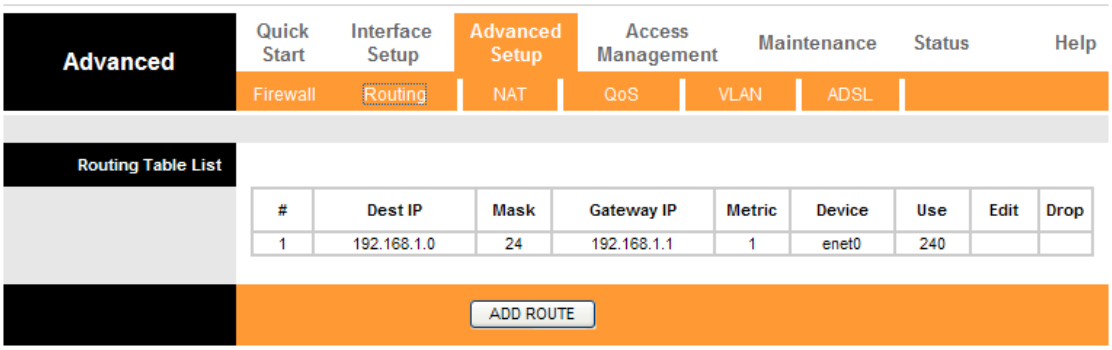
The following table describes the options in this screen.

LABEL	DESCRIPTION
Firewall	Toggle the firewall function Enables or Disabled.
SPI	Toggle the SPI function Enables or Disabled.

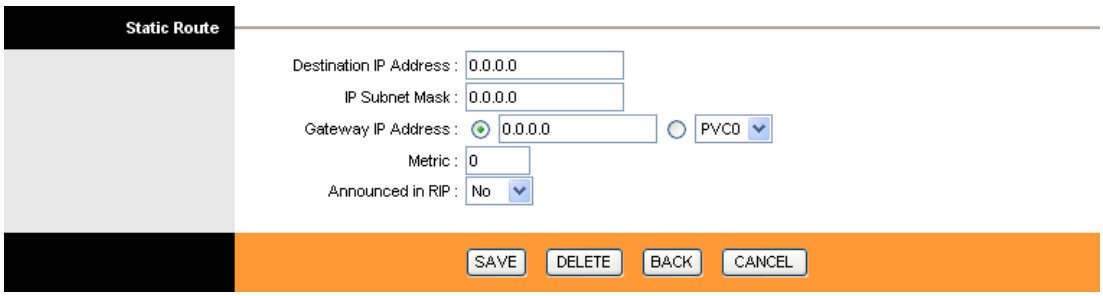
It is noticed that enabling SPI will block the previous setting on WAN.

5.2 The Routing Screen

Routing directs your DSL-2140/2140W to forward data to specific IP addresses.



This screen shows the routing rules you have already set. A few defaults have been configured for you. To add your own route, click on the Add Route button.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Destination IP Address	Enter the destination IP address for this routing rule.
IP Subnet Mask	Enter the destination IP subnet mask for this routing rule.
Gateway IP Address	Enter the gateway IP address for this routing rule or select which PVC will be affected by this routing rule.
Metric	Enter the metric for this routing rule.
Announce in RIP	Choose whether this route is included in RIP broadcasts.

The destination IP address is the IP network address of the final destination of packets routed by this rule.

The IP subnet mask is the subnet mask for the final destination.

A gateway does the actual forwarding of the packets. Enter the gateway's IP address in the field or select which PVC you wish to act as a gateway.

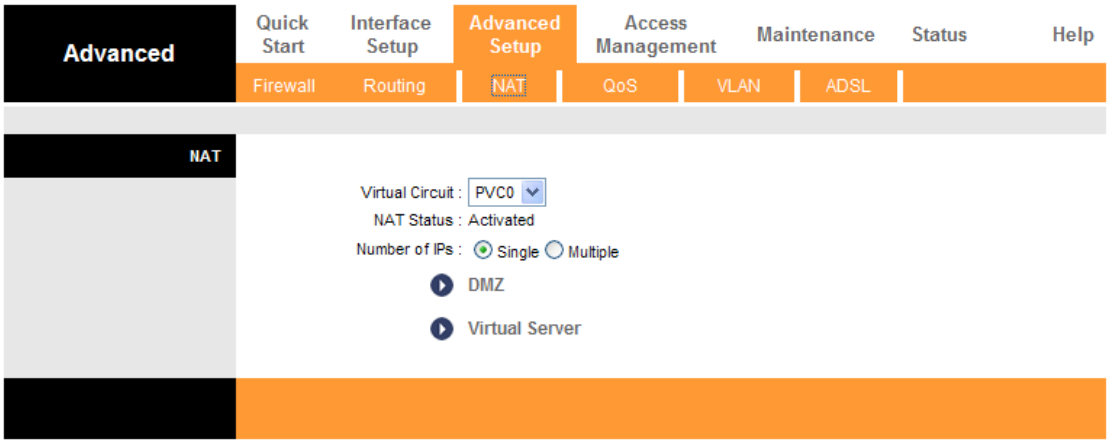
The metric is a rough estimate of the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. As a rough estimate, enter a number that approximates the cost for this link. The number must be within 1 and 15, inclusive. Generally, 2 or 3 is a good number to use.

If the route is announced in RIP, the route will be sent to other hosts through RIP broadcasts. If not announced, the route is private and not included in RIP broadcasts.

When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set, BACK to return to the previous screen or CANCEL to exit without saving.

5.3 The NAT Screen

Network Address Translation (NAT, RFC 1631) translates the host IP address in a packet used within one network to a different IP address known within another network.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Virtual Circuit	Select the virtual circuit you wish to edit from the dropdown list.
NAT Status	The NAT status of the selected VC.
Number of IPs	Toggle whether the Virtual Circuit NAT affects a Single IP or Multiple IPs.
DMZ	Click this link to go to the DMZ screen.
Virtual Server	Click this link to go to the Virtual Server screen.

5.3.1.1 What NAT Does

NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. You may also designate servers, such as a Web server and a telnet server, on your local network and make them accessible to the outside world. With no servers defined, your DSL-2140/2140W filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

Inside/outside indicates where a host is located relative to the DSL-2140/2140W. The computers hosts of your LAN are inside, while the Web servers on the Internet are outside.

Global/local indicates the IP address of a host in a packet as the packet traverses a router. The local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host of a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side.

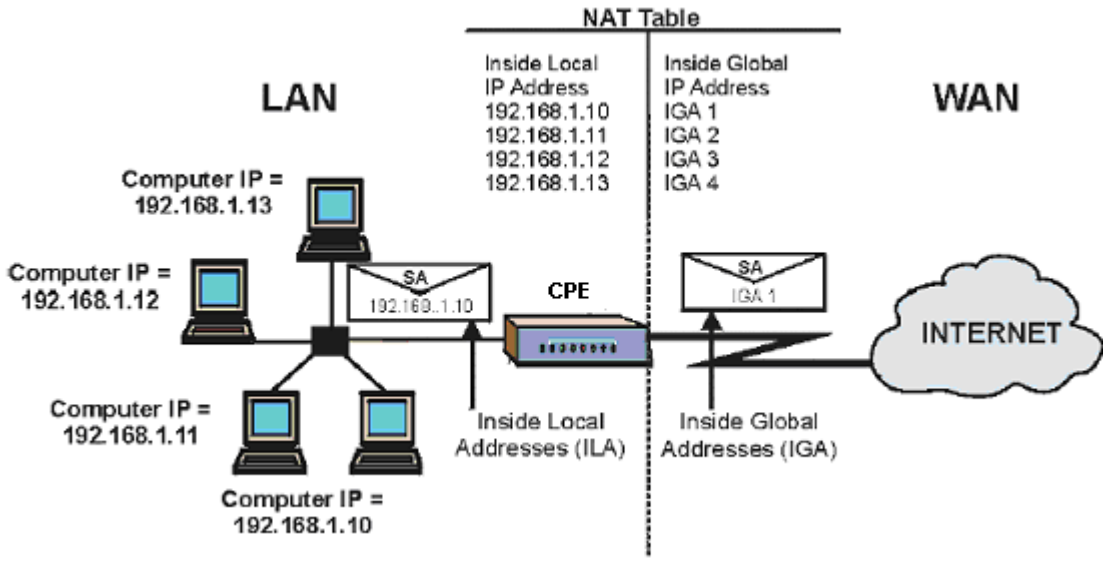
The following table summarizes this information.

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

5.3.1.2 How NAT Works

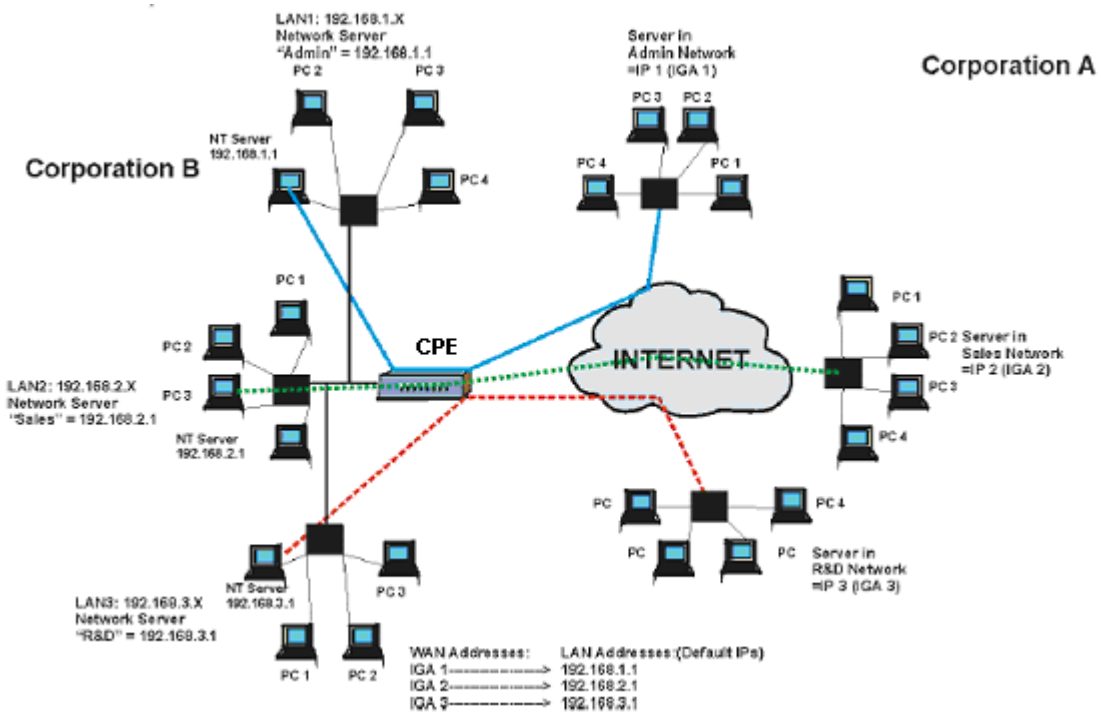
Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA is the source address on the LAN, and the IGA is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The DSL-2140/2140W keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.

The following figure illustrates this.



5.3.1.3 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the DSL-2140/2140W can communicate with three distinct WAN networks. More examples follow at the end of this chapter.



5.3.1.4 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

1. One-to-One: In One-to-One mode, the DSL-2140/2140W maps one local IP address to

one global IP address.

2. Many-to-One: In Many-to-One mode, the DSL-2140/2140W maps multiple local IP addresses to one global IP address.

3. Many-to-Many Overload: In Many-to-Many Overload mode, the DSL-2140/2140W maps multiple local IP addresses to shared global IP addresses.

4. Many-to-Many No Overload: In Many-to-Many No Overload mode, the DSL-2140/2140W maps each local IP address to a unique global IP address.

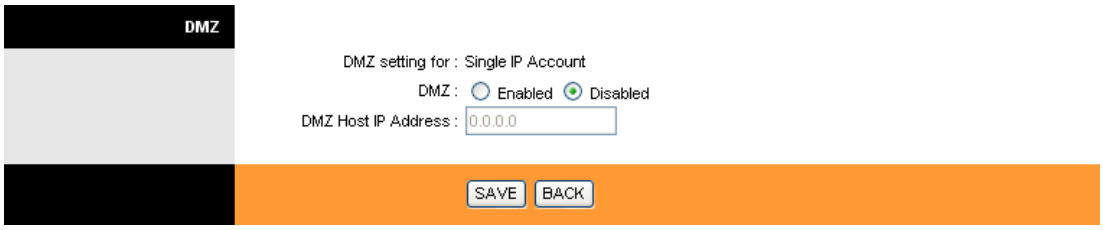
5. Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

The following table summarizes these types.

TYPE	IP MAPPING
One-to-One	ILA1 IGA1
Many-to-One (SUA/PAT)	ILA1 IGA1 ILA2 IGA1 …
Many-to-Many Overload	ILA1 IGA1 ILA2 IGA2 ILA3 IGA1 ILA4 IGA2 …
Many-to-Many No Overload	ILA1 IGA1 ILA2 IGA2 ILA3 IGA3 …
Server	Server 1 IP IGA1 Server 2 IP IGA1 Server 3 IP IGA1

5.3.2 DMZ

A demilitarized zone (DMZ) is a host between a private local network and the outside public network. It prevents outside users from gaining access to a server that you wish to keep private. Users of the public network outside the company can only access the DMZ host.



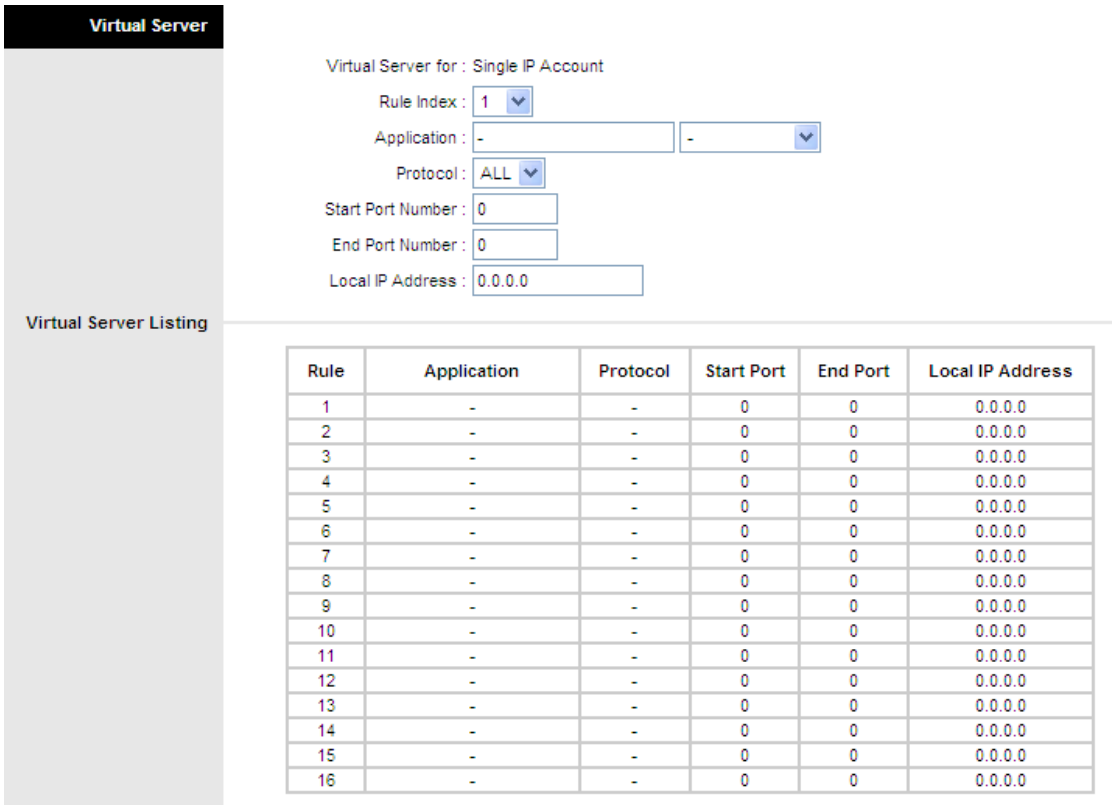
The following table describes the labels in this screen.

LABEL	DESCRIPTION
DMZ	Toggle the DMZ function Enabled or Disabled.
DMZ Host IP Address	Enter the IP address of the DMZ host you wish to use.

When you are done making changes, click on SAVE to save your changes or on BACK to return to the previous screen.

5.3.3 Virtual Server

A virtual server is a server behind NAT (on the LAN), such as a Web server or FTP server, which you can make visible to the outside world while NAT makes your network appear as a single machine.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Rule Index	Select which rule index to use with this virtual circuit. All VCs with the same IP will use the same rules.
Application	Select the Application you wish to support like: FTP, H.323…etc
Protocol	Select the protocol you wish to support: TCP, UDP or BOTH
Start Port Number	Enter the specific port number you wish to start forwarding at.
End Port Number	Enter the specific port number you wish to end forward at. This number may be the same as the Start Port Number.
Local IP Address	Enter the IP address of the virtual server on the LAN.
Virtual Server Listing	This is a listing of all virtual servers you have set.

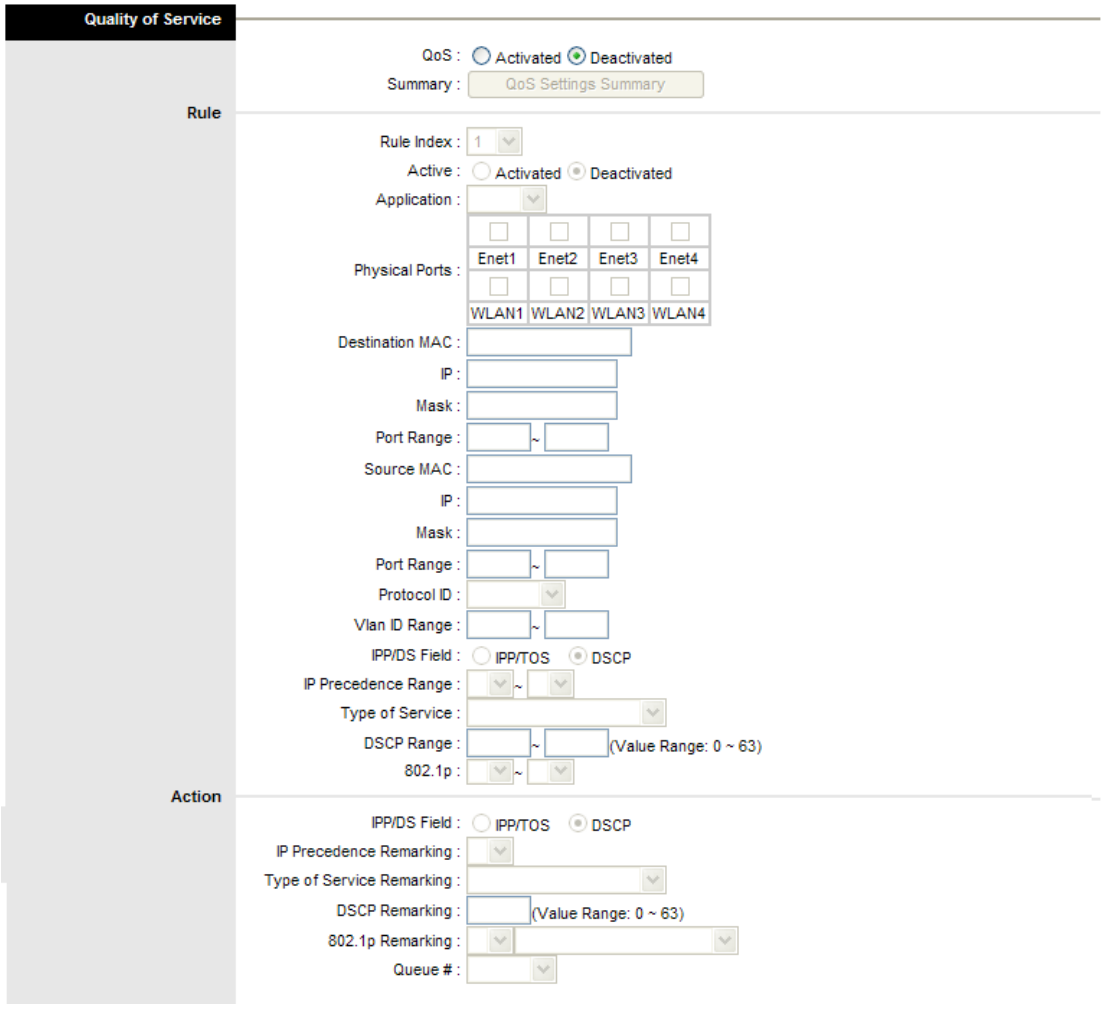
When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set, BACK to return to the previous screen or CANCEL to exit without saving.

5.4 The QoS Screen

Quality of Service (QoS) helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice data packets given higher priority than Web data packets.

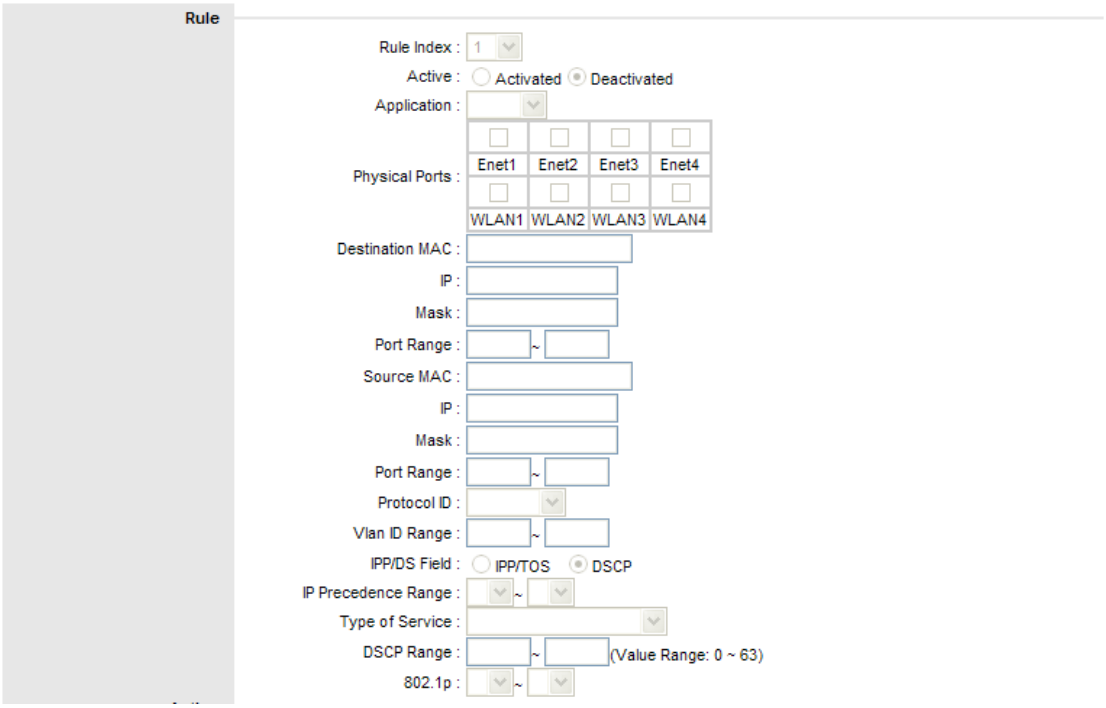
The main goal of QoS is prioritizing incoming data, preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn't interfere with other data flows.

QoS can be toggled Activated and Deactivated. QoS must be activated before you can edit the following options. When you are done making changes, click on SAVE to save your changes.



5.4.1 Rule

You can set 16 different QoS rules. Each QoS rule has its detail setting conditions like: 802.1p,application, DSCP, IP, MAC, Protocol, TOS, VLAN…etc, you can modify the default value to any new one you wish. Please notice that only when the packet fulfill every detail setting conditions here, then this packet will be remarked as the priority queue of each rule. The non-selected setting part will be treated as “don’t care” and the system will not handle this setting part. If the original packet does not have 802.1q tagged header, system will not add header for this packet even the detail setting condition has adding 802.1p priority ability.



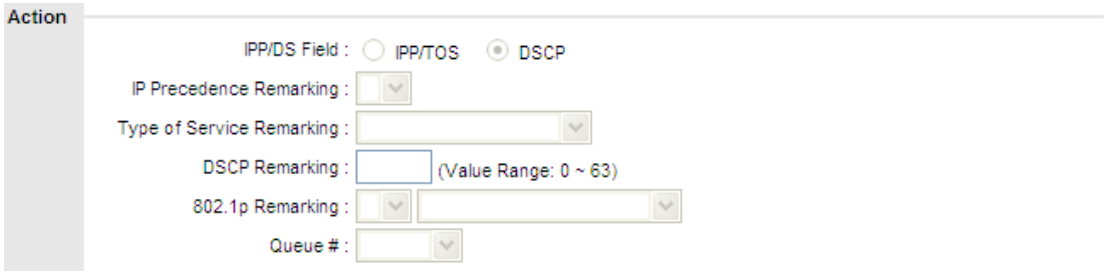
The following table describes the labels in this screen.

LABEL	DESCRIPTION
Rule Index	Select 16 different rules, each rule's detail can be set and saved
Active	Select QoS is activated or deactivated
Application	Select 11 different applications: IGMP, SIP, H.323, MGCP, SNMP, DNS, DHCP, RIP, RSTP, RTCP, RTP
Physical Ports	Once you select the application, the associated ports will be displayed
Destination MAC	Set the Ethernet MAC value that you want to filter in destination side
Destination IP	Set the IP address value that you want to filter in destination side
Destination Mask	Set the subnet mask value that you want to filter in destination side
Destination Port Range	Set the port range value that you want to filter in destination side
Source MAC	Set the Ethernet MAC value that you want to filter in source side
Source IP	Set the IP address value that you want to filter in source side
Source Mask	Set the subnet mask value that you want to filter in source side
Source Port Range	Set the port range value that you want to filter in source side
Protocol ID	Set the protocol ID type that you want to filter
Vlan ID Range	Set the Vlan value that you want to filter
IPP/DS Field	Select IP QoS format
IP Precedence Range	Select the IP precedence range
Type of Service	Select 5 different type of service
DSCP Range	Set the DSCP value that you want to filter

802.1p	Set the remarked new 802.1p priority value on the packet that fulfill every detail setting condition of each rule

5.4.2 Action

After finishing all rules detail condition setting, select the rule you want to execute and action here.



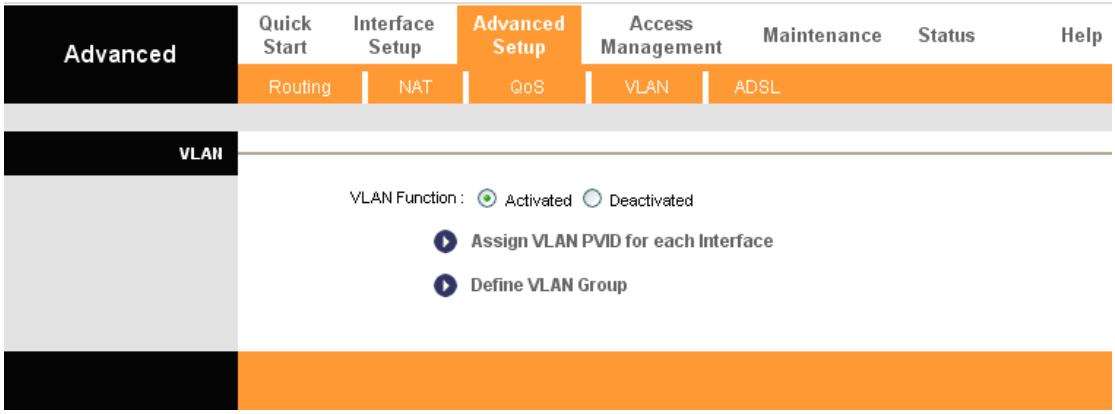
The following table describes the labels in this screen.

LABEL	DESCRIPTION
IPP/DS Field	Select IP QoS format
IP Precedence Remarking	Select the remarking value of IP precedence
Type of service Remarking	Select the remarking value of type of service
DSCP Remarking	Select the remarking value of DSCP
802.1p Remarking	Select the remarking value of 802.1p
Queue #	Select four types of Queue: Low, Medium, High, Highest

5.5 The VLAN Screen

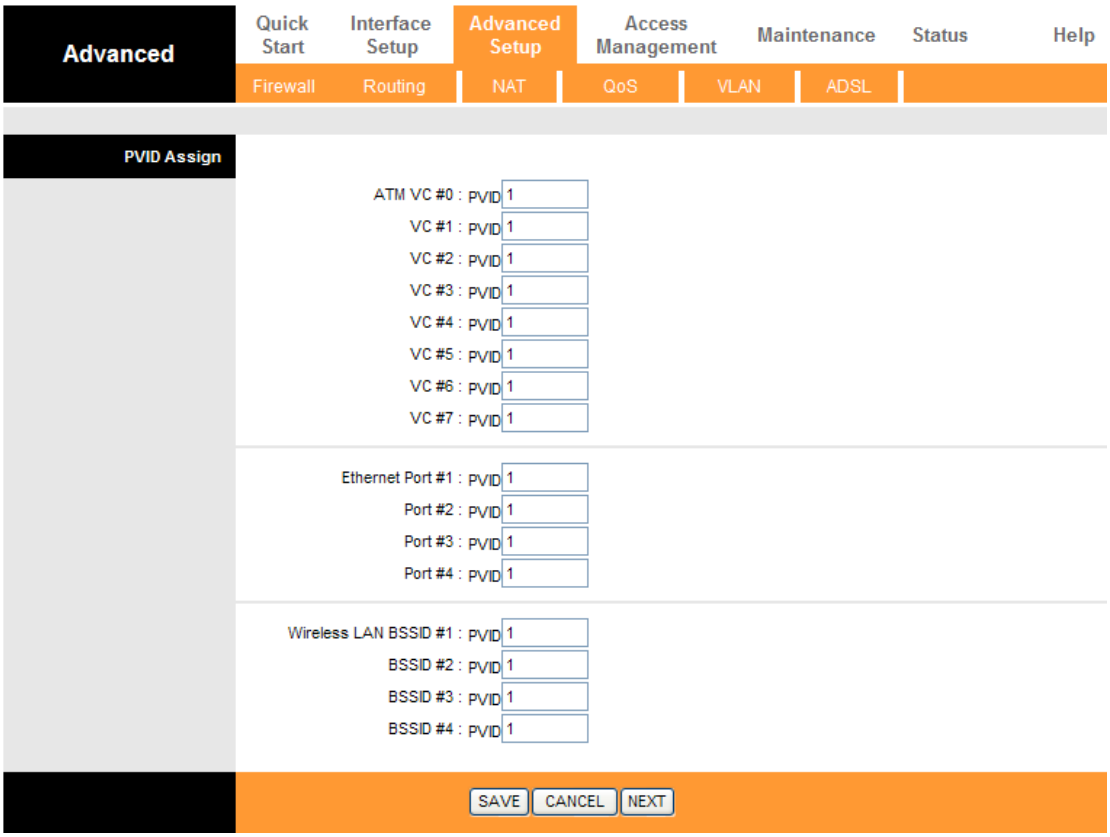
A Virtual LAN (VLAN) is a switched network logically segmented by functions, project teams, or applications; the physical location of VLAN members is unimportant. VLANs allow ports on the same or different switches to be grouped so that traffic is confined to members of only that group. In high-traffic networks, VLANs can reduce the amount of data sent to unnecessary destinations.

VLAN can be toggled Activated or Deactivated. Note that VLAN must be activated before you can access the next two screens.



Click on Assign VLAN PVID for each Interface or Define VLAN group to open the respective screens.

5.5.1 Assigning VLAN PVID for Each Interface



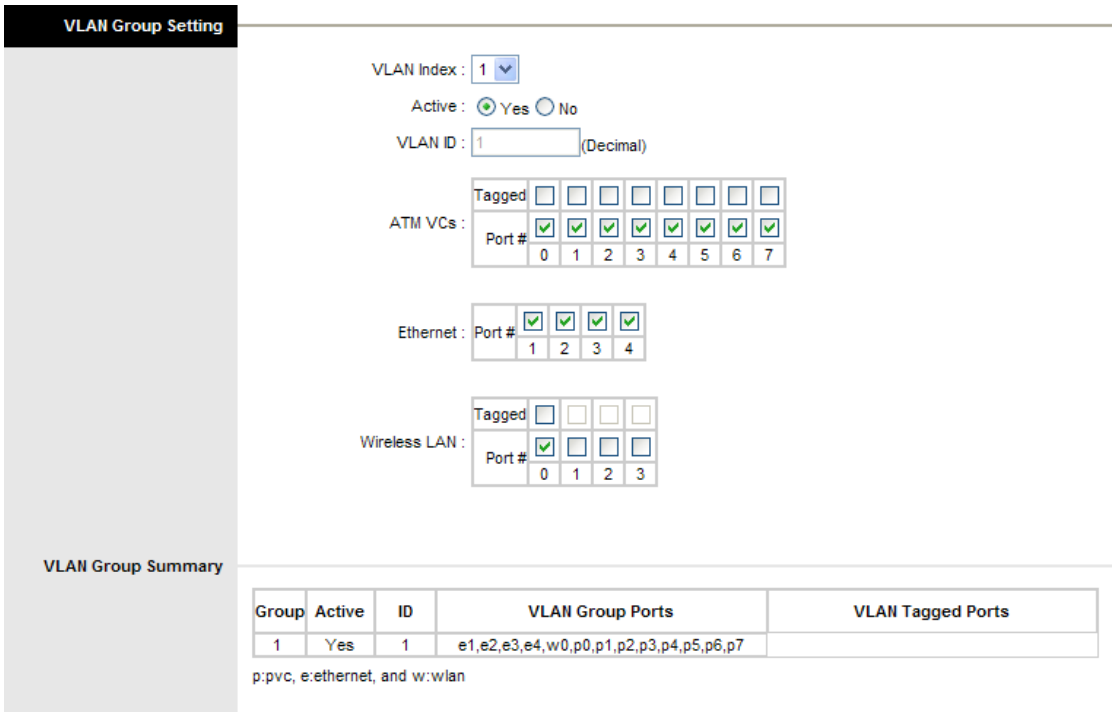
The following table describes the labels in this screen.

LABEL	DESCRIPTION
ATM VC #0: PVID	Enter the PVID number you wish to assign to ATM VC#0
VC #1: PVID	Enter the PVID number you wish to assign to ATM VC#1

VC #2: PVID	Enter the PVID number you wish to assign to ATM VC#2
VC #3: PVID	Enter the PVID number you wish to assign to ATM VC#3
VC #4: PVID	Enter the PVID number you wish to assign to ATM VC#4
VC #5: PVID	Enter the PVID number you wish to assign to ATM VC#5
VC #6: PVID	Enter the PVID number you wish to assign to ATM VC#6
VC #7: PVID	Enter the PVID number you wish to assign to ATM VC#7
Ethernet Port #1: PVID	Enter the PVID number you wish to assign to Ethernet Port #1
Ethernet Port #2: PVID	Enter the PVID number you wish to assign to Ethernet Port #2
Ethernet Port #3: PVID	Enter the PVID number you wish to assign to Ethernet Port #3
Ethernet Port #4: PVID	Enter the PVID number you wish to assign to Ethernet Port #4
Wireless LAN BSSID #1:PVID	Enter the PVID number you wish to assign to Wireless LAN BSSID #1
Wireless LAN BSSID #2:PVID	Enter the PVID number you wish to assign to Wireless LAN BSSID #2
Wireless LAN BSSID #3:PVID	Enter the PVID number you wish to assign to Wireless LAN BSSID #3
Wireless LAN BSSID #4:PVID	Enter the PVID number you wish to assign to Wireless LAN BSSID #4

When you are done making changes, click on SAVE to save your changes, CANCEL to exit without saving or NEXT to continue to the next screen.

5.5.2 Defining Each VLAN Group

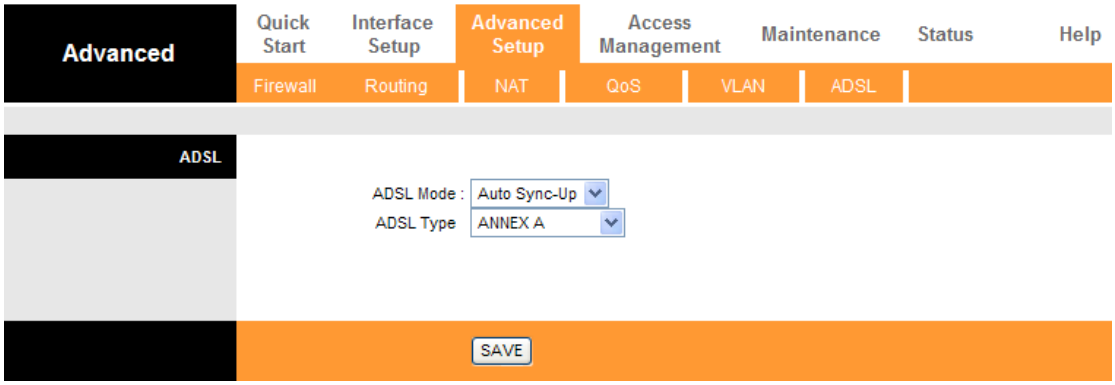


The following table describes the labels in this screen.

LABEL	DESCRIPTION
VLAN Index	The number of the index is determined by the model or IC.
Active	Toggle this index on or off with Yes and No, respectively.
VLAN ID	Enter the VLAN ID number.
ATM VCs	Checking the Tagged and Port # boxes for each port number will add a tag to let other devices know if they need to check the packet and allow the packet through to the port in question, respectively.
Ethernet	Checking the Tagged and Port # boxes for each port number will add a tag to let other devices know if they need to check the packet and allow the packet through to the port in question, respectively.
Wireless LAN	Checking the Tagged and Port # box will add a tag to let other devices know if they need to check the packet and allow the packet through to the port in question, respectively.

When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set or CANCEL to exit without saving.

5.6 The ADSL Screen



The following table describes the labels in this screen.

LABEL	DESCRIPTION
ADSL Mode	Select which mode your ADSL connection uses from the dropdown list.
ADSL Type	Select the ADSL type you use from the dropdown list.

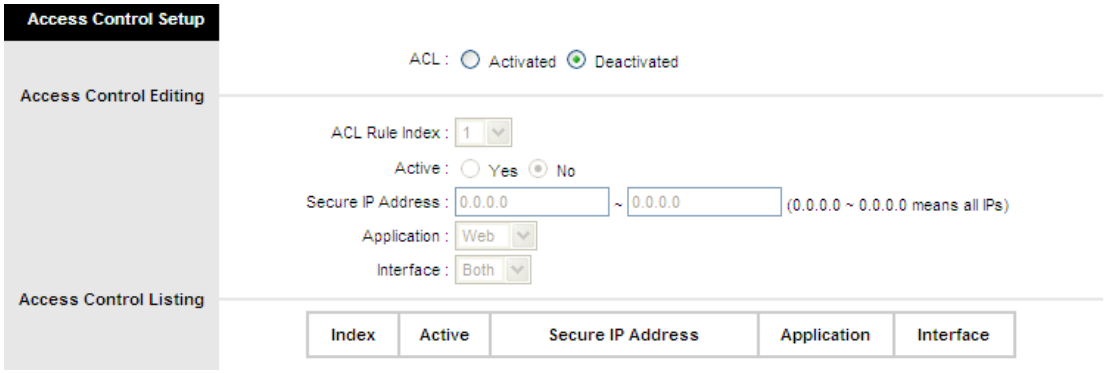
When you are done making changes, click on SAVE to save your changes.

Chapter 6 - The Access Management Screens

The access management screens help you manage what can access your network.

6.1 The ACL Screen

Access Control Listing (ACL) is a management tool that acts as a filter for incoming or outgoing packets, based on application.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
ACL	ACL can be toggled Activated or Deactivated. ACL must be Activated before you can edit the settings.
ACL Rule Index	Select the rule index you wish to edit.
Active	Toggle the rule on or off with Yes or No, respectively.
Secure IP Address	Enter the IP address you wish to give access. Note that entering 0.0.0.0 allows all packets access.
Application	Select the application you wish to give access. Note that the first application you give access should be Web, or you will no longer be able to access the router through the Web configurator.
Interface	Select the interface the above rules should modify.

Access Control Listing is a list of all the rules you have set for access control.

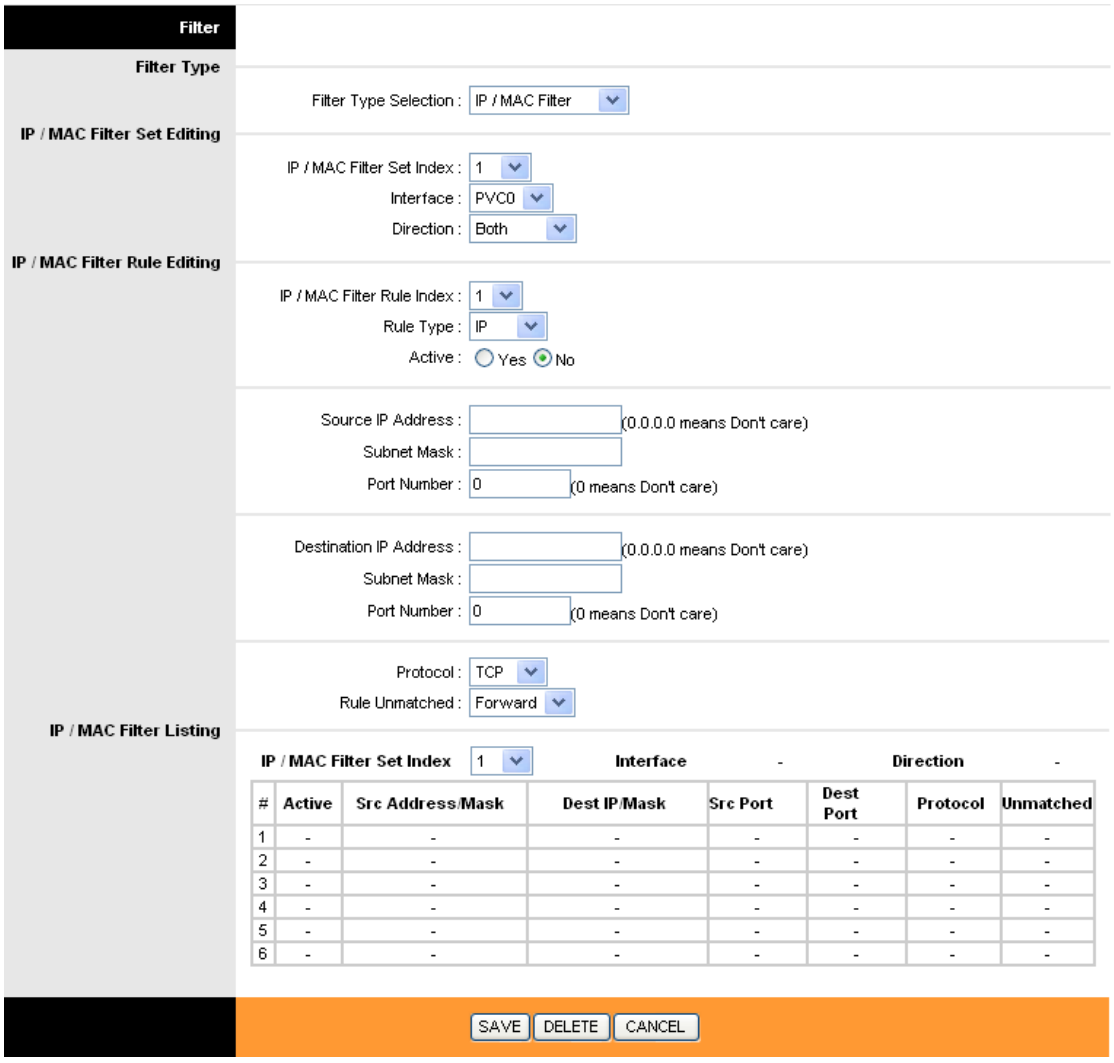
When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set or CANCEL to exit without saving.

6.2 The Filter Screen

Filter is a more complex filtering tool. Three filter types are available in DSL-2120: IP/MAC filter, Application Filter, and URL Filter.

6.2.1 Assigning IP/MAC Filter

Each of the indices can hold six rules, and each interface can have four associated indices, allowing 24 rules per interface. If all six rules in an index are Next rules, the data will be sent to the next index for filtering.

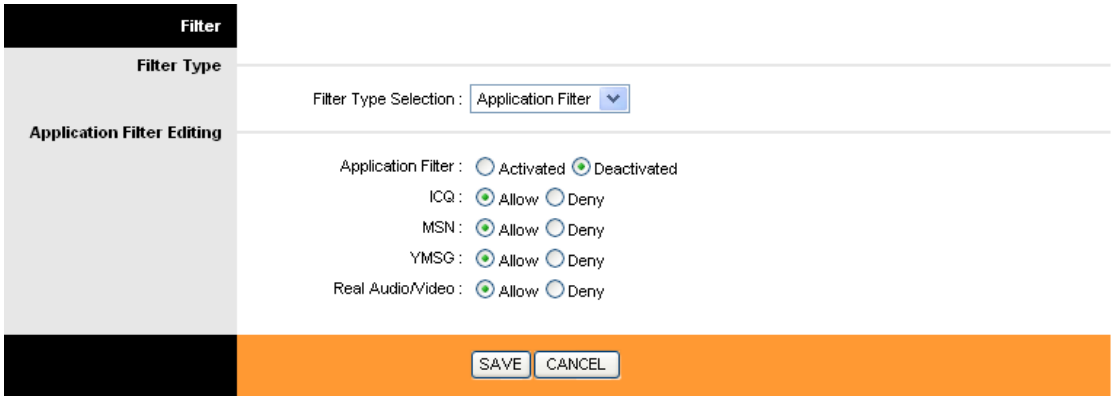


The following table describes the labels in this screen.

LABEL	DESCRIPTION
IP/MAC Filter Set Index	Select the IP/MAC Filter Set you wish to modify.
Interface	Select the Interface you wish to modify. PVC0-PVC7 are WAN interfaces
Direction	Select which direction of data flow you wish to apply the filters to. Note that Incoming and Outgoing are from the point of view of your router, relative to the interface you select. For WAN, data coming from outside your system is considered Incoming and data leaving your system is Outgoing. For LAN, data leaving your system is considered Incoming and data entering your system is Outgoing.
IP/MAC Filter Rule Index	Select the IP/MAC Filter Rule Index you wish to modify.
Rule Type	Select the filter rule type: IP or MAC.
Active	Toggle this rule index on or off with Yes or No, respectively.
For IP Filter Only	
Source IP Address	Enter the source IP address you wish to deny access to your system.
Subnet Mask	Enter the subnet mask of the source IP address.
Port Number	Enter the port number of the source IP address. Note that 0 means all that ports are allowed.
Destination IP Address	Enter the destination IP address that you wish to deny access to your system.
Subnet Mask	Enter the subnet mask of the destination IP address.
Port Number	Enter the port number of the destination IP address. Note that 0 means that all ports are allowed.
Protocol	Select the protocol to filter.
For MAC filter Only	
MAC Address	Enter the MAC address you wish to deny access to your system
Rule Unmatched	Select what happens to the data in question if the rule you are currently editing is unmatched. Next means that the data is then compared to the next IP/MAC filter rule. Forward means that the data will be allowed into your system. Note that a Forward rule should be the last rule, as no data will be compared to rules after a Forward rule.
IP/MAC Filter Set Index	Select the IP/MAC filter set you wish to view.

When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set or CANCEL to exit without saving.

6.2.2 Assigning Application Filter

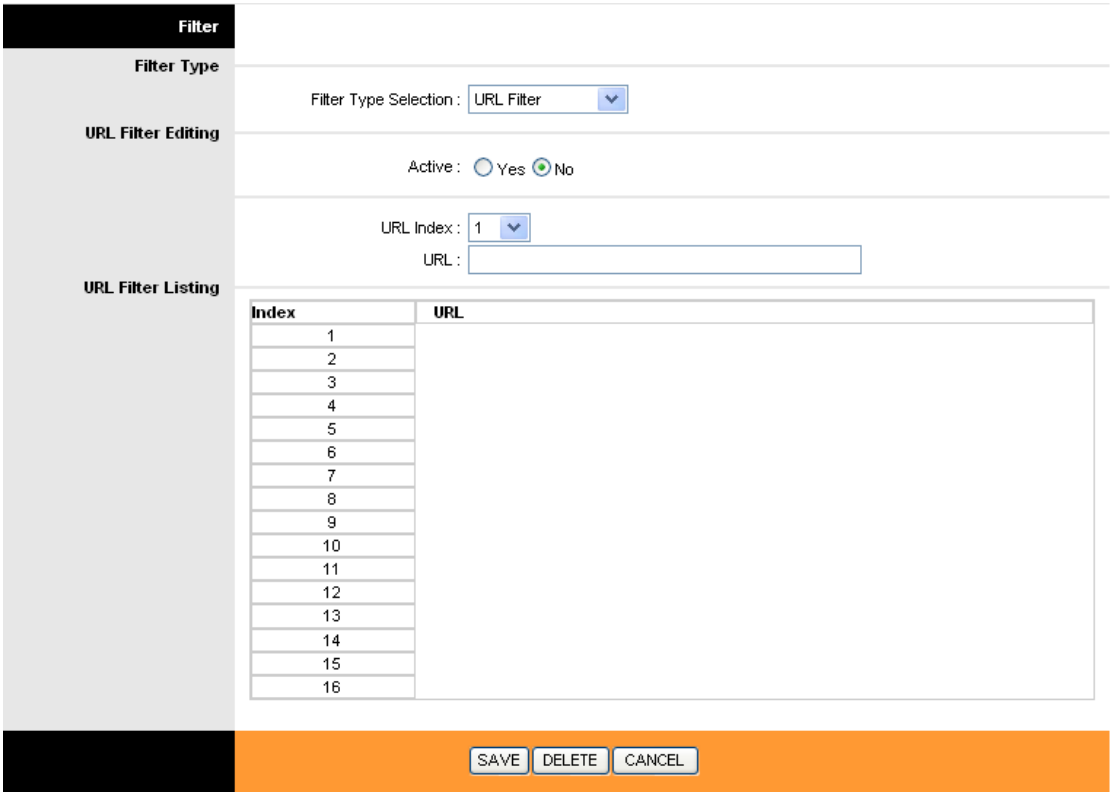


The following table describes the labels in this screen.

LABEL	DESCRIPTION
Application Filter	Select Application Filter is activated or deactivated.
ICQ	Select allow or deny ICQ traffic.
MSN	Select allow or deny MSN traffic.
YMSG	Select allow or deny Yahoo Messenger traffic.
Real Audi/Video	Select allow or deny Real Audio/Video traffic.

When you are done making changes, click on SAVE to save your changes or CANCEL to exit without saving.

6.2.3 Assigning URL Filter



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Active	Toggle the rule on or off with Yes or No, respectively.
URL Index	Select the URL Rule Index you wish to modify .
URL	Enter the URL you wish to deny access to your system .

When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set or CANCEL to exit without saving.

6.3 The SNMP Screen

Simple Network Management Protocol (SNMP) is a protocol for exchanging management information between network devices, and is part of the TCP/IP protocol suite.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Get Community	Enter the password for incoming Get- and GetNext requests from the management station.
Set Community	Enter the password for incoming Set requests from the management station.

The default password is ‘public’. When you are done making changes, click on SAVE to save your changes.

6.4 The UPnP Screen

Universal Plug and Play (UPnP) is an open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. A device can leave a network smoothly and automatically when it is no longer in use.

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (in Windows XP). Each UPnP-compatible device that is installed on your network will appear as a separate icon.

6.4.1.1 NAT Traversal

UPnP NAT traversal automates allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and

UPnP.

6.4.1.2 Cautions with UPnP

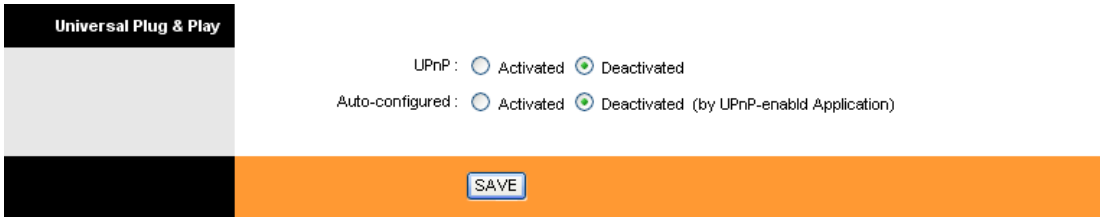
The automated nature of NAT traversal applications in establishing their own services may present network security issues. Network information and configuration may be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if you don't want this to occur.

UPnP broadcasts are only allowed on the LAN.

See later sections for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

6.4.1.3 Configuring UpnP



The following table describes the labels in this screen.

LABEL	DESCRIPTION
UPnP	UPnP can be toggled Activated or Deactivated.
Auto-configured	Auto-configuration can be toggled Activated or Deactivated (by Enabled-enabled Application).

Auto-configuration allows UPnP-enabled applications to automatically configure the DSL-2140/2140W so that they can communicate through; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

When you are done making changes, click on SAVE to save your changes.

6.4.2 Installing UPnP in Windows

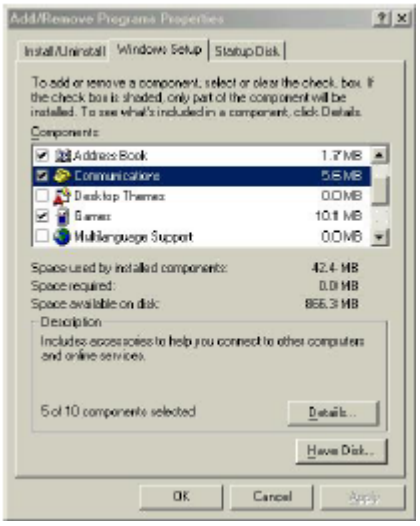
This section shows how to install UPnP in Windows Me and Windows XP.

6.4.2.1 Installing UPnP in Windows Me

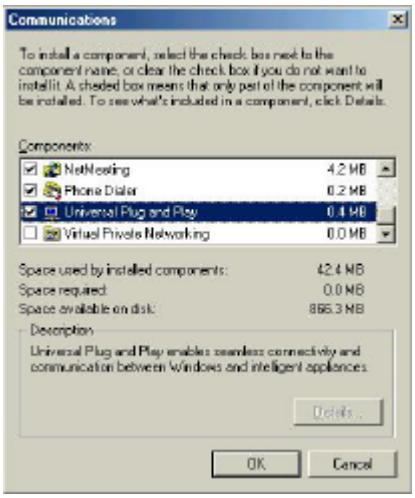
Follow the steps below to install the UPnP in Windows Me.

Step 1. Click on Start and then on Control Panel. Double-click Add/Remove Programs.

Step 2. Click on the Windows Setup tab and select Communication in the Components selection box. Click on Details...



Step 3. In the Communications window, check the Universal Plug and Play box in the Components selection box.



Step 4. Click on OK to go back to the Add/Remove Programs Properties window and click on Next.

Step 5. Restart the computer when prompted.

6.4.2.2 Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

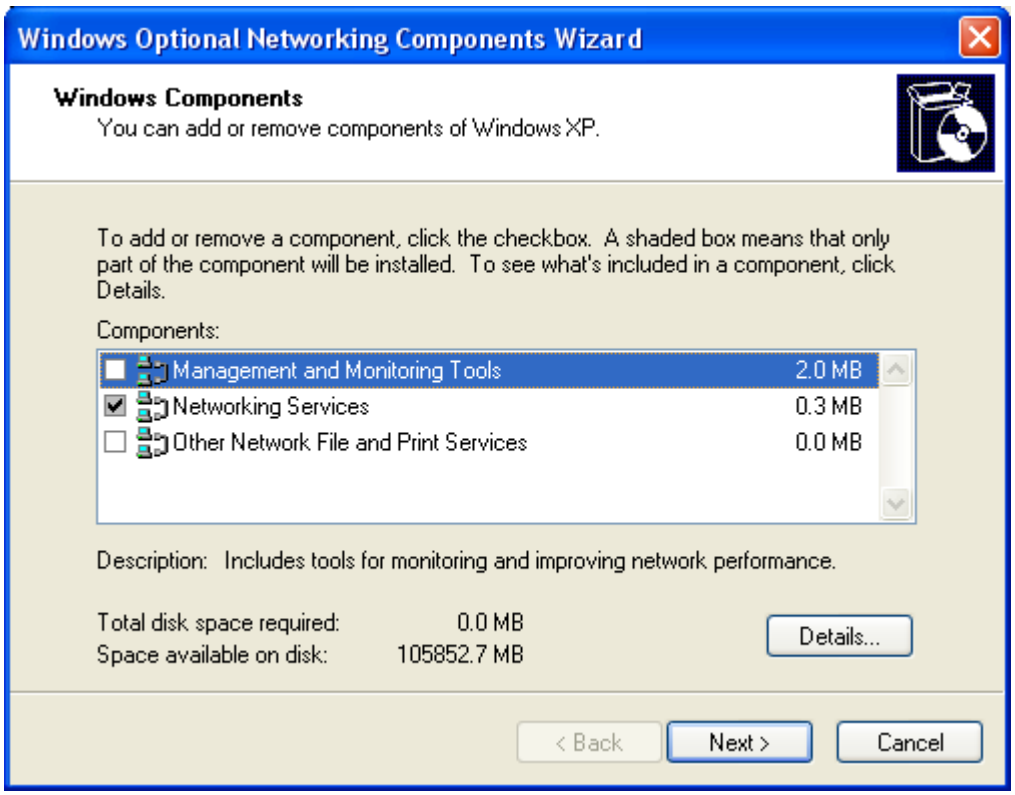
Step 1. Click on Start and then on Control Panel.

Step 2. Double-click on Network Connections.

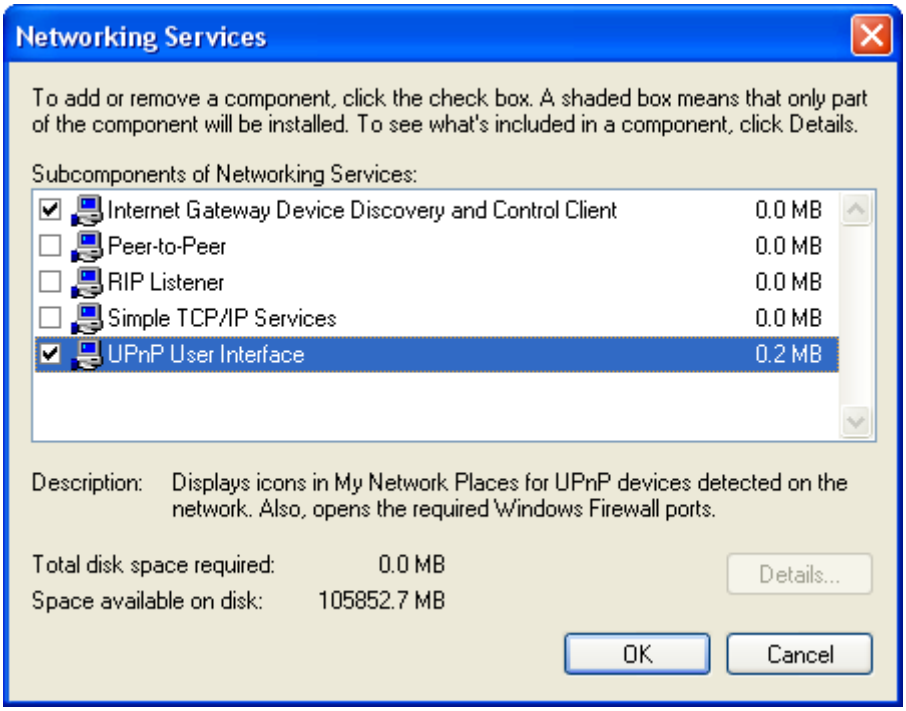
Step 3. In the Network Connections window, click on Advanced in the main menu and select Optional Networking Components...

The Windows Optional Networking Components Wizard window displays.

Step 4. Select Networking Service in the Components selection box and click on Details.



Step 5. Select Networking Services then click on the Details… button. In the window that opens, check the Universal Plug and Play box.



Step 6. Click on OK to go back to the Windows Optional Networking Component Wizard window and click on Next.

Using UPnP in Windows XP Example

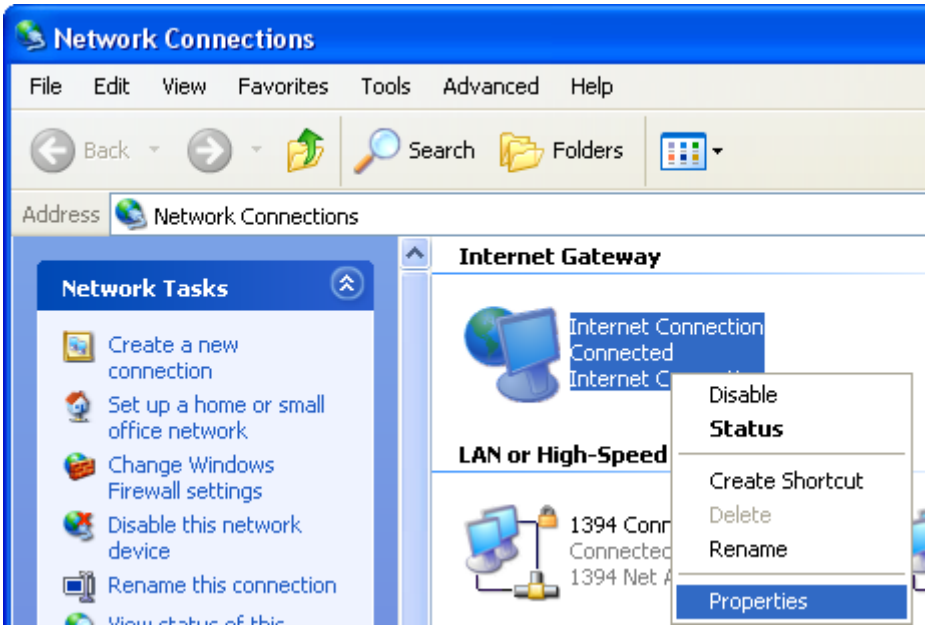
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the DSL-2140/2140W.

Make sure the computer is connected to a LAN port of the DSL-2140/2140W. Turn on your computer and the DSL-2140/2140W.

Auto-discover Your UPnP-enabled Network Device

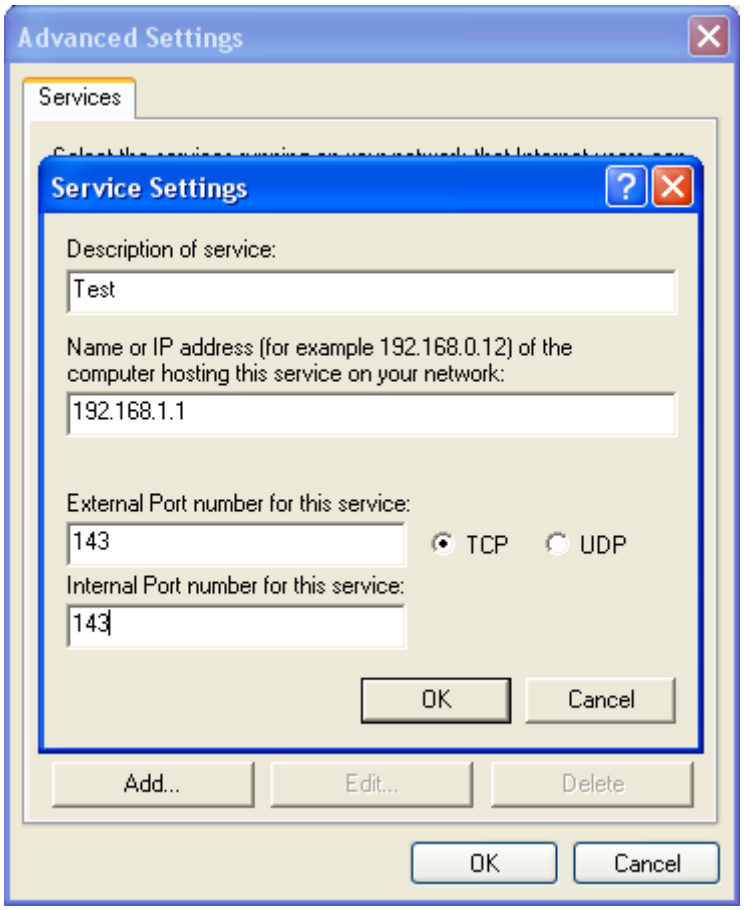
Step 1. Click on *start* and then on Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

Step 2. Right-click on the icon and select Properties.

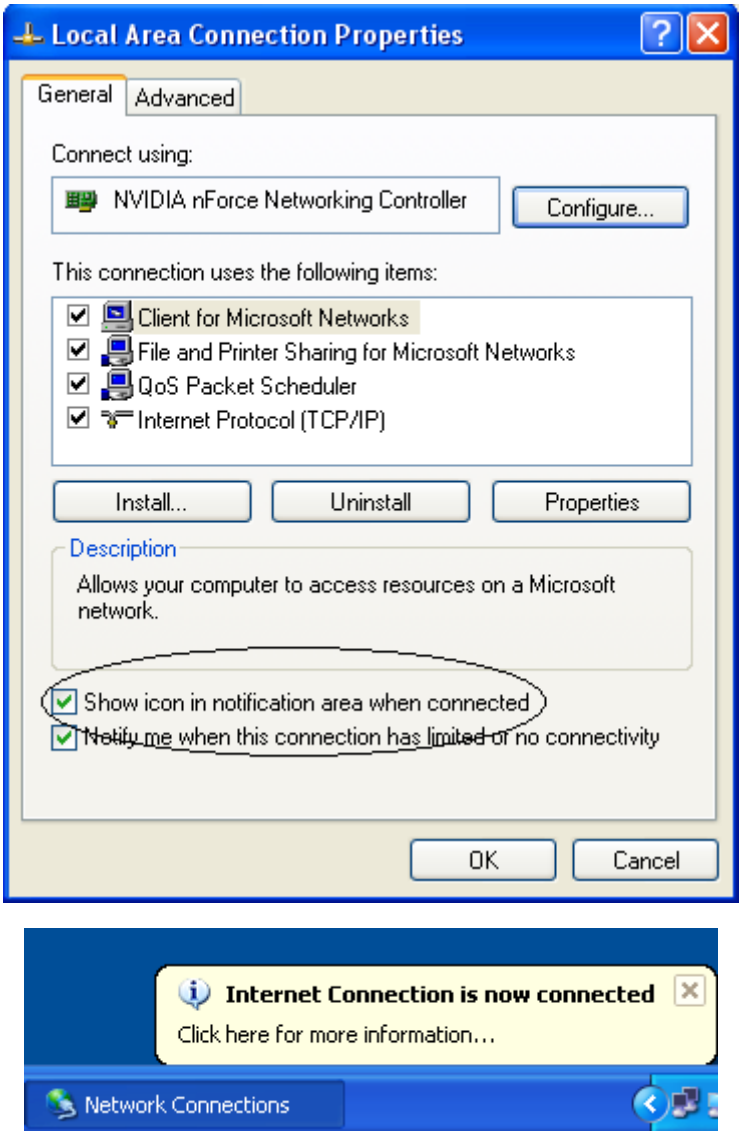


Step 3. In the Internet Connection Properties window, click on Settings to see the port mappings there were automatically created.

Step 4. You may edit or delete the port mappings or click on Add to manually add port mappings.



Step 5. Check the 'Show icon in notification area when connected' box and click on OK. An icon displays in the system tray.



Step 6. Double-click on the icon to display your current Internet connection status.

6.4.2.3 Web Configurator Easy Access

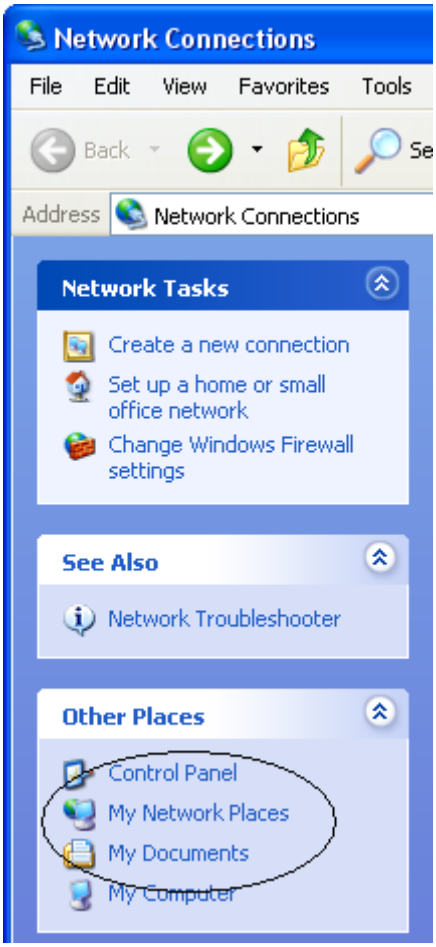
With UPnP, you can access the Web-based configurator on the DSL-2140/2140W without knowing the IP address of the DSL-2140/2140W.

Follow the steps below to access the Web configurator.

Step 1. Click Start and then Control Panel.

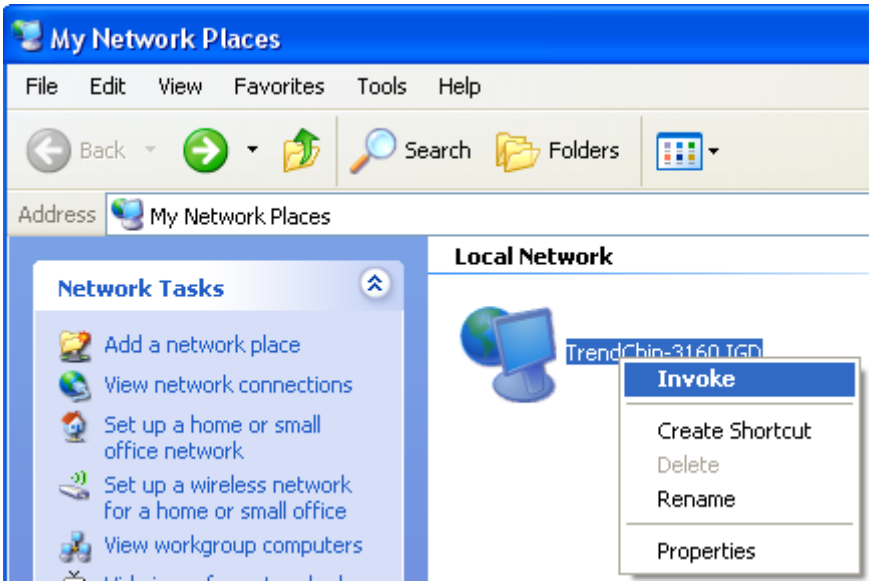
Step 2. Double-click Network Connections.

Step 3. Select My Network Places under Other Places.



Step 4. An icon with the description for each UPnP-enabled device displays under Local Network.

Step 5. Right-click on the icon for your DSL-2140/2140W and select Invoke. The Web configurator login screen displays.



Step 6. Right-click on the icon for your DSL-2140/2140W and select Properties. A properties window displays with basic information about the DSL-2140/2140W.

6.5 Dynamic DNS

Dynamic DNS (DDNS) allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you through various applications. You can also access your FTP server or Web site on your own computer using a DNS-like address that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

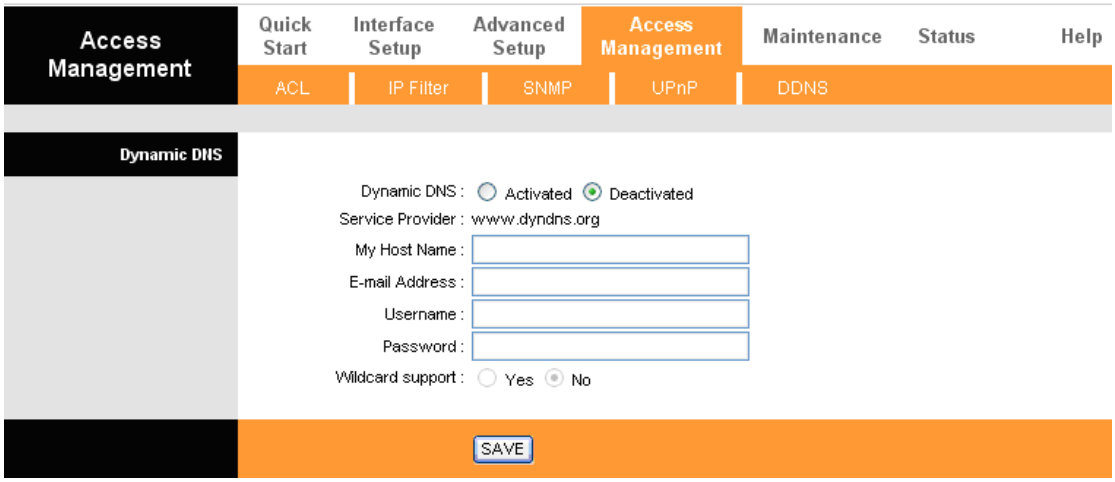
You need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name. The Dynamic DNS service provider will give you a password or key.

6.5.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

6.5.2 Configuring Dynamic DNS

To change your DSL-2140/2140W's DDNS, click on DDNS. The screen appears as shown.



The following table describes the labels in this screen.

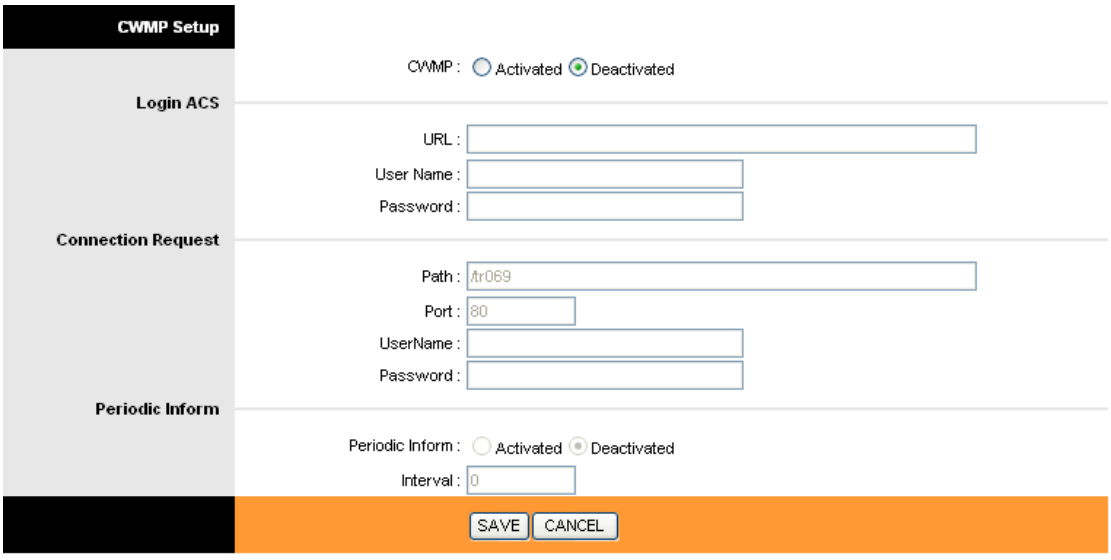
LABEL	DESCRIPTION
Active	Dynamic DNS can be toggled Activated or Deactivated.

Service Provider	Select the name of your Dynamic DNS service provider.
My Host Name	Enter the domain name assigned to your DSL-2140/2140W by your Dynamic DNS provider here.
E-mail Address	Enter your e-mail address here.
Username	Enter your user name here.
Password	Enter the password assigned to you here.
Wildcard support	Choose whether or not you have DYNDNS Wildcard.

Note that you must enter the user name exactly as your ISP assigned it. If the assigned name is in the form of user@domain where domain identifies a service name, enter it exactly as given. When you are done making changes, click on SAVE to save your changes.

6.6 CWMP

CWMP (CPE WAN Management Protocol), defined by DSL forum as TR-069, is a protocol used for “auto-configured complex services” between ACS (Auto-Configuration Server) and CPE.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
CWMP	CWMP can be toggled Activated or Deactivated.
URL	Enter the URL of ACS
User Name	Enter the username used to authenticate the CPE when login ACS.
Password	Enter the password used to authenticate the CPE when login ACS.
Path	Path used for Connection Request.
Port	Port used for Connection Request.

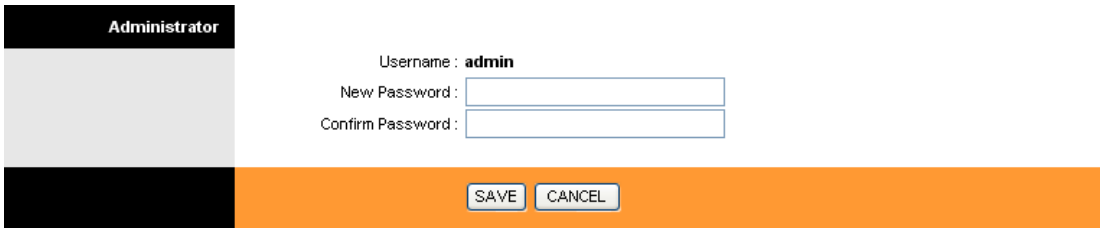
User Name	Enter the username used to authenticate an ACS making a Connection Request to the CPE.
Password	Enter the password used to authenticate an ACS making a Connection Request to the CPE.
Periodic Inform	Whether or not the CPE must periodically send CPE information to ACS using the inform method call.
Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the inform method if Periodic Inform is activated.

Chapter 7 - The Maintenance Screens

The maintenance screens help you manage your DSL-2140/2140W.

7.1 The Administration Screen

Use the Administration screen to change your password. If you used the Quick Start wizard, you have already changed your password once.

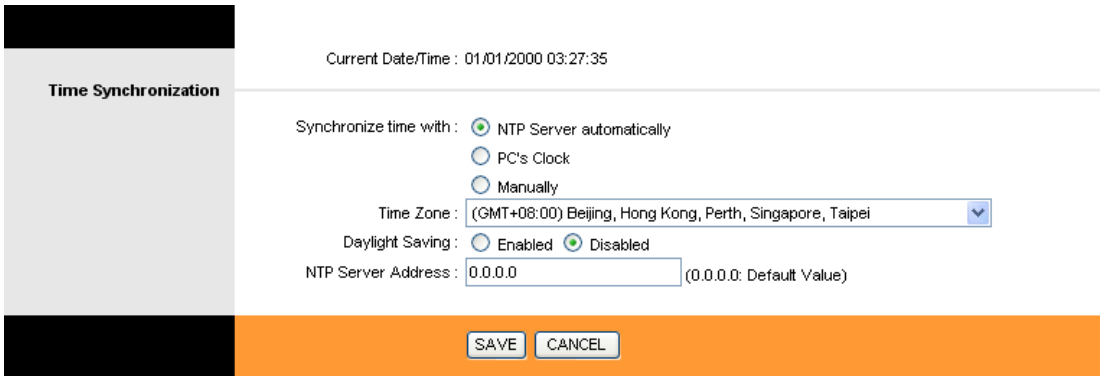


The following table describes the labels in this screen.

LABEL	DESCRIPTION
New Password	Enter the password you wish to use here.
Confirm Password	Enter the password again to confirm it.

7.2 The Time Zone Screen

Use the Time Zone screen to change your DSL-2140/2140W's time and date.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Synchronize time with	Chose how you want your DSL-2140/2140W to obtain the time.
Time Zone	Select your time zone from the dropdown list.

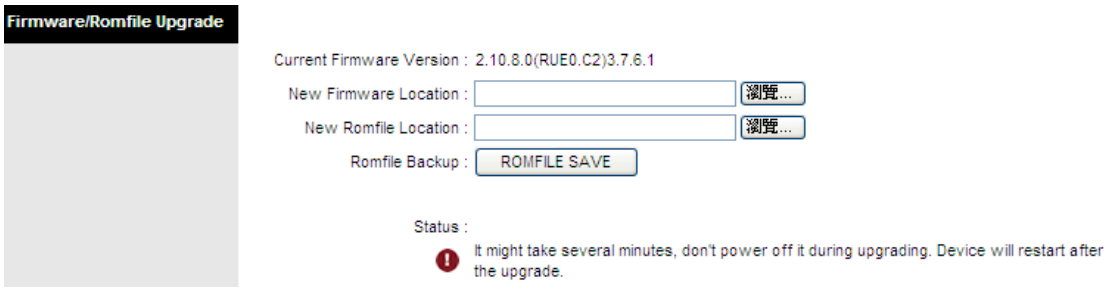
Daylight Saving	Daylight saving can be toggled Enabled or Disabled.
NTP Server Address	Enter the NTP server address you wish to use here.

A Network Time Protocol (NTP) server can automatically set the DSL-2140/2140W's time for you. If you use an NTP server, you will only need to select your time zone. If you manually set the time, you can enable Daylight Saving. The DSL-2140/2140W will automatically adjust when Daylight Saving goes into effect.

When you are done making changes, click on SAVE to save your changes or on CANCEL to exit without saving.

7.3 The Firmware Screen

Use the Firmware screen to view and update your DSL-2140/2140W's firmware. The Firmware screen provides a different way to update the firmware than those given in Chapter 2.



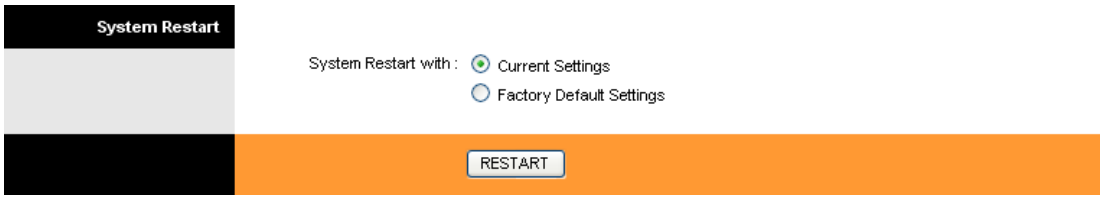
The following table describes the labels in this screen.

LABEL	DESCRIPTION
Current Firmware Ver	The current firmware version your DSL-2140/2140W is using.
New Firmware Location	The location on your computer of the firmware you wish to upload. Enter the location here, or click on Browse… to find it.
New Romfile Location	The location on your computer of the Romfile you wish to upload. Enter the location here, or click on Browse… to find it.
Romfile Backup	Click on "ROMFILE SAVE" to save Romfile on your computer

Once you have entered the new firmware's location in the field, click on UPGRADE to upload it to your DSL-2140/2140W. Note that upgrading might take several minutes. Do not turn off your DSL-2140/2140W during this time. It will restart automatically after upgrading finishes.

7.4 The SysRestart Screen

The SysRestart screen allows you to restart your DSL-2140/2140W with either its current settings still in place or the factory default settings.



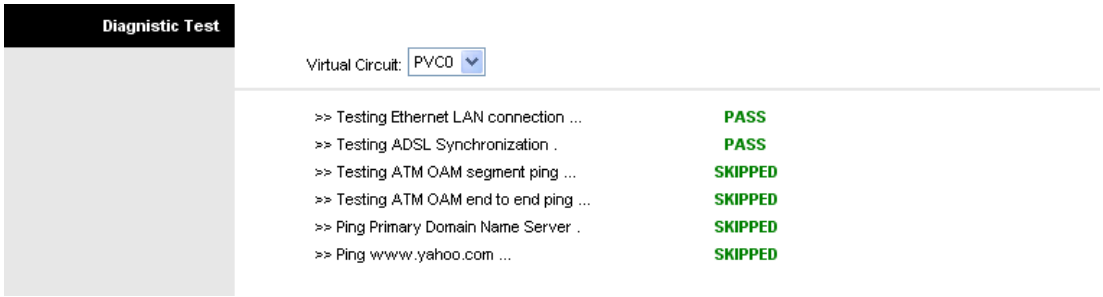
The following table describes the labels in this screen.

LABEL	DESCRIPTION
System Restart with	Select which settings you wish to use once the DSL-2140/2140W has finished restarting.

Once you have selected the settings you wish to use upon restart, click on RESTART to restart the DSL-2140/2140W.

7.5 The Diagnostics Screen

The Diagnostics screen tests the performance of your virtual circuits



Select which PVC you wish to test from the dropdown list. The DSL-2140/2140W will automatically run diagnostic tests on that circuit. A green PASS means that the given test was passed, a red FAIL means that the test was failed and a green SKIPPED means that the test was skipped.

Chapter 8 - The Status Screen

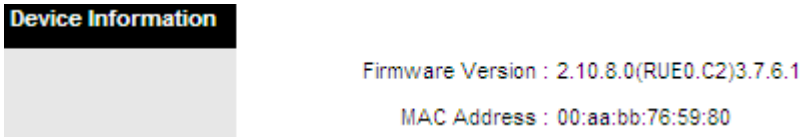
The status screens give you information about various aspects of your DSL-2140/2140W's settings.

8.1 The Device Info Screen

The Device Info screen gives you information about your DSL-2140/2140W's Internet-related settings.

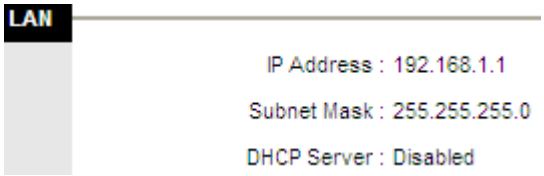
8.1.1 Device Information

The Device Information section tells you the current firmware your DSL-2140/2140W is using and what MAC address it is using.



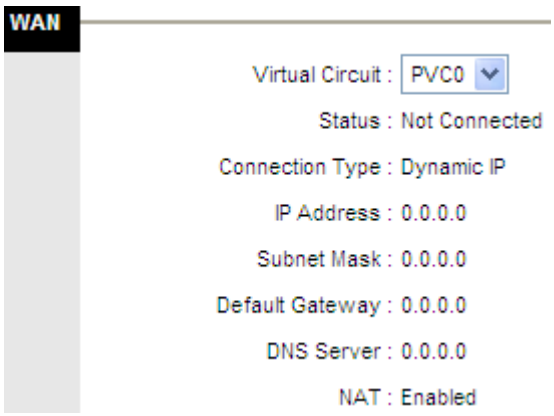
8.1.2 LAN

The LAN section tells you what IP address, subnet mask and DHCP server your DSL-2140/2140W is using.



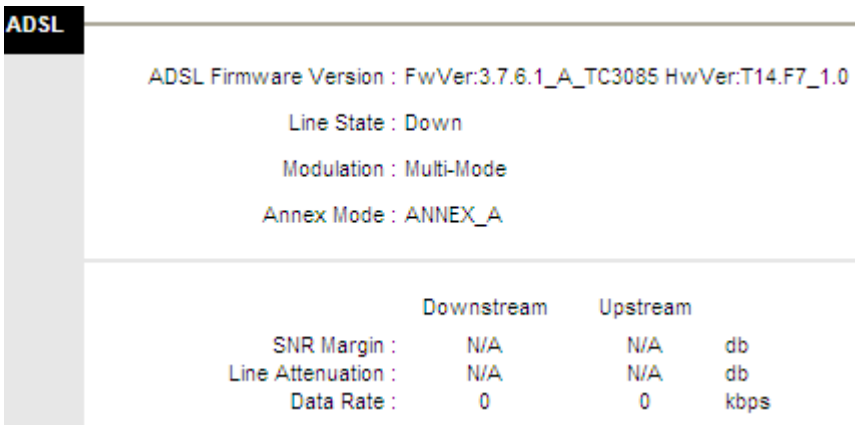
8.1.3 WAN

Select a virtual circuit from the dropdown list. The WAN section tells you the status, connection type, IP address, subnet mask, default gateway, DNS server of the virtual circuit chosen and NAT is in enable state or not.



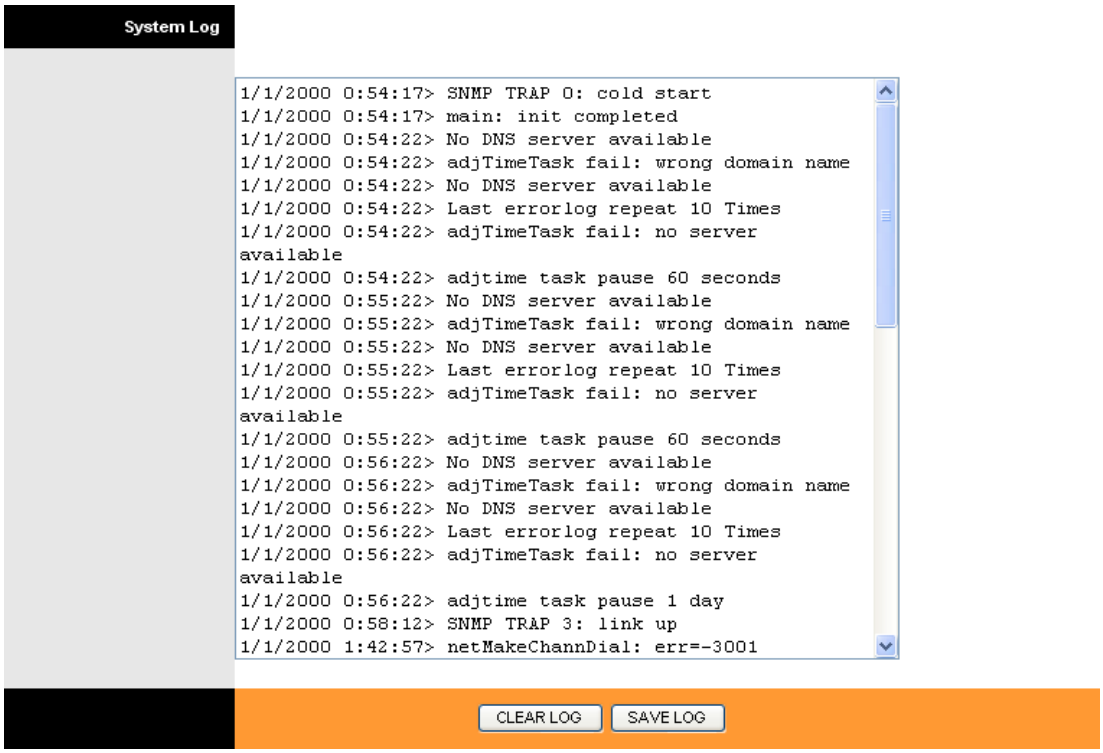
8.1.4 ADSL

The ADSL section tells you what ADSL firmware your DSL-2140/2140W is using, the line state, the modulation type and annex mode as well as the SNR margin, line attenuation and data rate.



8.2 The System Log Screen

The system log screen displays a log of the DSL-2140/2140W's functioning. Click on CLEAR LOG to clear the log or on SAVE LOG, which will save the log data to a separate file.

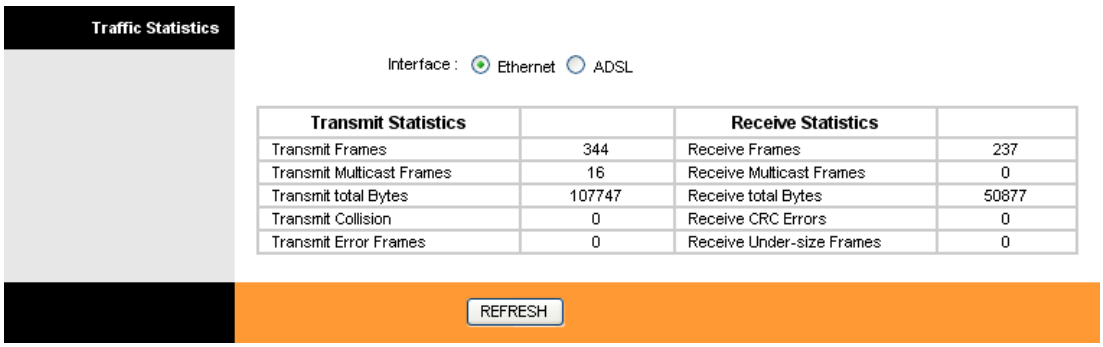


8.3 The Statistics Screen

The statistics screen gives you information on how much data your DSL-2140/2140W has processed. Choose Ethernet or ADSL to view the respective statistics screens.

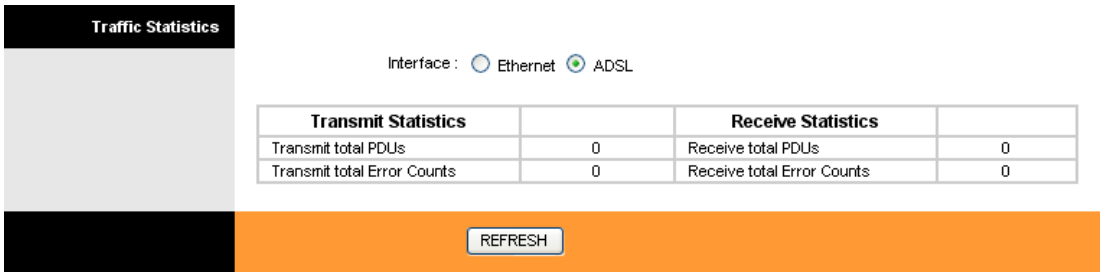
8.3.1 Ethernet

The Ethernet screen gives you information on how much data your DSL-2140/2140W has transmitted and received across the Ethernet connection. Click on REFRESH to update the screen.



8.3.2 ADSL

The ADSL screen gives you information about how much data your DSL-2140/2140W has transmitted or received across the ADSL connection. Click on REFRESH to update the screen.



Appendix - Troubleshooting

This chapter covers potential problems and the corresponding remedies.

A.1 Using LEDs to Diagnose Problems

The Light-Emitting Diodes (LED) are useful aides for finding the possible causes of problems.

A.1.1 Problem: POWER LED Doesn’t Light Up

The Power (PWR) LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Make sure that the DSL-2140/2140W’s power adaptor is connected to the DSL-2140/2140W and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the DSL-2140/2140W and the power source are both turned on and the DSL-2140/2140W is receiving sufficient power.
3	Turn the DSL-2140/2140W off and on.
4	If the error persists, you may have a hardware problem. Contact your vendor.

A.1.2 Problem: ETHERNET LED Doesn’t Light Up

The ETHERENT LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the Ethernet cable connections between your DSL-2140/2140W and the computer or hub.
2	Check for faulty Ethernet cables.
3	Make sure your computer’s Ethernet card is working properly.
4	If the error persists, contact your local distributor for assistance.

A.1.3 Problem: DSL LED Doesn’t Light Up

The DSL LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the telephone wire and connections between the DSL-2140/2140W DSL port and the wall jack.
2	Make sure that the telephone company has checked your phone line and set it up for DSL service.
3	Reset your ADSL line to reinitialize your link to the DSLAM.
4	If the problem persists, contact your local distributor for assistance.

A.2 Problem: Can't Access Through Telnet

I cannot telnet into the DSL-2140/2140W.

STEPS	CORRECTIVE ACTION
1	Check the LAN port and the other Ethernet connections.
2	Make sure you are using the correct IP address of the DSL-2140/2140W. Check the IP address of the DSL-2140/2140W.
3	Ping the DSL-2140/2140W from your computer. If you cannot ping the DSL-2140/2140W, check the IP addresses of the DSL-2140/2140W and your computer. Make sure your computer is set to get a dynamic IP address; or if you want to use a static IP address on your computer, make sure that it is on the same subnet as the DSL-2140/2140W.
4	Make sure you entered the correct password. The default password is "1234". If you forgot your username or password, refer to *Section A.4*.
5	If the problem persists, contact the distributor.

A.3 Problem: Can't Access Web Configurator

I cannot access the Web configurator.

STEPS	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the DSL-2140/2140W. Check the IP address of the DSL-2140/2140W.
2	Make sure that a console session isn't running.
3	Check that you have enabled Web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details.
4	For WAN access, you must configure remote management to allow server access from the WAN (or all).

5	Your computer's and the DSL-2140/2140W's IP addresses must be on the same subnet for LAN access.
6	If you changed the DSL-2140/2140W's LAN IP address, enter the new one as the URL.
7	Remove any filters in LAN or WAN that block Web service.
8	See also *Section A.4*.

The Web configurator does not display properly.

STEPS	CORRECTIVE ACTION
1	Make sure you are using Internet Explorer 5.0 or later versions.
2	Delete the temporary Web files and log in again. In Internet Explorer, click **Tools**, **Internet Options** and then click the **Delete Files ...** button. When a **Delete Files** window displays, select **Delete all offline content** and click **OK**. (Steps may vary depending on the version of your Internet browser.)

A.4 Problem: Forgotten Login Username and Password

I forgot my login username and/or password.

STEPS	CORRECTIVE ACTION
1	If you have changed the password and forgotten it, you will need to upload the default configuration file. This will erase all custom configurations and restore factory defaults, including the password.
2	Press the **RESET** button for five seconds, and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the DSL-2140/2140W restarts. Or refer to the *Resetting the DSL-2140/2140W* section for uploading a configuration file via console port.
3	The default username is "admin". The default password is "1234". The **Password** and **Username** fields are case-sensitive. Make sure that you use the proper casing.
4	It is highly recommended to change the default username and password. Make sure you record the username and password in a save place.

A.5 Problem: Can't Access LAN Interface

I cannot access the DSL-2140/2140W from the LAN or ping any computer on the LAN.

STEPS	CORRECTIVE ACTION
1	Check the Ethernet LEDs on the front panel. A LAN LED should be on if the port is

	connected to a computer or hub. If the 10M/100M LEDs on the front panel are both off, refer to *Section A.1.2*.
2	Make sure that the IP address and the subnet mask of the DSL-2140/2140W and your computer(s) are on the same subnet.

A.6 Problem: Can't Access WAN Interface

Initialization of the ADSL connection failed.

STEPS	CORRECTIVE ACTION
1	Check the cable connections between the ADSL port and the wall jack. The DSL LED on the front panel of the DSL-2140/2140W should be on.
2	Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as that you obtained from your telephone company and ISP.
3	Restart the DSL-2140/2140W. If you still have problems, you may need to verify your VPI, VCI, type of encapsulation and type of multiplexing settings with the telephone company and ISP.

I cannot get a WAN IP address from the ISP.

STEPS	CORRECTIVE ACTION
1	The ISP provides the WAN IP address after authenticating you. Authentication may be through the username and password, the MAC address or the host name.
2	The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing).

A.7 Problem: Can't Access the Internet

I cannot access the Internet.

STEPS	CORRECTIVE ACTION
1	Make sure the DSL-2140/2140W is turned on and connected to the network.
2	If the DSL LED is off, refer to *Section A.1.3*.
3	Verify your WAN settings.
4	Make sure you entered the correct username and password.
5	For wireless stations, check that both the DSL-2140/2140W and wireless station(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).

Internet connection disconnects.

STEPS	CORRECTIVE ACTION
1	Check the schedule rules.
2	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting.
3	Contact your ISP.

A.8 Problem: Can't Access Remote Management

I cannot remotely manage the DSL-2140/2140W from the LAN or WAN.

STEPS	CORRECTIVE ACTION
1	Refer to the *Remote Management Limitations* section in the *Firmware and Configuration File Management* chapter for scenarios when remote management may not be possible.
2	Use the DSL-2140/2140W's WAN IP address when configuring from the WAN. Use the DSL-2140/2140W's LAN IP address when configuring from the LAN.
3	Refer to *Section A.5* for instructions on checking your LAN connection. Refer to *Section A.6* for instructions on checking your WAN connection.
4	See also the *Section A.3*.

A.9 Problem: Can't Access Remote Node Connection

I cannot connect to a remote node or ISP.

STEPS	CORRECTIVE ACTION
1	Check the WAN screen to verify that the username and password are entered properly.
2	Verify your login name and password for the remote node.
3	If the problem persists, you may need to verify your login and password with your ISP.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits 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 not 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 of the following measures:
. Reorient or relocate the receiving antenna.
. Increase the separation between the equipment and receiver.
. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
. Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.