USER MANUAL
DVA-G3340S

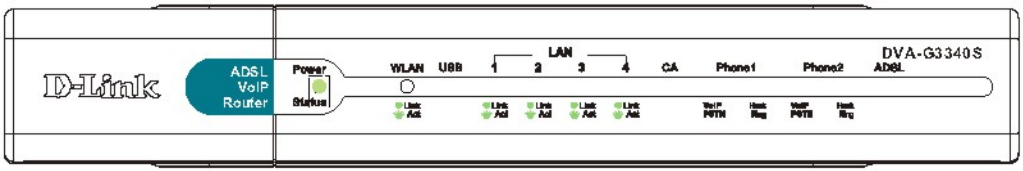
VERSION 1.10

D-Link®

BROADBAND

Contents

Package Contents



Contents of Package:

- D-Link DVA-G3340S High-Speed 2.4GHz Wireless ADSL VoIP Router
- Power Adapter - DC 12V, 1.25A
- Manual and Warranty on CD
- RJ-11 Cable
- Ethernet Cable
- USB Cable

Note: Using a power supply with a different voltage rating than the one included with the DVA-G3340S will cause damage and void the warranty for this product.

If any of the above items are missing, please contact your reseller.

System Requirements for Configuration:

- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0 or Netscape Navigator Version 6.0 and Above

Introduction

The D-Link DVA-G3340S High-Speed Wireless Router is an 802.11g high-performance, wireless router that supports high-speed wireless networking at home, at work or in public places.

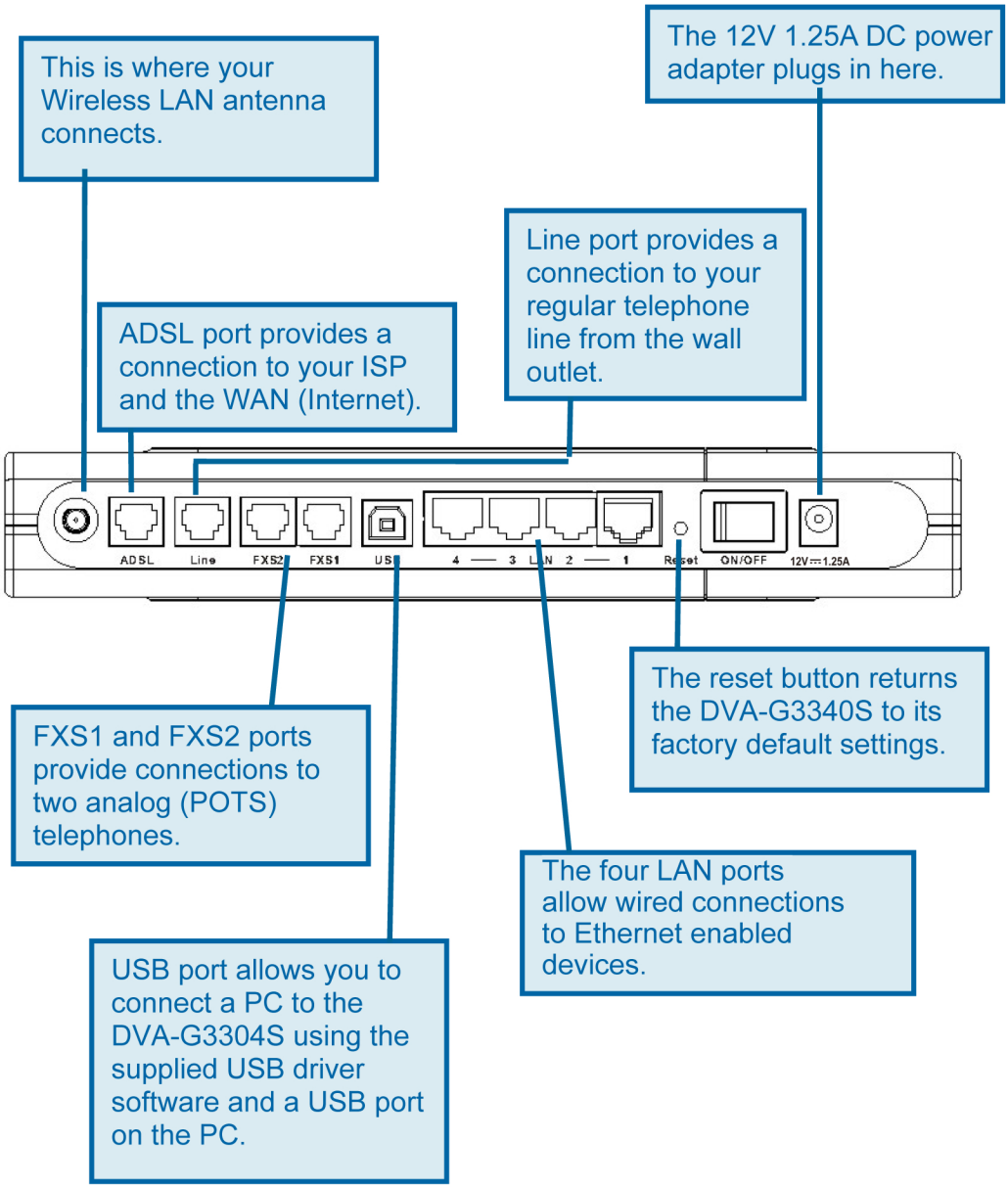
Unlike most routers, the DVA-G3340S provides data transfers at up to 5X (compared to the standard 11 Mbps) when used with other D-Link AirPlus G products. The 802.11 g standard is backwards compatible with 802.11 b products. This means that you do not need to change your entire network to maintain connectivity. You may sacrifice some of 802.11 g's speed when you mix 802.11 b and 802.11 g devices, but you will not lose the ability to communicate when you incorporate the 802.11g standard into your 802.11 b network. You may choose to slowly change your network by gradually replacing the 802.11 b devices with 802.11 g devices.

In addition to offering faster data transfer speeds when used with other 802.11g products, the DVA-G3340S has the newest, strongest, most advanced security features available today. When used with other 802.11 g WPA (WiFi Protected Access) and 802.1x compatible products in a network with a RADIUS server, the security features include:

WPA *Available around Q4/2003 as a free download: Wi-Fi Protected Access authorizes and identifies users based on a secret key that changes automatically at a regular interval. WPA uses TKIP (Temporal Key Integrity Protocol) to change the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security. (By contrast, the older WEP encryption required the keys to be changed manually.)

For home users that will not incorporate a RADIUS server in their network, the security for the DVA-G3340S, used in conjunction with other 802.11g products, will still be much stronger than ever before. Utilizing the Pre Shared Key mode of WPA, the DVA-G3340S will obtain a new security key every time it connects to the 802.11g network. You only need to input your encryption information once in the configuration menu. No longer will you have to manually input a new WEP key frequently to ensure security, with the DVA-G3340S, you can automatically receive a new key every time you connect, vastly increasing the safety of your communications.

Connections

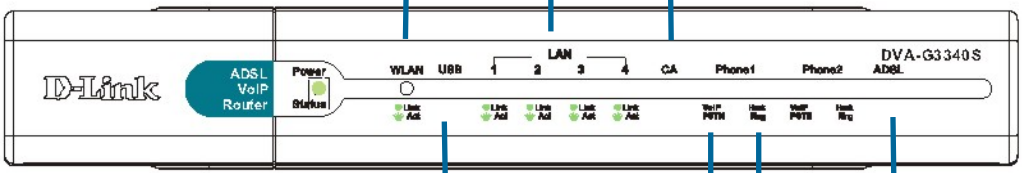


LEDs

LAN – These LEDs will be lit green when a LAN connection is detected. They will blink when there is data activity on the connection.

WLAN – This LED will be lit green when a Wireless LAN connection is detected. It will blink when there is data activity on the connection.

CA (Call Agent) – This LED will blink when you are connected to a VOIP SIP Server.



USB – This LED will light green when a USB connection is detected. It will blink when there is data activity on the connection.

VoIP – LED will light green when you are making a VoIP call.

PSTN (Public Switched Telephone Network) – LED will not be lit when the telephone is making a PSTN telephone call.

Hook LED will light green when the telephone is off the hook.

Ring LED will flash quickly when an incoming call is detected

ADSL – This LED will light green when an ADSL connection is detected. It will blink when there is data activity on the connection.

Features

- Fully compatible with the 802.11g standard to provide a wireless data rate of up to 54Mbps
- Backwards compatible with the 802.11b standard to provide a wireless data rate of up to 11 Mbps
- WPA (WiFi Protected Access) authorizes and identifies users based on a secret key that changes automatically at a regular interval, for example:
    - Pre Shared Key mode means that the home user, without a RADIUS server, will obtain a new security key every time the he or she connects to the network, vastly improving the safety of communications on the network.
- 802.1x Authentication in conjunction with the RADIUS server verifies the identity of would be clients
- Utilizes OFDM technology (Orthogonal Frequency Division Multiplexing)
- User-friendly configuration and diagnostic utilities
- Operates in the 2.4GHz frequency range
- Advanced Firewall features
    - Supports NAT with VPN pass-through, providing added security
    - MAC Filtering
    - IP Filtering
    - URL Filtering
    - Domain Blocking
    - Scheduling
- DHCP server supported enables all networked computers to automatically receive IP addresses
- Web-based interface for Managing and Configuring
- Access Control to manage users on the network
- Supports special applications that require multiple connections
- Equipped with 4 10/100Mbps Ethernet ports, 1 WAN port, Auto MDI/MDIX
- Supports ADSL, ADSL2 and ADSL2+ according to ISP's service.
- ADSL2+ Performance up to 24Mbps downstream and 1Mbps upstream.

Using the Web Interface

Whenever you want to configure your network or the DVA-G3340S, you can access the Configuration Menu by opening the web-browser and typing in the IP Address of the DVA-G3340S. The DVA-G3340S default IP Address is shown below:

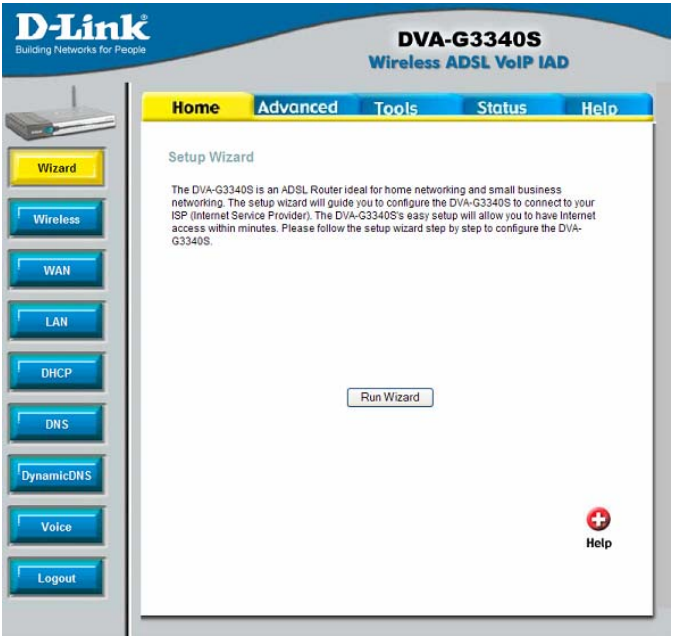
- Open your web browser
- Type in the IP Address of the Router (http://10.1.1.1)

Note: if you have changed the default IP Address assigned to the DVA-G3340S, make sure to enter the correct IP Address.

- Type ***admin*** in the User Name field
- Type ***admin*** in the Password field
- Click OK

Home > Wizard

The Home>Wizard screen will appear. Please refer to the Quick Installation Guide for more information regarding the Setup Wizard.



These buttons appear on most of the configuration screens in this section. Please click on the appropriate button at the bottom of each screen after you have made a configuration change.

Wireless Settings

Home > Wireless

The two essential settings for wireless LAN operation are the SSID and Channel Number. The SSID (Service Set Identifier) is used to identify a group of wireless LAN components. The SSID can be broadcast or can be hidden (not broadcast). Use the Advanced Wireless Settings menu to configure these basic settings. Wireless security using encryption (WEP) or access limitation (WPA) is also configured with the Wireless Settings method. Read more below about setting up security for Wireless LAN.

Wireless Settings menu

Configure Basic Wireless Settings

Follow the instructions below to change basic wireless settings.

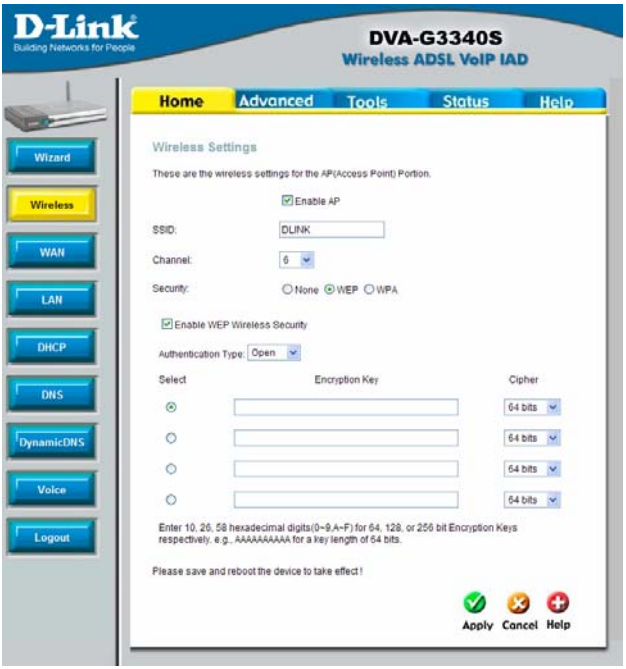
1. **To disable the wireless interface**: click in the **Enable AP** check box to remove the check mark and click the **Apply** button. This will immediately disable the wireless access point, it is not necessary to restart the access point to make this change.
2. **If the wireless interface has been disabled:** click the **Enable AP** check box to place a check mark in it. Click the **Apply** button. It is not necessary to restart the access point unless you have also changed the channel or SSID.
3. The **SSID** can be changed to suit your wireless network. Remember that any wireless device using the access point must have the same SSID and use the same channel. The SSID can be a continuous character string (i.e. no spaces) of up to 16 characters in length. To disable SSID sharing (SSID broadcast), you will need to go to the Advanced > Wireless Performance page. A hidden SSID makes it more difficult for wireless clients to join or leave the SSID as they must be manually configured to join. Click the **Apply** button to save any changes made to the SSID.

4. The **Channel:** may be changed to channels that are available in your region. Channels available for wireless LAN communication are subject to regional and national regulation. Click the **Apply** button to save any change to the Channel.
5. Make sure you save the new wireless settings. Use the Tools > System menu to save the new settings.

Wireless Settings – WEP

Home > Wireless > WEP

The wireless LAN interface of the DVA-G3340S has various security features used to limit access to the device or to encrypt data and shared information. The available standardised security for wireless LAN includes WEP and WPA Wireless security is configured with the **Wireless Settings** menu located in the **Home** directory.



Wireless Security – WEP

Security Options for Wireless

In the Wireless Settings menu, select the type of security you want to configure. The menu will change to present the settings specific to the method being configured. The Router's wireless security options include three levels of WEP encryption and WPA for IEEE 802.1x network authentication or WPA with a user configured Pre Shared Key (PSK).

WEP Encryption

WEP (Wireless Encryption Protocol or Wired Equivalent Privacy) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys. Decryption of the data contained in each packet can only be done if the both the receiver and transmitter have the correct key.

WEP is disabled by default. To enable **WEP**, select the **Enable** option. Configure the Encryption Keys as desired and click the **Apply** button. The encryption key setup is described below.

WEP can use open or shared keys, or may be configured to allow the clients to use either type of key. Use the **Authentication Type:** drop-down menu to choose **Open**, **Shared** or **Both**.

- Select **Open** to allow any wireless station to associate with each other through the access point. Wireless devices will be able to communicate with all devices on a network unless they require a Shared key.
- Select **Shared** to only allow stations using a shared key encryption to associate with each other through the access point. That is, only devices with the same key are allowed to communicate over a network with devices that share the same key. Shared key requires additional configuration of the keys to be used. Follow the instructions below to configure the Shared Keys.
- Select **Both** if you want to allow Wireless clients to specify using a shared or open key.

Setup Encryption Keys

WEP Keys may be configured using **Hex** or **ASCII** characters. In addition there are three levels of encryption available; each level requires a different number of characters. Select **Hex** or **ASCII** from the **Key Type** drop-down menu. Hex or Hexadecimal digits are defined as the numerical digits 0 – 9 and the letters A – F (upper and lower case are recognized as the same digit). ASCII characters include numbers and letters but no spaces. An upper case ASCII character is NOT recognized as the same lower case character, and therefore must be configured exactly as typed for all wireless nodes using the access point. The length of the key depends on the level of encryption used.

Select the **Key Length** from the drop-down menu. The available key lengths are 64, 128 or 256-bit encryption. In the spaces provided type in **Key 1**, **Key 2**, **Key 3** and **Key 4**. The length of the character string used of the keys depends on the level (Key Length) of encryption selected. Only one key can be active. The active key is selected by clicking the radio button for the key you want to use.

Click the **Apply** button when you have configured WEP as desired to put the changes into effect.

Wireless Settings – WPA

Home > Wireless > WPA

WPA security for wireless communication has been developed to overcome some of the shortcomings of WEP. WPA uses an improved encryption method combined with an authentication procedure.

Wireless Security – WPA

Configure WPA Settings

To configure WPA settings, select the **WPA** option. The menu will change to offer the appropriate settings.
WPA can be configured to work with **802.1x** network authentication, or to use a **PSK Hex** or **PSK String** key. Follow the instruction below according to the authentication method used. All the WPA methods require the **Group Key Interval** update. The default is 60 seconds. To change this type in the desired number of seconds to define the time interval between key changes for all WPA clients.
To use WPA with 802.1x:

1. Select the **802.1x** option.
2. Type in the **Server IP Address** field for the RADIUS server used for authentication.
3. Change the **Port:** if necessary, type in the password in the shared **Secret** field and change the **Group Key Interval** as desired.
4. Click the **Apply** button to put the changes into effect. Remember to save the settings using the System Settings menu.

Wireless Settings – WPA-PSK

Home > Wireless > WPA-PSK

WPA-PSK requires a shared key but does not use a separate server for authentication. PSK keys can be ASCII or Hex type.

Wireless Security – WPA-PSK

Configuring WPA-PSK Security for WLAN

To use WPA with a PSK key:

1. Select the **PSK Hex** (Hexadecimal key) or **PSK String** (ASCII key) option.
2. Type in the **Hex: or String:** key in the appropriate entry field.

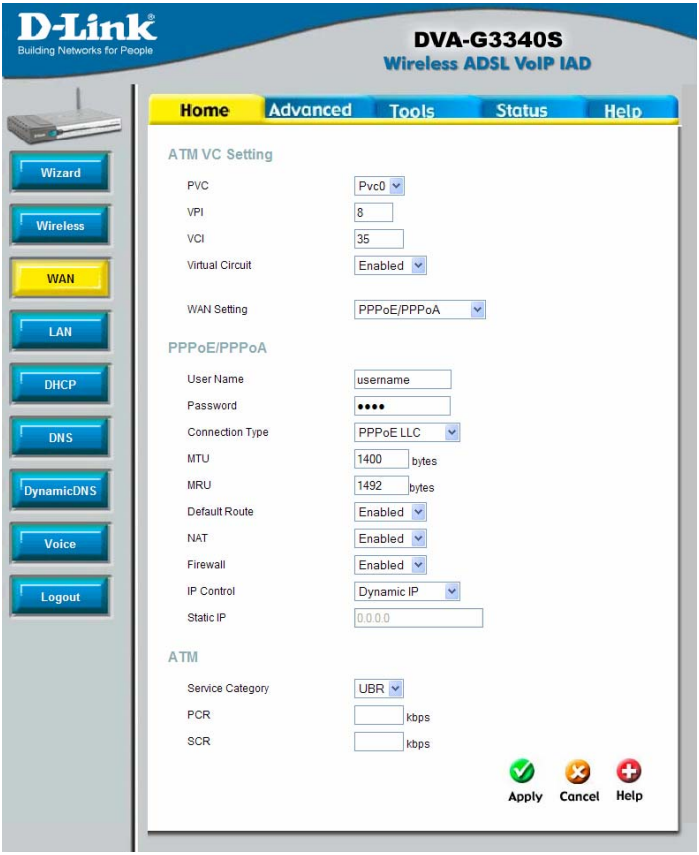
Click the **Apply** button to put the changes into effect. Remember to save the settings using the System Settings menu.

Configuring the WAN Connection

Home > WAN > PPPoE/PPPoA

Please be sure to remove any existing PPPoE client software installed on your computers.

To configure the Router's basic configuration settings without running the Setup Wizard, you can access the menus used to configure WAN, LAN, DHCP and DNS settings directly from the **Home** directory. To access the WAN Settings menu, click on the **WAN** link button on the left side of the first window that appears when you successfully access the web manager. The WAN Settings menu is also used to configure the Router for multiple virtual connections (Multiple PVCs).



WAN Settings Menu – PPPoE / PPPoA

Select the connection type used for your account. The menu will display settings that are appropriate for the connection type you select. Follow the instruction below according to the type of connection you select in the WAN Settings menu.
The new settings must be saved and the Router must be restarted for the settings to go into effect. To save the new settings and restart the Router, click on the **Tools** directory tab and then click the **System** menu button. Click the **Reboot** button under **Force the DVA-G3340S to system restart**. The Router will save the new WAN settings, restart and attempt to establish the WAN connection.

PPPoE and PPPoA Connection for WAN

Follow the instructions below to configure the Router to use a PPPoE or PPPoA for the Internet connection. Make sure you have all the necessary information before you configure the WAN connection.

1. If not already selected, choose the **PPPoE/PPPoA** option from the **WAN Settings** pull-down menu. PPPoE/PPPoA is selected by default if you are configuring the Router for the first time.

2. Under the **ATM VC Settings** at the top of the menu should not be changed unless you have been instructed to change them. However, if you are instructed to change the **VPI** or **VCI** values, type in the values assigned for your account. Leave the **PVC** and **Virtual Circuit** setting at the default (*Pcv0* and *Enabled*) values for now. This can be used later if you are configuring multiple virtual circuits for your ADSL service. For more information on ATM VC Settings, see the table on page 31 below.

3. Under the **PPPoE/PPPoA** heading, type the **User Name** and **Password** used for your ADSL account. A typical User Name will be in the form user1234@isp.com.au, the Password may be assigned to you by your ISP or you may have selected it when you set up the account with your ISP.

4. Choose the **Connection Type** from the pull-down menu located under the User Name and Password entry fields. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are *PPPoA VC-MUX*, *PPPoA LLC* and *PPPoE LLC.* If have not been provided specific information for the Connection Type setting, leave the default setting.

5. Leave the **MTU** value at the default setting (default = 1400) unless you have specific reasons to change this (see table below).

6. Leave the **MRU** value at the default setting (default = 1492) unless you have specific reasons to change this (see table below).

7. Leave the **Default Route** enabled if you want to use the Router as the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the Router becomes the Internet gateway to the computer. If you have an alternative route for Internet traffic you may disable this without effecting the Router's connection.

8. **NAT** should remain enabled. If you disable NAT, you not be able to use more than one computer for Internet connections. NAT is enabled and disabled system-wide, therefore if you are using multiple virtual connections, NAT will disabled on all connections.

9. The **Firewall** should remain enabled for most users. If you choose to disable this

you will not be able to use the features configured in the Firewall and Filters menus located in the Advanced tab. See the next chapter for more details on these menus.

10. Typically the global IP settings (i.e. IP address for the WAN interface) for a PPPoA or PPPoA connection will use Dynamic IP assignment from the ISP. Some accounts may be assigned a specific global IP address. If you have been give an IP address for you PPPoE/PPPoA connection, select the **Static IP** option from the **IP Control** pull-down menu. This menu can be used to configure the WAN port as an Unnumbered IP interface. (See table below for Unnumbered IP)

11. Most users will not need to change **ATM** settings. If this is the first time you are setting up the ADSL connection it is recommended that you leave the **Service Category** settings at the default values until you have established the connection. See the table on page 29 for a description of the parameters available for ATM traffic shaping.

12. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.

13. The new settings must be saved and the Router must be restarted for the settings to take effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **System** menu button. In the System menu, click the **Save & Reboot** button under **Save Settings and Reboot the System**. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

Additional settings for PPPoE/PPPoA connections:

PPPoE/PPPoA Parameters	Description
User Name	For PPP connections, a User Name and Password are used to identify and verify your account to the ISP. Enter the User Name for your ADSL service account. User names and passwords are case-sensitive, so enter this information exactly as given to you by your ISP.
Password	Together with the User Name, this is used to verify your account to the ISP. Enter the Password exactly as given to you by your ISP.
Connection Type	This specifies the protocol (PPPoE or PPPoA) and the encapsulation method (LLC or VC-MUX) used for your connection. The options available are *PPPoE LLC*, *PPPoA LLC* or *PPPoA VC-MUX*.

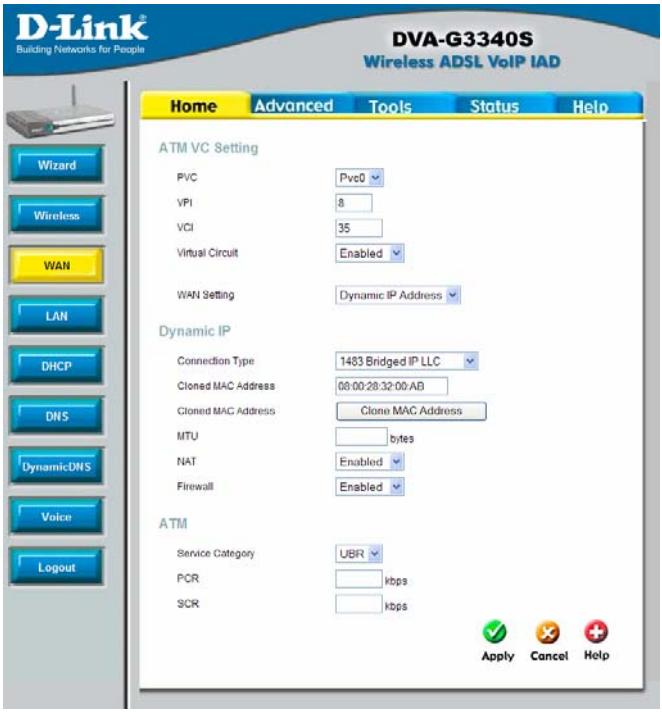
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (1400 bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic for better or worse.
MRU	Similar to the MTU, except this applies to Maximum Received Unit size for downloading data. Most users will be happy with the default setting (1492 bytes). However this may also be optimized for fast downloads of general bulk Internet traffic, for low latency or for downloading to computers on the Wireless LAN. As with the MTU setting, the user should carefully consider how changing the MRU may effect Internet downloads for all systems on your LAN.
Default Route	When this is enabled, the Router will be considered to be the primary gateway to the Internet and WAN for systems on your network. If you are using the Router on a network with one or more alternative gateway routers, you may prefer to disable this if you will use another router as the primary gateway.
NAT	Network Address Translation may be enabled or disabled with the pull-down menu. Keep in mind that disabling NAT allows only a single computer to be used for Internet access through the Router. NAT is enabled for the Router on all connections (i.e. Pvc0 – Pvc7) if your Router is set up for multiple virtual connections.
Firewall	Use this to universally enable or disable the Firewall and Filter features available in the Router. If you disable this you will not be able to configure settings in the Firewall or Filters menus in the Advanced directory.
IP Control	This is used to determine how global IP settings are handled for the WAN interface. Typically PPPoE or PPPoA connections will use the default setting for *Dynamic IP*. Some users will be given a specific IP address for the WAN interface. In this case you need to change this setting to *Static IP*. When Static IP is selected in the IP Control menu, you need to type in

	the global IP address provided to you by your ISP. The *IP Unnumbered* option is used if you want to set up a non-TCP/IP port protocol link through the WAN interface. An IP Unnumbered interface does not have an IP address and therefore cannot be managed via Telnet or any other TCP/IP application.
Static IP	If you have selected the *Static IP* option in the IP Control menu, type in the global IP address used for your WAN interface. This should be given to you by your ISP.

Dynamic IP Address Connection for WAN

Home > WAN > Dynamic IP Address

A Dynamic IP Address connection configures the Router to automatically obtain its global IP address from a DHCP server on the ISP's network. The service provider assigns a global IP address from a pool of addresses available to the service provider. Typically the IP address assigned has a long lease time, so it will likely be the same address each time the Router requests an IP address.
To configure a Dynamic IP Address connection, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose. See the table below for a description of all the settings available in this menu.



WAN Settings for Dynamic IP Address Connection

1. Choose the **Dynamic IP Address** option from the **WAN Settings** pull-down menu.
2. Under the **ATM VC Settings** at the top of the menu should not be changed unless you have been instructed to change them. However, if you are instructed to change the **VPI** or **VCI** values, type in the values assigned for your account. Leave the **PVC** and **Virtual Circuit** setting at the default (*Pcv0* and *Enabled*) values for now. This can be used later if you are configuring multiple virtual circuits for your ADSL service. For more information on ATM VC Settings, see the table on page 31 below.
3. Under the **Dynamic IP** heading, choose the **Connection Type** from the pull-down menu. This defines both the connection type and encapsulation method used for your ADSL service. The available options are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux.* If have not been provided specific information for the Connection Type setting, leave the default setting.
4. Some ISPs record the unique MAC address of your computer's Ethernet

adapter when you first access their network. This can prevent the Router (which has a different MAC address) from being allowed access to the ISPs network (and the Internet). To clone the MAC address of your computer's Ethernet adapter, type in the MAC address in the **Cloned MAC Address** field and click the **Clone MAC Address** button.

5. Leave the **MTU** value at the default setting (default = 1400) unless you have specific reasons to change this (see table below).
6. **NAT** should remain enabled. If you disable NAT, you not be able to use more than one computer for Internet connections. NAT is enabled and disabled system-wide, therefore if you are using multiple virtual connections, NAT will disabled on all connections.
7. The **Firewall** should remain enabled for most users. If you choose to disable this you will not be able to use the features configured in the Firewall and Filters menus located in the Advanced tab. See the next chapter for more details on these menus.
8. Most users will not need to change **ATM** settings. If this is the first time you are setting up the ADSL connection it is recommended that you leave the **Service Category** settings at the default values until you have established the connection. See the table on page 29 for a description of the parameters available for ATM traffic shaping.
9. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
10. The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **System** menu button. In the System menu, click the **Save & Reboot** button under **Save Settings and Reboot the System**. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

Additional settings for Dynamic IP Address connections:

Dynamic IP Parameters	Description
Connection Type	This specifies the connection type and encapsulation method used for your Dynamic IP Address connection. The options available are *Bridged IP LLC* or *Bridged IP VC-MUX*.
Cloned MAC Address	This is not always necessary, but may be required for some ISPs. Type in the MAC address of your computer's Ethernet adapter in the Cloned MAC Address field and click the **Clone MAC Address** button. This will copy the information to a file used by the Router to present to the ISP's server used for DHCP. Some ISPs record the unique MAC address of your computer's Ethernet adapter when you first access their network. If you want to later replace the

	cloned MAC address with the factory default setting, type in all zeros - 0:0:0:0:0:0 - and click the Clone MAC Address button.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (1400 bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic for better or worse.
NAT	Network Address Translation may be enabled or disabled with the pull-down menu. Keep in mind that disabling NAT allows only a single computer to be used for Internet access through the Router. NAT is enabled for the Router on all connections (i.e. Pvc0 – Pvc7) if your Router is set up for multiple virtual connections.
Firewall	Use this to universally enable or disable the Firewall and Filter features available in the Router. If you disable this you will not be able to configure settings in the Firewall or Filters menus in the Advanced directory.

Bridged Connection for WAN

Home > WAN > Bridge Mode

For Bridged connections it will be necessary for most users to install additional software on any computer that will the Router for Internet access. The additional software is used for the purpose of identifying and verifying your account, and then granting Internet access to the computer requesting the connection. The connection software requires the user to enter the User Name and Password for the ISP account. This information is stored on the computer, not in the Router.
Follow the instructions below to configure a Bridged connection for the WAN interface.

WAN Settings Menu – Bridge Mode

To configure a Dynamic IP Address connection, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose. See the table below for a description of all the settings available in this menu.

1. Choose the **Bridge Mode** option from the **WAN Settings** pull-down menu.

2. Under the **ATM VC Settings** at the top of the menu should not be changed unless you have been instructed to change them. However, if you are instructed to change the **VPI** or **VCI** values, type in the values assigned for your account. Leave the **PVC** and **Virtual Circuit** setting at the default (*Pcv0* and *Enabled*) values for now. This can be used later if you are configuring multiple virtual circuits for your ADSL service. For more information on ATM VC Settings, see the table on page 31 below.

3. Under the **Bridge Mode** heading, choose the **Connection Type** from the pull-down menu. This defines both the connection type and encapsulation

method used for your ADSL service. The available options are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux.* If have not been provided specific information for the Connection Type setting, leave the default setting.

4. Most users will not need to change **ATM** settings. If this is the first time you are setting up the ADSL connection it is recommended that you leave the **Service Category** settings at the default values until you have established the connection. See the table on page 29 for a description of the parameters available for ATM traffic shaping.

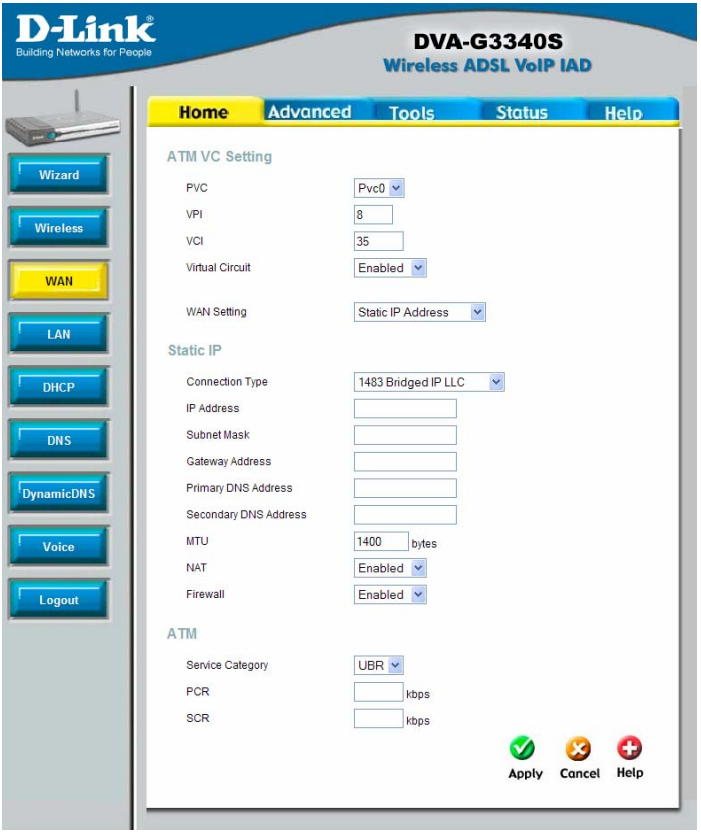
5. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.

6. The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **System** menu button. In the System menu, click the **Save & Reboot** button under **Save Settings and Reboot the System**. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

Static IP Address for Connection WAN

Home > WAN > Static IP Address

When the Router is configured to use Static IP Address assignment for the WAN connection, you must manually assign a global IP Address, Subnet Mask and Gateway IP Address used for the WAN connection. Most users will also need to configure DNS server IP settings in the DNS Settings configuration menu (see below). Follow the instruction below to configure the Router to use Static IP Address assignment for the WAN connection.
To configure a Dynamic IP Address connection, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose. See the table below for a description of all the settings available in this menu.



WAN Settings - Static IP

Additional settings for Static IP Address connections:

Static IP Parameters	Description
Connection Type	This specifies the connection type and the encapsulation method used for your Static IP Address connection. The options available are *Bridged IP LLC*, *Bridged IP VC-MUX*, *Routed IP LLC*, *Routed IP VC-MUX* or *IPoA*.

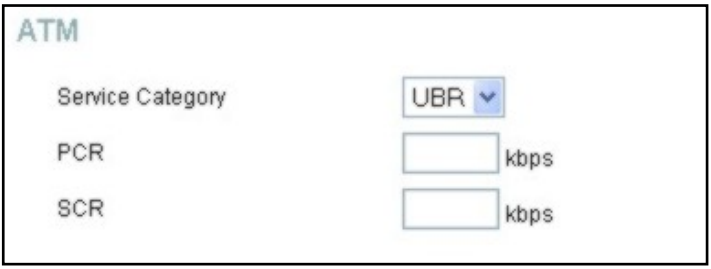
IP Address	This is the permanent global IP address for your account. This is the address that is visible outside your private network. Get this from your ISP.
Subnet Mask	This is the Subnet mask for the WAN interface. Get this from your ISP.
Gateway Address	This is the IP address of your ISP's Gateway router. It provides the connection to the Router for IP routed traffic that is outside your ISP's network. That is, this will be the primary connection from the Router to most of the Internet. Get this IP address from your ISP.
ARP Server Address (for IPoA connection only)	This is not required for all IPoA connections. Check with your ISP for an ARP server IP address if this is necessary for your IPoA connection.
Primary DNS Address	This is the IP address of the first choice for Domain Name Service (DNS) used to match the named URL web address used by most browsers with the actual global IP address used for a web server. Usually this will be a server owned by the ISP. Get this IP address from your ISP.
Secondary DNS Address	This is the second choice for a DNS server. Get this IP address from your ISP.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (1400 bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic for better or worse.
MRU	Similar to the MTU, except this applies to Maximum Received Unit size for downloading data. Most users will be happy with the default setting (1492 bytes). However this may also be optimized for fast downloads of general bulk Internet traffic, for low latency or for downloading to computers on the Wireless LAN. As with the MTU setting, the user should carefully consider how changing the MRU may effect Internet downloads for all systems on your LAN.

Firewall	Use this to universally enable or disable the Firewall and Filter features available in the Router. If you disable this you will not be able to configure settings in the Firewall or Filters menus in the Advanced directory.

ATM Traffic Shaping

Home > WAN > ATM

The ATM settings in the WAN configuration menus for the different connection types can be used to adjust QoS parameters for ADSL clients. This may not be available to all ADSL accounts. Ask your ISP if ATM Traffic Shaping is available for your account.



ATM Settings for WAN connection (PPPoE/PPPoA menu)

Additional ATM settings for PPPoE or PPPoA connections:

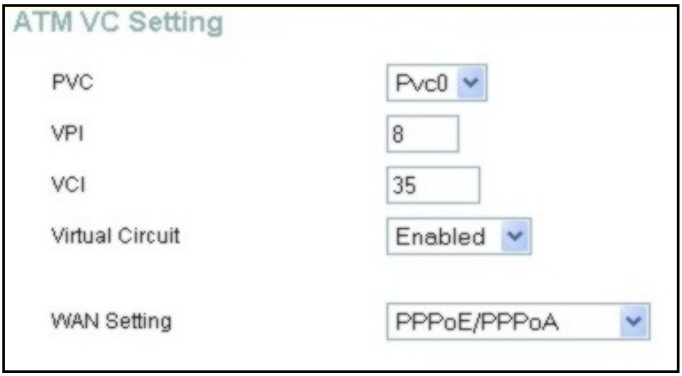
ATM QoS Parameters	Description
Service Category	The ATM settings allow the user to adjust ATM Quality of Service (QoS) or traffic parameters to suit specific traffic requirements. For applications or circumstances where packet loss or packet delays are a concern, ATM QoS can be adjusted to minimize problems. For most accounts, it will not be necessary to change these settings. Altering QoS settings can adversely affect performance of some commonly used Internet applications. If you plan to change QoS or traffic parameters, contact your ISP or network services provider for information on what types of adjustment are available or possible for your account. Your ISP may not support the class of service you want to use. To adjust ATM QoS parameters, select one of the Service Categories listed here and type in the PCR value in the entry field below. For the VBR service category, an additional parameter (SCR) must also be defined. *UBR* – Unspecified Bit Rate, this is the default category used for general-purpose Internet traffic where normal levels of packet loss and delay are acceptable. For some applications or for multiple connection accounts, it may be

	desirable to specify the PCR. *CBR* – Constant Bit Rate, usually used in circumstances where very low packet loss and very low Cell Delay Variable (CDV) are desirable. *VBR* – Variable Bit Rate, usually used when network traffic is characterized by bursts of packets at variable intervals, and some moderate packet loss and delay is acceptable. This category is typically used for audio and video applications such as teleconferencing. The network must support QoS Class 2 to use VBR.
PCR	Peak Cell Rate – The PCR is inversely related to the time interval between ATM cells. It is specified for all three service categories (UBR, CBR and VBR) in Kbps.
SCR	Sustainable Cell Rate – The SCR is defined for the VBR service category. This is the rate that can be sustained for "bursty", on-off traffic sources. It is a function of Maximum Burst Size (MBS) and the time interval (between cells).

ATM VC Settings

Home > WAN > ATM VC Settings

The ATM settings in the WAN configuration menus for the different connection types can be used to adjust QoS parameters for ADSL clients. This may not be available to all ADSL accounts. Ask your ISP if ATM Traffic Shaping is available for your account.



ATM VC Settings in WAN connection menu

The table below describes the ATM VC settings used to configure a connection for an ADSL account.

ATM VC Parameters	Description
PVC	The Router supports using up to eight multiple virtual connections. This menu allows the user to configure WAN settings for all the available connections (see instructions below on how to set up Multiple Virtual Connections). Use the PVC menu to select the connection (Pvc0 to Pvc7) you want to configure. Since most users will use only a single connection, the default setting Pvc0 can be used for any changes made to the WAN settings.
VPI	The Virtual Path Identifier is used with the VCI to define a dedicated circuit on the ATM network portion of the connection to the Internet and WAN. Most users will not need to change this setting.
VCI	The Virtual Channel Identifier is used with the VPI to define a dedicated circuit on the ATM network portion of the connection to the Internet and WAN. Most users will not need to change this setting.
Virtual Circuit	As with the PVC setting, this is mainly for use by clients who are configuring the Router for multiple virtual connections. Use this to enable or disable the PVC you are currently configuring. By default, the Pvc0 is enabled and the remaining PVCs are

	disabled.
WAN Setting	Use this to change the type of connection used. The options are: *PPPoE/PPPoA*, *Dynamic IP Address*, *Static IP Address* and *Bridge Mode*. Each option will offer different settings for configuration.

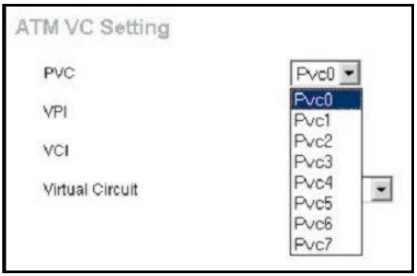
Multiple Virtual Connections

Home > WAN > Multiple PVC Settings

The Router supports multiple virtual connections. Up to eight PVCs to eight separate destinations can be created and operated simultaneously utilizing the same bandwidth. Additional PVC connections can be added for various purposes. For example, you may want to establish a private connection to remote office in order to create an extended LAN, or setup a server on a separate connection. Provisioning for additional PVC profiles must be done through your telecommunications services provider. Extended LAN operations employing multiple virtual connections require ADSL routers or modems at the remote site for a successful connection. Contact your ISP or telecommunications service provider if you are interested in setting up multiple virtual connections.
After the necessary arrangements have been made to use the Router with multiple virtual connections, follow the instructions below to setup the Router using the VPI/VCI settings given to you by your server provider.

Configure Multiple PVCs

Additional PVCs can be configured by first accessing the WAN configuration menu in the Home directory.



Select new PVC to configure in the WAN menu

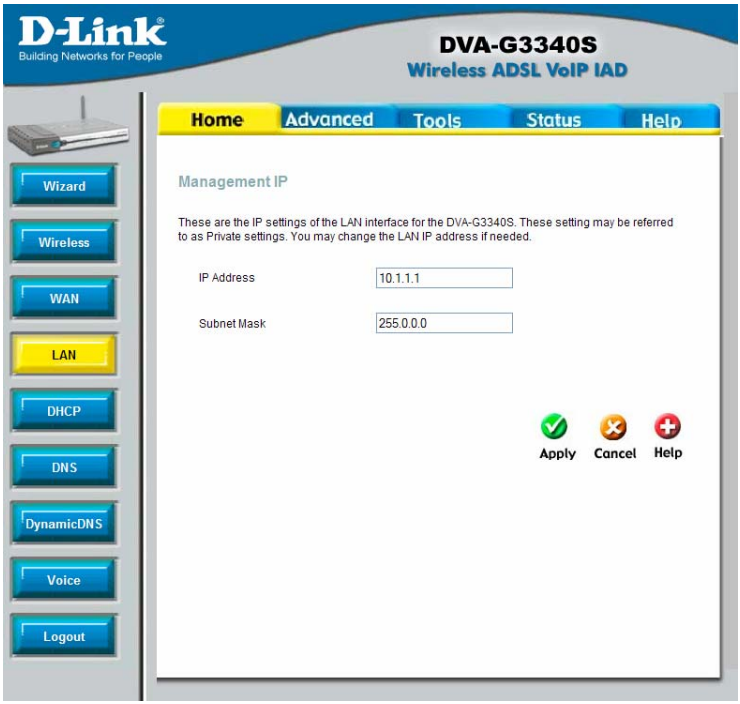
The PVC pull-down menu offers 8 virtual connections available for configuration. The default PVC used by the Router is labelled Pvc0. Any additional connections that are configured must have a VPI/VCI combination that is unique to the Router. These numbers will have been already been established by your service provider on their network.
To add a new virtual connection:

1. Select the new **PVC** to configure from the pull-down menu.
2. Enter the values for the **VPI** and **VCI** given to you by your service provider.
3. To activate the VC, select *Enabled* from the **Virtual Circuit** pull-down menu. Configure the WAN Settings and Connection Type as desired.

LAN IP Settings

Home > LAN

You can configure the LAN IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the Router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the Router. See the next section for information on DHCP setup.



Configure LAN IP settings

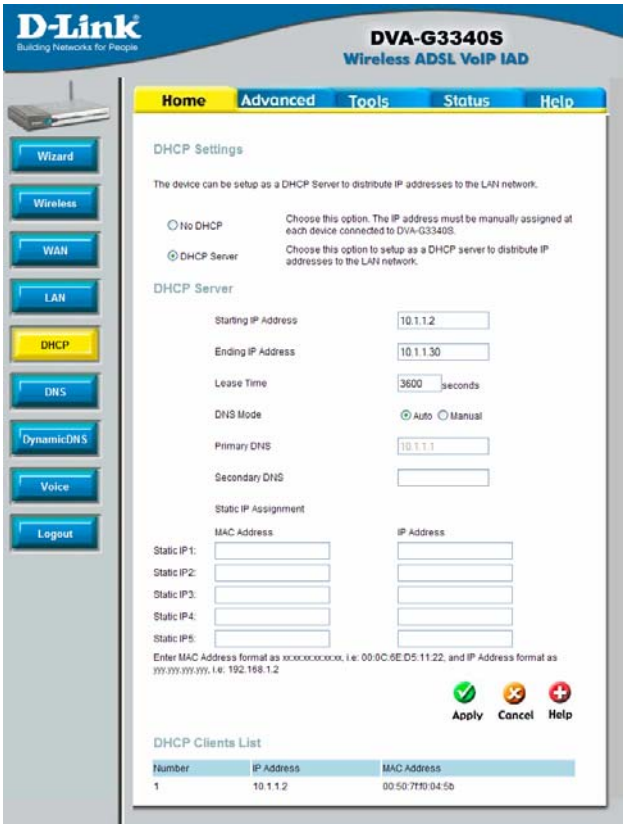
To change the **LAN IP Address** or **LAN Network Mask**, type in the desired values and click the **Apply** button. Your web browser should automatically be redirected to the new IP address. You will asked to login again to the Router's web manager.

DHCP Settings

Home > DHCP

The DHCP server is enabled by default for the Router's Ethernet LAN interface. DHCP service will supply IP settings to workstations configured to automatically obtain IP settings that are connected to the Router though an Ethernet port. When the Router is used for DHCP it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Router the range of IP addresses in the pool used for DHCP on the LAN will also be changed. The IP address pool can be up to 253 IP addresses.

To display the **DHCP Server** menu, click the **DHCP** button in the **Home** directory. Any active DHCP Clients appear listed in the **DHCP Client List** below the configuration menu. The IP address and MAC address for active DHCP clients are displayed in the list.



Configure DHCP server settings for the LAN

The two options for DHCP service are as follows:

- You may use the Router as a DHCP server for your LAN.
- You can disable DHCP service and manually configure IP settings for your workstations.

You may also configure DNS settings for the LAN when using the Router in DHCP mode. In Auto **DNS Mode,** the Router will automatically relay DNS settings to properly configured DHCP clients. To manually enter DNS IP addresses, select the **Manual** DNS Mode option and type in a **Primary** and **Secondary DNS** IP Address in the field provided. The manually configured DNS settings will be supplied to clients that are configured to request them from the Router.

Follow the instructions below according to which of the above DHCP options you want to use. When you have configured the DHCP Settings as you want them, click the **Apply** button to commit the new settings. The new settings must be saved and the

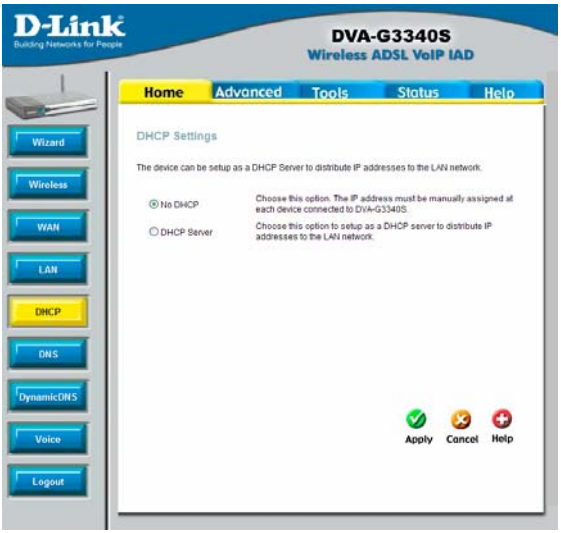
Router must be restarted for the settings to go into effect. To save the new settings and restart the Router, click on the **Tools** directory tab and then click the **System** menu button. Click the **Save & Reboot** button under **Save Settings and Reboot the System**. The Router will save the new DHCP settings and restart.

Use the Router for DHCP

To use the built-in DHCP server, click to select the **DHCP Server** option if it is not already selected. The IP Address Pool settings can be adjusted. The **Starting IP Address** is the lowest available IP address (default = 10.1.1.2). If you change the IP address of the Router this will change automatically to be 1 more that the IP address of the Router. The **Ending IP Address** is the highest IP address number in the pool. Type in the **Lease Time** in the entry field provided. This is the amount of time in seconds that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off.

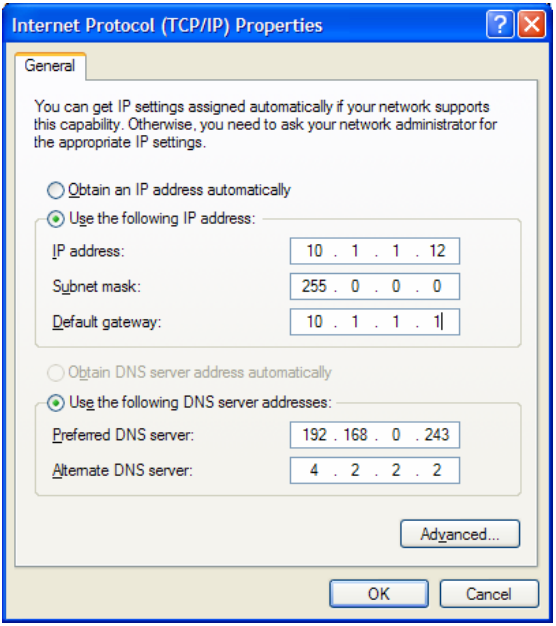
Disabling the DHCP Server

To disable DHCP, click to select the **No DHCP** option and click on the **Apply** button. Choosing this option requires that workstations on the local network must be configured manually or use another DHCP server to obtain IP settings.
If you configure IP settings manually, make sure to use IP addresses in the subnet of the Router. You will need to use the Router's IP address as the Default Gateway for the workstation in order to provide Internet access.



DHCP Settings menu with DHCP disabled

To manually configure IP settings on Windows workstations, open the TCP/IP Properties menu and select the "Use the following IP address" option. You will need to supply the IP address, Subnet mask and Default gateway for each workstation. The example here also uses manually configured DNS settings.



DNS Settings

Home > DNS

The Router can be configured to relay DNS settings from your ISP or another available service to workstations on your LAN. When using DNS relay, the Router will accept DNS requests from hosts on the LAN and forward them to the ISP's, or alternative DNS servers. DNS relay can use auto discovery or the DNS IP address can be manually entered by the user. Alternatively, you may also disable the DNS relay and configure hosts on your LAN to use DNS servers directly. Most users who are using the Router for DHCP service on the LAN and are using DNS servers on the ISP's network, will leave DNS relay enabled (either auto discovery or user configured).

Configure DNS Settings

In the DNS Relay Selection pull-down menu, choose to *Use Auto Discovery*, *Use User Configured* or *Disable* DNS relay.

If you have not been given specific DNS server IP addresses or if the Router is not pre-configured with DNS server information, select the Auto Discover option for DNS relay. Auto discovery DNS instructs the Router to automatically obtain the DNS IP address from the ISP through DHCP. If your WAN connection uses a Static IP address, auto discovery for DNS cannot be used.

If you have DNS IP addresses provided by your ISP, enter these IP addresses in the available entry fields for the **Preferred DNS Server** and the **Alternative DNS Server**.

If you choose to disable DNS relay, it will be necessary to configure DNS settings for hosts on the LAN since they will not be depending on the Router to forward the DNS requests.

When you have configured the DNS settings as desired, click the **Apply** button.

Dynamic DNS Settings

Home > Dynamic DNS

The Router supports DDNS, a service that maps Internet domain names to IP addresses. DDNS serves a similar purpose to DNS in that DDNS allows anyone hosting a Web or FTP server to advertise a public name to prospective users. Unlike DNS that only works with static IP addresses, DDNS works with dynamic IP addresses, such as those assigned by an ISP or other DHCP server.

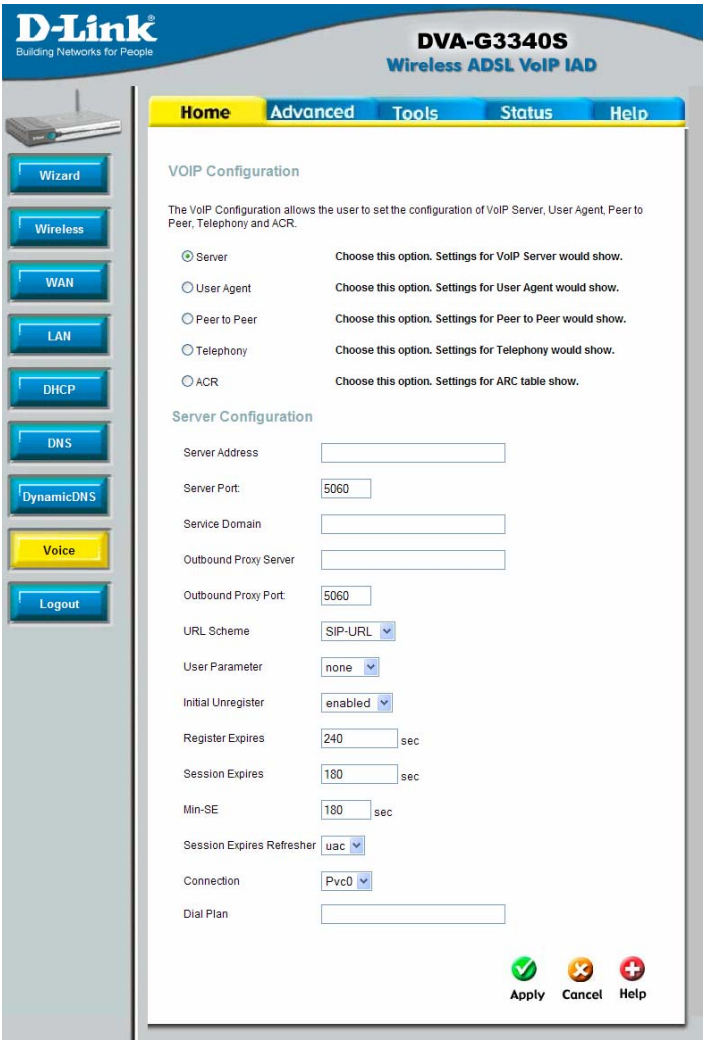
Configure DDNS Settings

DDNS is popular with home networkers, who typically receive dynamic, frequently-changing IP addresses from their service provider. To use DDNS, one simply signs up with a provider and installs network software on their host to monitor its IP address.

VOIP Settings – Server Settings

Home > Voice > Server

The Router can be configured to handle voice signals over the Internet Protocol (Voice Over IP – VOIP).



Configure VOIP Server Settings

The table below describes the VOIP Server settings.

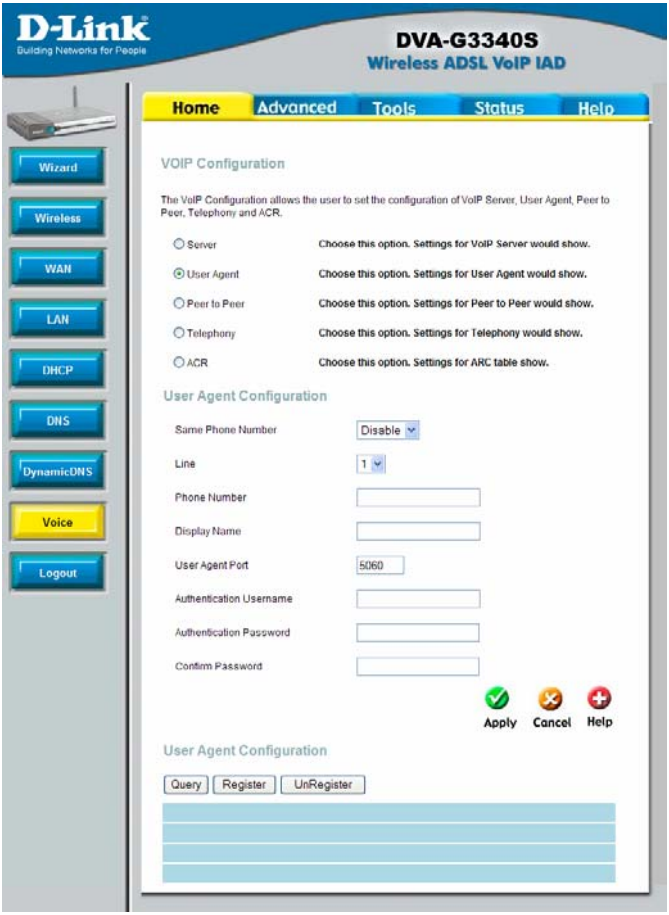
VOIP Server Parameters	Description
Server Address	Enter the IP address of the SIP Server in this field.
Server Port	Enter the SIP server's listening port for the SIP in this field. Leave this field set to the default if your

	VoIP service provider did not give you a server port number for SIP.
Service Domain	Enter the SIP service domain name in this field.
URL Scheme	Select **SIP-URL** to have the router include the domain name with the SIP number in the SIP messages that it sends. Select **TEL-URL** to have the router use the SIP number without a domain name in the SIP messages that it send.
User Parameter	You can set this to **phone** or **none**. This determines whether or not the phone number is appended to the information forwarded to your SIP server. Your VoIP service provider will instruct you which setting to use.
Initial Unregister	You can set this to **enabled** or **disabled**. Some SIP servers can become unstable if you are registered more than once (due to a power outage and subsequent reboot of the router, for example). This setting allows your router to "unregister" itself when it is rebooted, removing the previously sent registration information.
Register Expires	Use this field to set how long the router will wait before sending a repeat registration request if a registration attempt fails or there is no response from the registration server.
Session Expires	This field will set the longest time that the router will allow a SIP session to remain idle (without traffic) before dropping it.
Min-SE	When two SIP devices negotiate a SIP session, they must negotiate a common expiration time for idle SIP sessions. This field sets the shortest expiration time that the router will accept. The router checks the session expiration values of incoming SIP INVITE requests against the minimum session expiration value that you enter here. If the session expiration of an incoming INVITE request is less than this value, the router negotiates with the other SIP device to increase the session expiration value to match the minimum session expiration value.
Session Expires Refresher	This determines which side of an expired call session will initiate the session refresh. **uac** – specifies the Caller side will initiate the session refresh. **uas** – specifies the Call receiver (the "Callee") will initiate the session refresh.

VOIP Settings – User Agent

Home > Voice > User Agent

The Router can be configured to handle voice signals over the Internet Protocol (Voice Over IP – VOIP).



Configure VOIP User Agent Settings

The table below describes the VOIP User Agent settings.

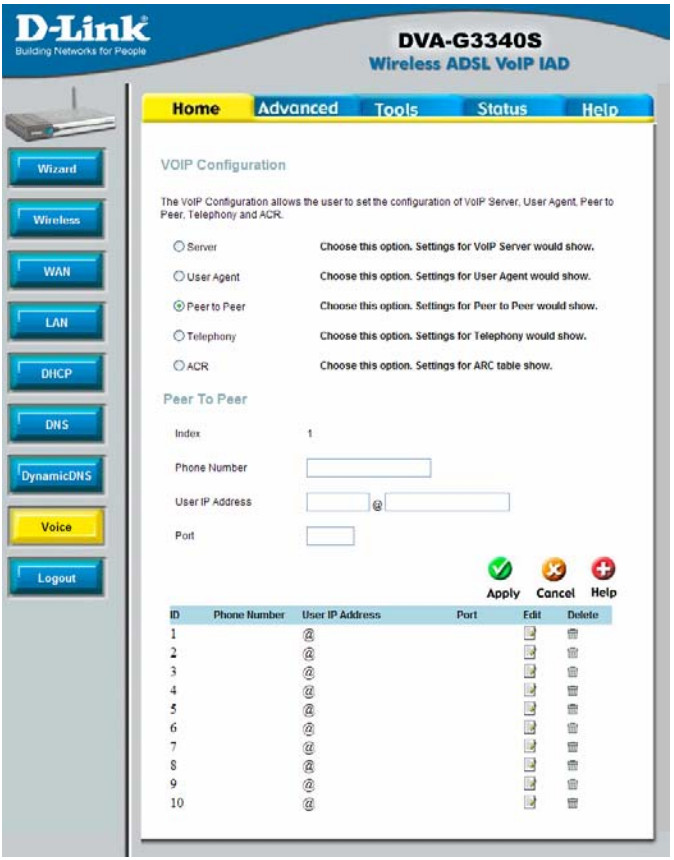
VOIP User Agent Parameters	Description
Same Phone Number	Use this field to **Enable** or **Disable** the use of the same telephone number for the User Agent as for the Server Agent.
Line	Use this field to assign **line 1** or **line 2** telephone sockets (on the back of the router) to the information entered in the User Agent.
Phone Number	The telephone number assigned to the User Agent.

Display Name	The name that will be displayed when the User Agent is in use.
User Agent Port	This selects the port number the router will listen to when determining when calls are being made.
Authentication Username	The Username used to access your SIP server and your VoIP service provider.
Authentication Password	The Password used to access your SIP server and your VoIP service provider.
Confirm Password	Retype your password to confirm.

VOIP Settings – Peer to Peer

Home > Voice > Peer to Peer

The Router can be configured to handle voice signals over the Internet Protocol (Voice Over IP – VOIP).



Configure VOIP Peer to Peer Settings

The table below describes the VOIP Peer to Peer settings.

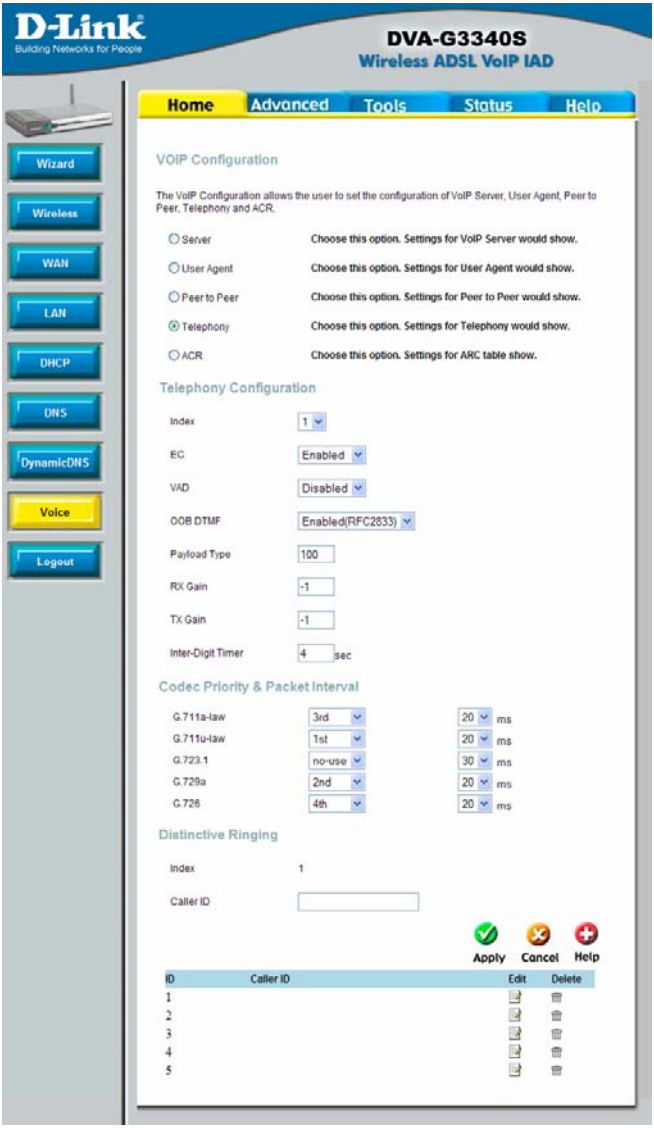
VOIP Peer to Peer Parameters	Description
Index	Index shows you what the current ID is for the rules you are creating in the table.
Phone Number	Allows you to configure the Phone Number that you wish to use to make this call.
User IP Address	Allows you to configure the IP Address of the Phone you are trying to call. You will notice there is a field either side of the "@" this will allow for you to enter the predefined extension of the phone if it has

	one in the first field. The second field is for the IP address of the Phone.
Port	This selects the port number the router will contact when this call is being made.

VOIP Settings – Telephony

Home > Voice > Telephony

The Router can be configured to handle voice signals over the Internet Protocol (Voice Over IP – VOIP).



Configure VOIP Telephony Settings

The table below describes the VOIP Telephony settings.

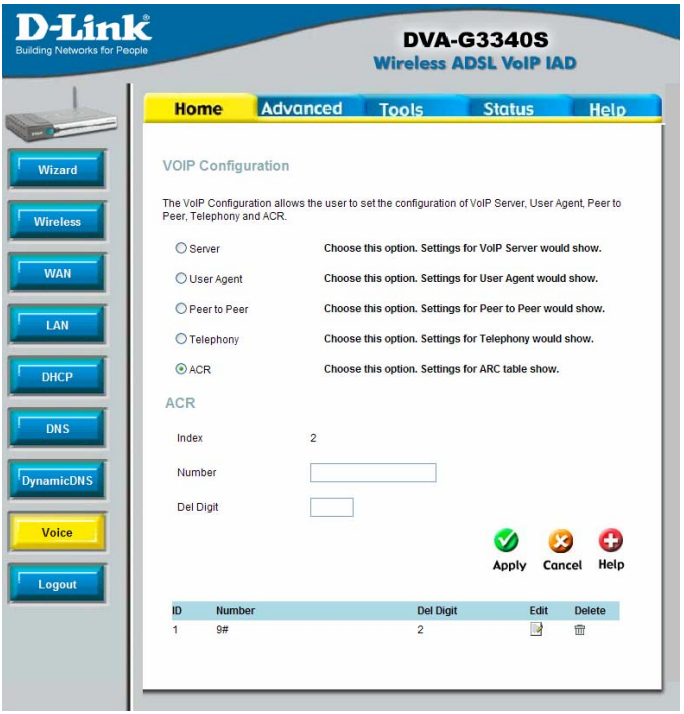
VOIP Telephony Parameters	Description
Index	Index allows you to select the current port you want to configure. This directly relates to the FXS1 or FXS2 ports on the back of the unit.
EC	Echo Cancellation (EC) – G.168 is an ITU standard for eliminating echo. Select **Enabled** to cancel the echo caused by the sound of your voice reverberating in the telephone receiver when you speak.
VAD	Voice Activity Detection (VAD) – detects whether or not speech is present. This lets the router reduce the bandwidth that a call uses by not transmitting "silent Packets" when you are not speaking.
OOB DTMF	Out-of band Dual Tone Multi-frequency – The Dual Tone Multi-frequency (DTMF) mode sets how the router will handle the tones that your telephone makes when you push its buttons. It is recommended that you use the same mode that your VoIP service provider uses. Select **Enabled (RFC 2833)** to send the DTMF tones in RTP packets. Select **Disabled (G.711)** to include the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711).
Payload Type	A Payload Type is a number from 96 through 127 that identifies the type of payload carried in the packet. For example, a payload type of 122 denotes a fax payload. This field is only active when the DTMF method is set to RFC 2833.
RX Gain	Allows you to control the decibel rating of the incoming data.
TX Gain	Allows you to control the decibel rating of the outgoing data.
Inter-Digit Timer	Determines the amount of time that will elapse between sending dialled digits when making a VoIP telephone call.
Codec Priority & Packet Interval	Allows you to configure the order in which the codec's will be used to establish and maintain a call. It is recommended to leave these in their default state unless required to change via VoIP Service Provider. The Packet Interval is used to specify the size of the packet used for the VoIP traffic while used in conjunction with the specific codec. It is not recommended that you change this unless specified via your VoIP Service Provider.

Caller ID	Set a numerical Caller ID of up 32 digits. 5 caller IDs can be created and will be listed below the Distinctive Ringing area. To edit or delete an entry that has already been created, find the entry in the list and click on the appropriate icon.

VOIP Settings – ACR

Home > Voice > ACR

The Router can be configured to handle voice signals over the Internet Protocol (Voice Over IP – VOIP).



Configure VOIP ACR Settings

The table below describes the VOIP Telephony settings.

VOIP ACR Parameters	Description
Index	Index shows you what the current ID is for the rules you are creating in the table.
Number	Allows you to configure a number that is used as a prefix for dialing out to the PSTN.
Del Digit	This feature will remove this amount of prefix digits from the number before dialing.

Advanced Settings

The Advanced tab has many pages of settings for you to view and configure: UPnP, Virtual Server, LAN Clients, SNMP, Filters, Bridge Filters, Routing, DMZ, Firewall, RIP, PPP, ADSL, ATM VCC, Wireless Management, and Wireless Performance.

Universal Plug n Play

Advanced > UPnP

UPnP supports zero-configuration networking and automatic discovery for many types of networked devices. When enabled, it allows other devices that support UPnP to dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS service can also be used if available on the network. UPnP also allows supported devices to leave a network automatically without adverse effects to the device or other devices on the network.
UPnP can be supported by diverse networking media including Ethernet, Fire wire, phone line and power line networking.

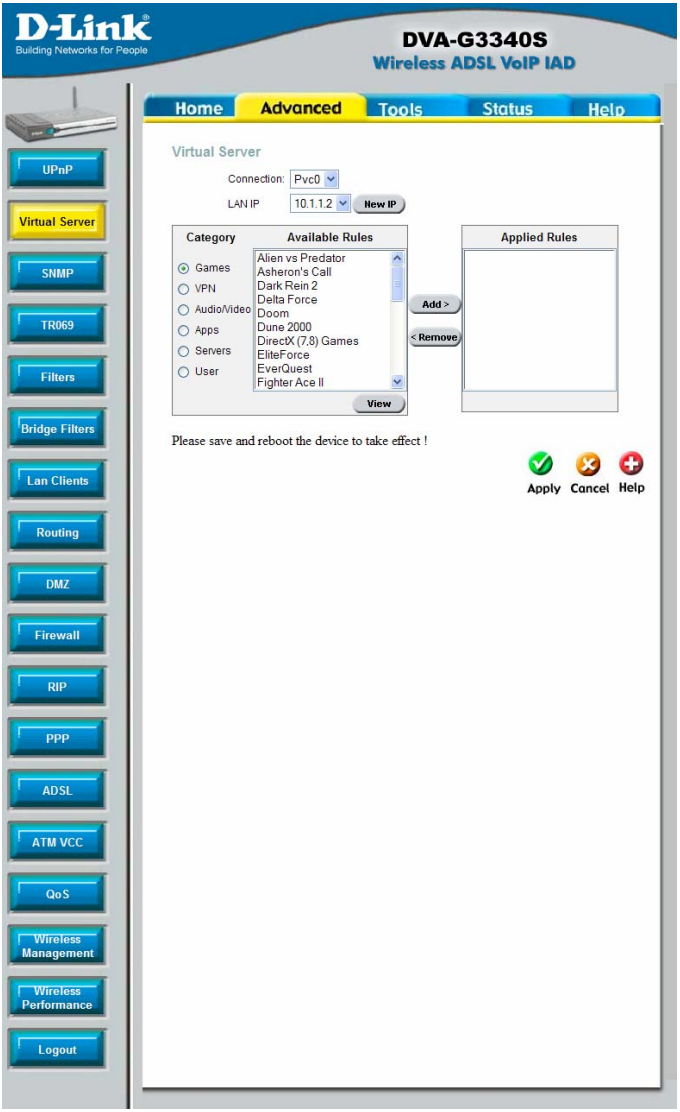
Enable UPnP Menu

To enable UPnP for any available connection, click to check the **Enable UPnP** selection box, select the connection or connections on which you will enable UPnP listed under **Available Connections** and click the **Apply** button.

Virtual Server

Advanced > Virtual Server

Use the Virtual Server menu to set up port forwarding rules in the Router. The Virtual Server function allows remote users to access services on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The DVA-G3340S will accept remote requests for these services at your Global IP Address, using the specified TCP or UDP protocol and port number, and then redirect these requests to the server on your LAN with the Private IP address you specify.



Virtual Server Configuration Menu

The Virtual Server will allow remote users access to various services outside of their LAN through a public IP address, such as FTP (File Transfer Protocol) or HTTPS (Secure Web). Select a connection type and IP address for the Virtual Server. After configuring the Router for these features, the Router will redirect these external

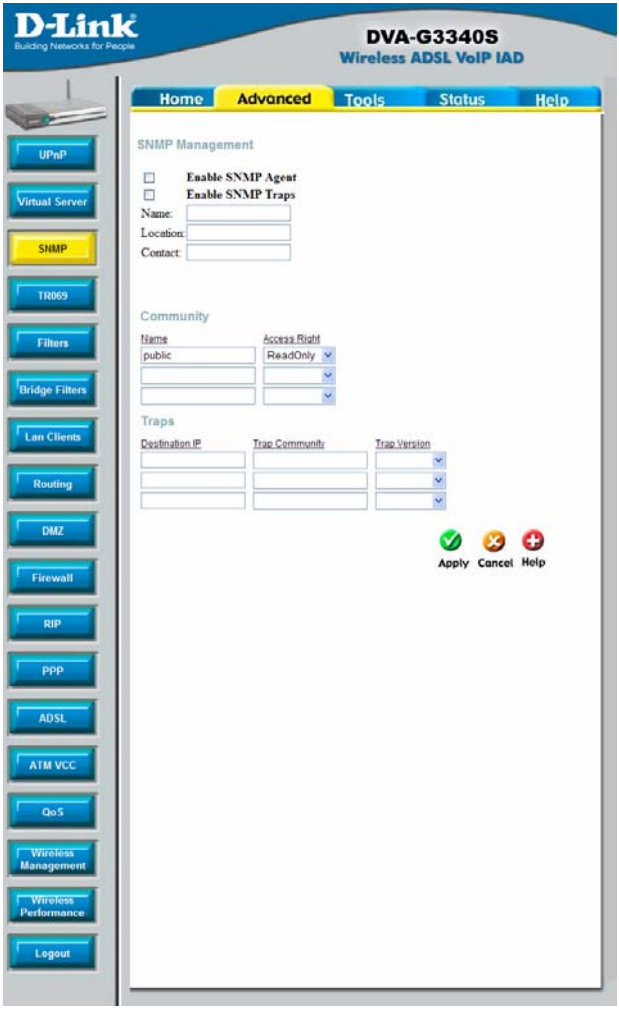
services to an appropriate server on the users' LAN. To choose a particular service click a radio button from the category list and highlight the service from the Available Rules list. Click Add, and then click Apply to save the rule. Ensure you Save & Reboot to make this rule effective.

You may be prompted to add a LAN IP to the Client list, this will redirect you to the LAN Clients page, see below for more info.

SNMP

Advanced > SNMP

This menu can be accessed directly by clicking on the **SNMP** button or hyperlink in the **Advanced** setup menu. Simple Network Management Protocol (SNMP) is an OSI Layer 7 Application designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, performance monitoring, and detection of potential problems in the Router or network.



SNMP Configuration Menu

TR-069

Advanced > TR069

This menu can be accessed directly by clicking on the **TR069** button or hyperlink in the **Advanced** setup menu.

This feature is currently only supported by certain Internet Service Providers and will not require any changes unless instructed.

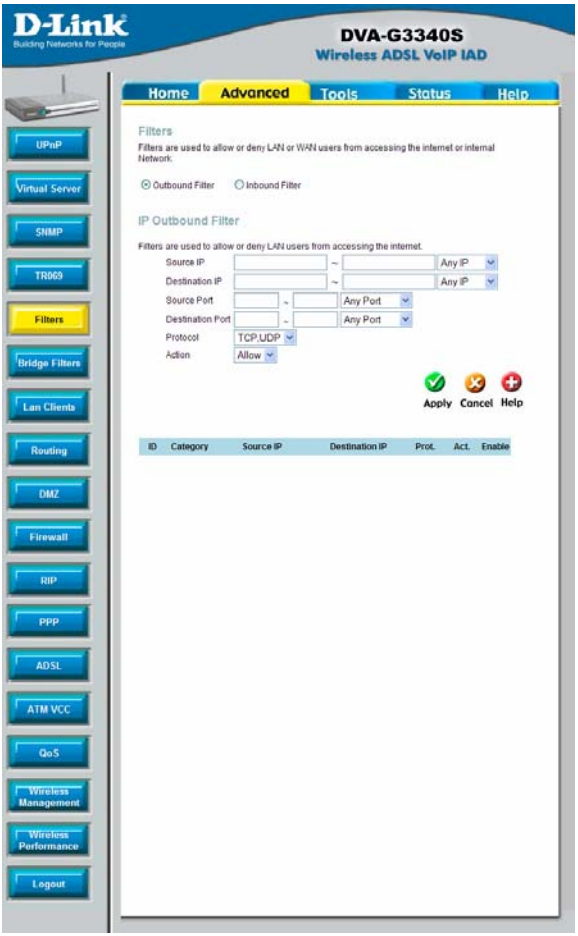
TR069 Configuration Menu

IP Filters

Advanced > Filters

Filter rules in the Router are put in place to allow or block specified traffic. The Filter Rules however can be used in a single direction to examine and then Allow or Deny traffic for Inbound (WAN to LAN) or Outbound (LAN to WAN) routed data. The rules based on IP address and TCP/UDP port.

Configure the filter rules as desired and click the **Apply** button to create the rule. The newly created rule appears listed in the Outbound Filter List at the bottom of the menu. The table below describes the various parameters that are configured for the filter rules.



Filters Configuration Menu

To modify any previously created filter rule, click on the note pad icon in the right hand column of the Filter List for the set you want to configure. Adjust the settings as desired and click the **Apply** button to put the new settings into effect.

First determine the direction of the traffic you want the rule to filter. To filter WAN to LAN traffic, select the **Inbound Filter** option. Any new Inbound Filter rules created will appear in the list. Likewise, should you to filter LAN to WAN traffic, create an **Outbound Filter** rule.

The parameters described below are used to set up filter rules.

Parameter	Description
Source IP	For an Outbound Filter, this is the IP address or IP addresses on your LAN for which you are creating the filter rule. For an Inbound Filter, this is the IP address or IP addresses for which you are creating the filter rule. You can opt to indicate a *Mask Range*, a *Single IP*, an *IP Range* or *Any IP* from the pull-down menu. Choosing Any IP will apply the rule to all WAN or all LAN IP addresses depending on which type of rule (Inbound or Outbound) is being configured.
Destination IP	Where the Destination IP address resides also depends on if you are configuring an Inbound or Outbound filter rule. You can opt to indicate a *Mask Range*, a *Single IP*, an *IP Range* or *Any IP* from the pull-down menu.
Source Port	The Source Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. Select one of the following options from the pull-down menu to define a *Any Port*, *Single Port*, *Port Range* or *Safe Range* (ports above 1024).
Destination Port	The Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. Select one of the following options from the pull-down menu to define a *Any Port*, *Single Port*, *Port Range* or *Safe Range* (ports above 1024).
Protocol	Select the transport protocol (*TCP*, *UDP* or *All*) that will be used for the filter rule.
Action	Select to *Allow* or *Deny* transport of the data packets according to the criteria defined in the rule. Packets that are allowed are routed to their destination; packets that are denied are blocked.

Click the **Apply** button to put the new rule into effect. Any filter rule configured in the menu will appear in the Filters List with the new settings. The Router must save the new settings and reboot before the new rules are applied.

Bridge Filters

Advanced > Bridge Filters

Bridge filters are used to block or allow various types of packets through the WAN interface. This may be done for security or to improve network efficiency. The rules are configured for individual devices based on MAC address. Filter rules can be set up for source, destination or both. You can set up filter rules and disable the entire set of rules without loosing the rules that have been configured.

Bridge Filter Configuration Menu

To add a bridge filter rule, check **Enable Bridge Filters**, type in a Source MAC, a Destination MAC or both in the entry fields. Select *Any* to apply the rule to any protocol that the router receives. The user may also specify a protocol to be filtered by using the pull-down menu, and then choose either *Allow*, to allow the specified protocol to pass through the router, or *Deny* to filter the protocol from the router. The protocols that may be specifically allowed or denied to pass through the WAN interface are *IPv4*, *IPv6*, *RARP*, *PPPoE Discovery* and *PPPoE Session.* Click the **Add**

button. The rule will appear in the entry field below as it is currently configured. To edit an existing rule, select the rule by clicking the corresponding **Edit** radio button. Make the desired changes and click the **Add** button. To remove a bridge filter from the table in the bottom half of the window, click to select the corresponding **Delete** box, and then click **Apply**. Remember to save the configuration changes.

LAN Clients

Advanced > Lan Clients

The LAN Clients menu is used when establishing Port Forwarding, Access Control and Advanced Security rules for IP addresses on the LAN. This menu can be accessed directly by clicking on the **LAN Clients** button or hyperlink in the **Advanced** setup menu. You can also click on the New IP button located in the Port Forwarding, Access Control and Advanced Security menus to access this menu. In order to use these advanced features it is necessary to have IP addresses available for configuration. If there are no IP addresses listed in the LAN Clients menu, it will not be possible to configure Port Forwarding, Access Control and Advanced Security.

Bridge Filter Configuration Menu

Use the LAN Clients menus to add or delete static IP addresses for the advanced functions mentioned above, or to reserve a Dynamically assigned IP address for an advanced function. Dynamically assigned IP addresses will only be listed if DHCP is enabled on the Router. To add a static IP address to the list of available IP addresses, type an IP address that falls within the range a available IP addresses and click on the Add button. In the example above, available addresses range from 10.0.0.1 to 10.255.255.254. Any addresses added will appear in the list of Static Addresses available for advanced configuration. These addresses can then be used in the other Port Forwarding, Access Control and Advanced Security menus. To delete an IP address from the list of Static Addresses, click the Delete box for the address or addresses you want to eliminate and click on the Apply button.

Routing

Advanced > Routing

Use Static Routing to specify a route used for data traffic within your Ethernet LAN or to route data on the WAN. This is used to specify that all packets destined for a particular network or subnet use a predetermined gateway.

Routing Menu

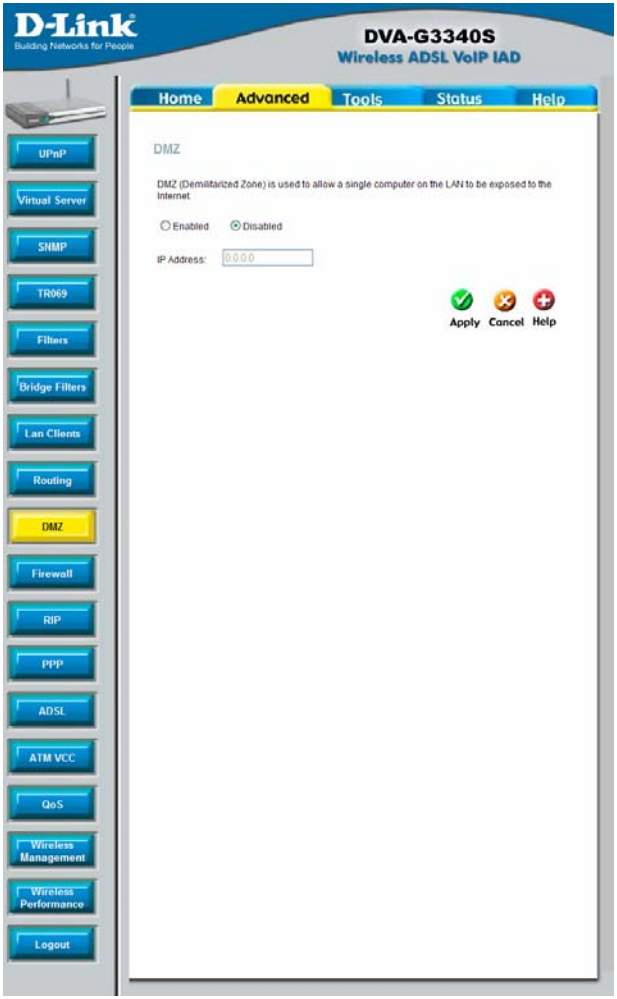
To add a static route to a specific destination IP on the local network, enter a **Destination** IP address, **Netmask**, then click the **Gateway** radio button and type in the Gateway's IP address. Click **Apply** to enter the new static route in the table below. The route becomes active immediately upon creation.
To add a static route to a specific destination IP on the WAN, click the Connection

radio button and choose a connection from the pull-down menu, then enter a **Destination** IP address and **Netmask**. Click **Apply** to enter the new static route in the table below. The route becomes active immediately upon creation
To remove a static route from the table in the bottom half of the window, choose to **Delete** it from the table and click the **Apply** button. Remember to save the configuration changes.

DMZ

Advanced > DMZ

Since some applications are not compatible with NAT, the Router supports use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and will therefore be visible to agents on the Internet with the right type of software. Keep in mind that any client PC in the DMZ will be exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through the DMZ.



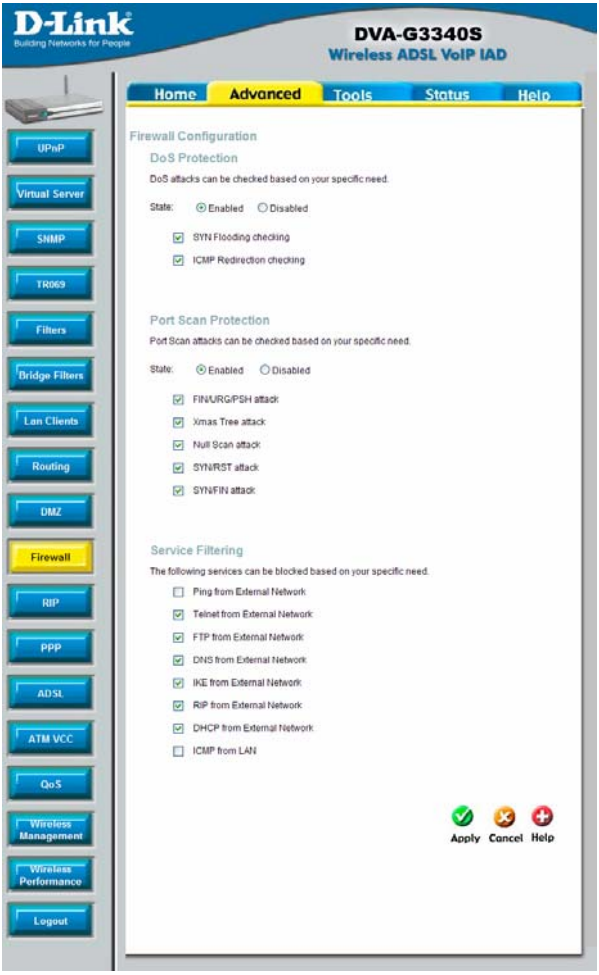
DMZ Menu

To designate a DMZ IP address, select the **Enabled** radio button, type in the **IP Address** of the server or device on your LAN, and click the **Apply** button. To remove DMZ status from the designated IP address, select the Disabled radio button and click Apply. It will be necessary to save the settings and reboot the Router before the DMZ is activated.

Firewall

Advanced > Firewall

The Firewall Configuration menu allows the Router to enforce specific predefined policies intended to protect against certain common types of attacks. There are two general types of protection (DoS, Port Scan) that can be enabled on the Router, as well as filtering for specific packet types sometimes used by hackers. You can choose to **Enable** or **Disable** protection against a customized basket of attack and scan types. To enable **DoS Protection** or **Port Scan Protection**, select the **Enable** radio button for the protection type and click in the selection boxes for the various types of protection listed under each.



Firewall Configuration Menu

When DoS, Port Scan, or Service Filtering Protection is enabled, it will create a firewall policy to protect your network against the following:

Dos Protection	Port Scan Protection	Service Filtering
SYN Flood check	Nmap/FIN attack	Telnet from WAN
ICMP Redirection check	URG/PSH attack	FTP from WAN
	Xmas Tree Scan	DNS from WAN

	Null Scan attack	IKE from WAN
	SYN/RST attack	RIP from WAN
	SYN/FIN Scan	DHCP from WAN

A DoS "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service, or, attempts to disrupt service to a specific system or person.
Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.
The Service Filtering options allow you to block FTP, Telnet response, Pings, etc, from the external network. Check the category you want to block to enable filtering of that type of packet.
When you have selected the desired Firewall policies, click the **Apply** button to enforce the policies. Remember to save any configuration changes.

Routing Information Protocol (RIP)

Advanced > RIP

The Router supports RIP v1 and RIP v2 used to share routing tables with other Layer 3 routing devices on your local network or remote LAN.

Dynamic Routing (RIP) menu

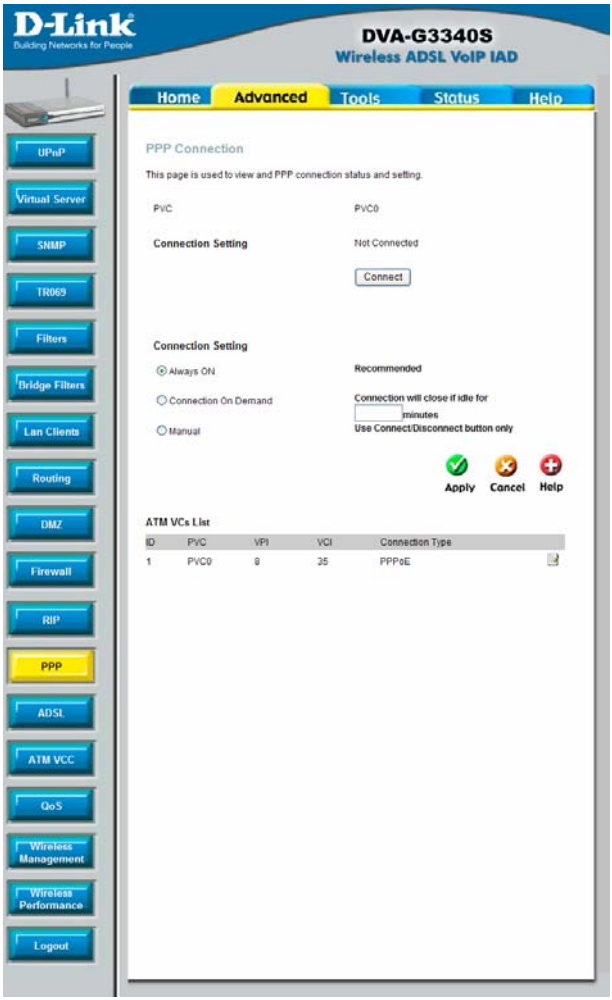
To enable RIP, select *Enabled* from the **RIP** pull-down menu, select the **Protocol** (*RIPv1* and *RIPv1 Compatible*) and **Direction** (*In*, *Out*, or *Both*), and click **Apply**. The RIPv1 Compatible option will transmit RIPv2 broadcast packets and receive both RIP v1 and RIP v2 packets.

The direction configuration refers to the RIP request. Select In to allow RIP requests from other devices. Select Out to instruct the Router to make RIP requests for routing tables from other devices. Select Both to share routing tables in both directions.

PPP Connection State

Advanced > PPP

When the WAN connection is configured for either PPPoA or PPPoE, you can configure the Router's PPP session to remain on all the time, or to disconnect after some period of no activity. You may also choose to instruct the Router to connect each time you want to access the WAN or the Internet.



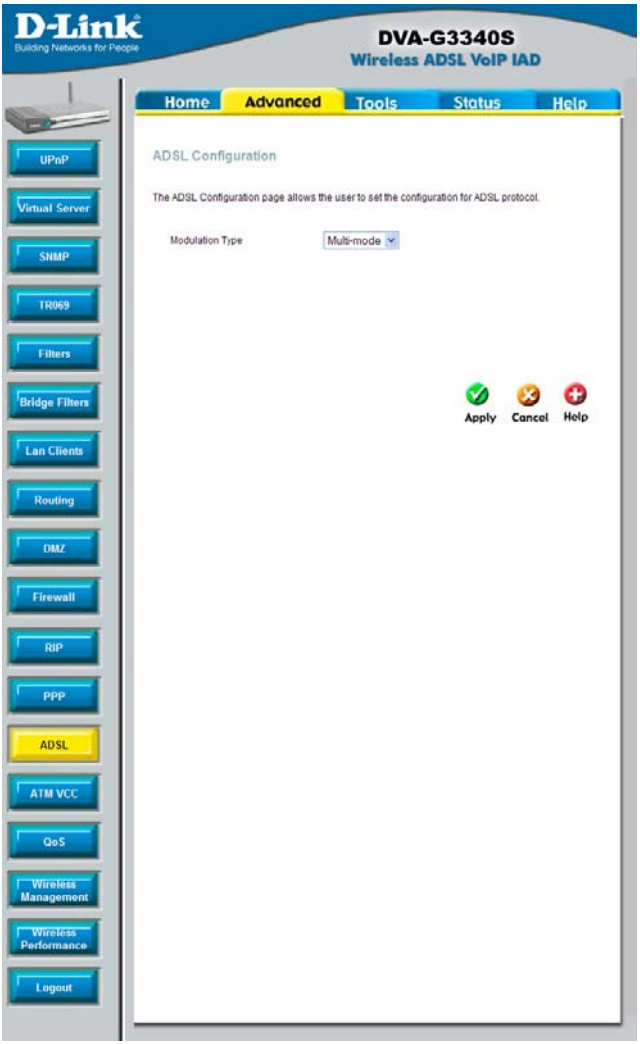
PPP Connection settings menu

If you want the Internet or WAN connection to be available any time a host on your LAN requests access, select the **Always On** option. If your ISP account is billed according to the amount of time the Router is connected, choose the **Connection On Demand** option. You can configure an idle time in minutes to disconnect the PPP connection after a period of inactivity. This will discontinue the PPP session and require a few seconds to reconnect when a host requests access to the WAN. Alternatively you can choose the **Manual** option and use the **Connect** button to initiate a PPP connection each time you want to use the Router to access the WAN. If you use the Manual option, you must return to this menu and click the **Disconnect** button to terminate the PPP session.

ADSL

Advanced > ADSL

The ADSL Configuration page allows the user to set the configuration for ADSL protocols. For most ADSL accounts the default settings *Multi-mode* will work. This configuration works with all ADSL implementations. If you have been given instructions to change the Modulation method used, select the desired option *T1.413*, *G.dmt*, or *G.lite* and click the **Apply** button.



ADSL Modulation Configuration

ATM VC Setting

Advanced > ATM VCC

The ATM Virtual Circuit connection menu is used to configure the WAN connection. If you are using multiple PVCs, you can change the configuration of any PVC in this menu. To create new or additional PVCs, read the section below on Multiple PVCs.
This menu can be used as an alternative menu to configure the same settings found on the WAN menu in the Home directory.

ATM Virtual Circuit configuration menu

To configure an existing PVC configuration set, click the corresponding notepad icon in the right-hand column of the ATM VCs List. The PVCs current settings appear above in the entry fields of the ATM VC Settings menu. Configure the appropriate settings and click the **Apply** button to put the new settings into effect.

Quality of Service (QoS)

Advanced > QoS

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large bandwidth or have a high priority, such as VoIP (Voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Not only can a larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. Each physical port on the Router can have up to 8 **PVC**s (Permanent Virtual Circuits) to which traffic from various sources can be mapped to, and in turn prioritized. Select a PVC that has been configured (to configure a PVC click Home > WAN), and then assign a **Priority** of 1 (low) to 4 (high). To enable QoS settings click the **Enable Port Based QoS** check box. To enable **IGMP Snooping / Proxy** on a particular PVC click on the PVC and then click the radio button to *Enabled*.

QoS configuration menu

Wireless Management

Advanced > Wireless Management

The **Wireless Management** menu located in the **Advanced** directory is used to control MAC address access to the wireless access point and to view a list of MAC addresses that are currently associated with the access point. This menu is also be used to enable and configure use of multiple SSIDs. To use more than one SSID, WEP and WPA security must first be disabled (see below).

Wireless Management Access List

To view a list of stations currently associated with the access point, click the **Associated Stations** radio button.

Configure Wireless Access Control

To create a list of MAC addresses that are banned or allowed association with the wireless access point:

1. Click in the **Enable Access List** option box to select it.
2. Select the action to perform on the MAC address to be specified. Choose to **Allow** or **Ban** association.
3. Type in the **MAC Address** in the entry field provided.
4. Click the **Add** button to add the MAC address to the list. The AMC address will appear listed in the table below.
5. After compiling the list of MAC addresses as desired, click the **Apply** button to enforce access control for the MAC addresses in the list.

To remove any MAC address from the list, click the radio button in the left column of the list for the MAC address to be removed and click the **Apply** button.

Configure Multiple SSID
Multiple SSID cannot be used if the access point has either WPE or WPA enabled. This must first be disabled in the Wireless menu located in the Home directory.
To configure multiple SSID:

1. Disable WEP or WPA in the **Wireless** menu of the **Home** directory.
2. Click in the **Enable Multiple SSID** option box to select it.
3. Enter the **SSID** you want to add.
4. Click the **Add** button to add the SSID to the list.
5. Click the **Apply** button to enable the listed SSIDs.

To remove an SSID from the list, click the radio button in the left column of the list for the SSID to be removed and click the **Apply** button.

Wireless Performance

Advanced > Wireless Performance

If you want to tweak wireless settings, click the **Wireless Performance** menu button in the **Advanced** directory

Wireless LAN Performance settings

Tools

The Tools tab allows you to set up basic maintenance features on the ADSL router. The windows available under this tab include Admin, Time, Remote Log, System, Firmware, Miscellaneous, and Test.

Administrator Settings

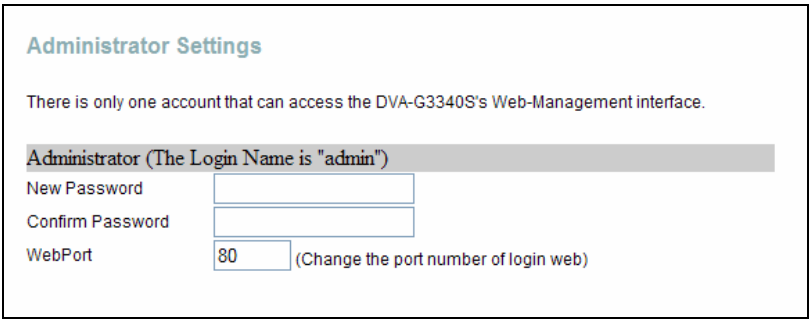
Tools > Admin

Click the **Tools** tab to reveal the menu buttons for various functions located in this directory. The **Administrator Settings** is the first menu that appears in the Tools directory. This menu is used to change the system password used to access the web manager, to save or load Router configuration settings and to restore default settings. The functions in this and the other Tools menus are described below.

Administrator settings

Change System Password

To change the password used to access the Router web manager, click the **Admin** button in the **Tools** directory to display the Administrator Settings menu. Under the Administrator heading, type the **New Password** and **Confirm Password** to be certain you have typed it correctly. Click the **Apply** button to activate the new password. The System User Name remains "admin", this cannot be changed using the web manager interface. Be sure to save the new setting.



Administrator Settings change password menu

Remote Web Management and Telnet Access

The Administrator Settings menu is also used to enable remote Telnet management and remote web management access to the Router. To enable remote management of the Router, select the **Enabled** radio button for either Remote Web or Remote Telnet Management and type the IP Address and Netmask of the remote network or system used for management. Click the **Apply** button to activate remote management from the chosen IP address. Be sure to save the new setting.

Time (SNTP)

Tools > Time

The Router provides a number of options to maintain current date and time including SNTP.

Time & Date Configuration

To configure system time on the Router, select the method used to maintain time. The options available include SNTP, using your computer's system clock (default) or set the time and date manually. If you opt to use SNTP, you must enter the SNTP server URL or IP address. Click the **Apply** button to set the system time.

Remote Log

Tools > Remotelog

The router provides the ability to send the data from the log to a remote server using a Syslog Service. This can be configured to be basic log data to more sophisticated debug information from the unit for troubleshooting.

Remotelog Configuration

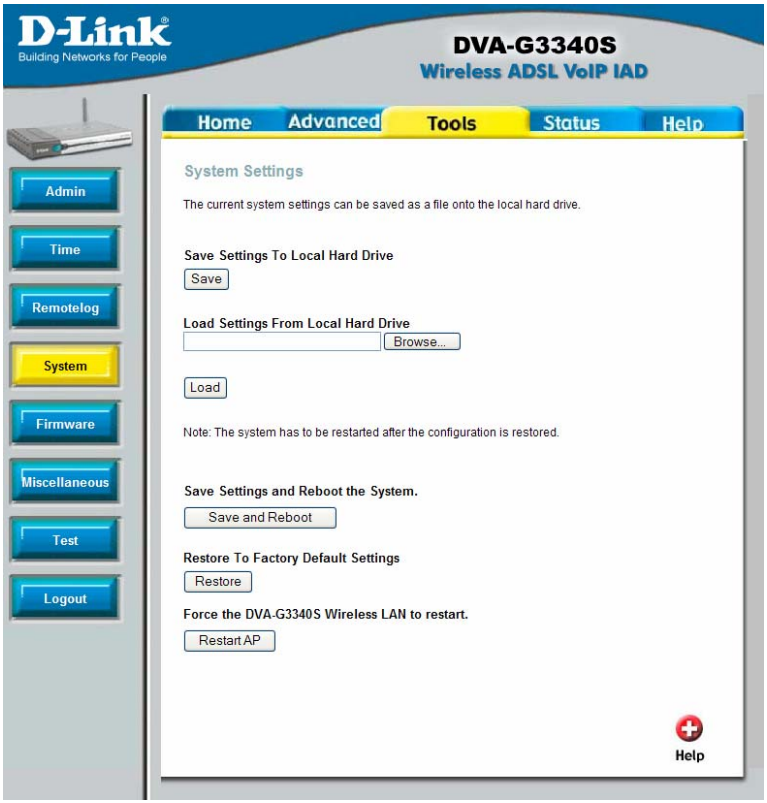
You can even configure multiple logs for different Log Levels to different IP addresses.

System Settings

Tools > System

Save or Load Configuration File

Once you have configured the Router to your satisfaction, it is a good idea to back up the configuration file to your computer. To save the current configuration settings to your computer, click the **Admin** button in the **Tools** directory to display the Administrator Settings menu. Click the **Save** button to **Save Settings to Local Hard Drive**. You will be prompted to select a location on your computer to put the file. The file type is .xml (HTML) and may be named anything you wish.
To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Click the **Load** button to **Load Settings From Local Hard Drive**. Confirm that you want to load the file when prompted and the process is completed automatically. The Router will reboot and begin operating with the configuration settings that have just been loaded.



System Settings

Save Settings and Reboot the System

Pressing the Save & Reboot button will save all current settings to the devices memory. The unit will then restart with all of these saved settings.

Restore Factory Default Settings

To reset the Router to its factory default settings, click the **Restore** button in the Administrator Settings menu. You will be prompted to confirm your decision to reset the Router. The Router will reboot with the factory default settings including IP settings and Administrator password.

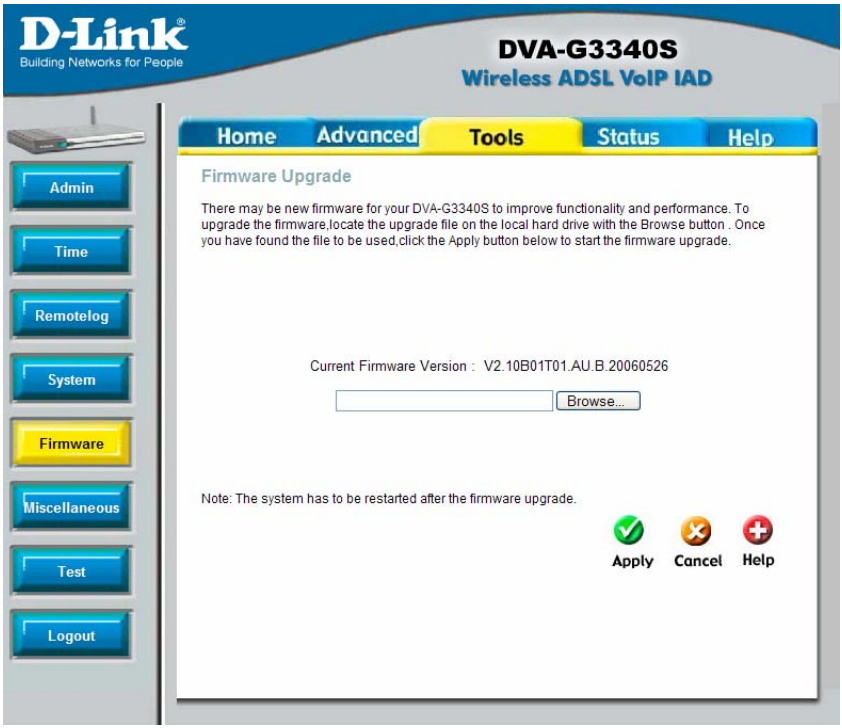
Force the DVA-G3340S Wireless LAN to restart

To save you having to restart the entire router you can just reboot the Wireless portion of the unit. This comes in handy when making changes to the Wireless LAN security settings as you can make these changes effective without having to disconnect from a VoIP call / Internet Connection.

Firmware Upgrade

Tools > Firmware

Use the **Firmware Upgrade** menu to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you save the configuration settings with the System Settings menu described above.



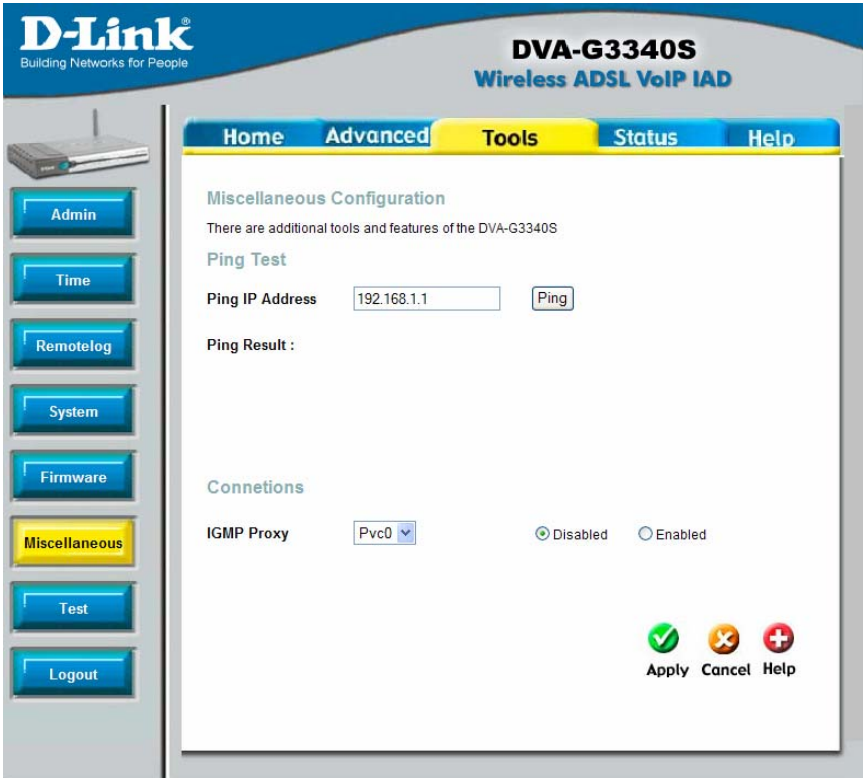
Firmware Upgrade

To upgrade firmware, type in the name and path of the file or click on the **Browse** button to search for the firmware file. Click the **Apply** button to begin copying the file. The file will load and restart the Router automatically.

Ping Test

Tools > Miscellaneous

To perform a standard Ping test for network connectivity, click the **Misc.** menu button in the Tools directory to view the **Miscellaneous Configuration** menu.



Miscellaneous Configuration menu

Ping Test

The Ping test functions on the WAN and LAN interfaces. Type the IP address you want to check in the space provided and click the **Ping** button. Read the Ping test result in the space immediately below.

IGMP Proxy

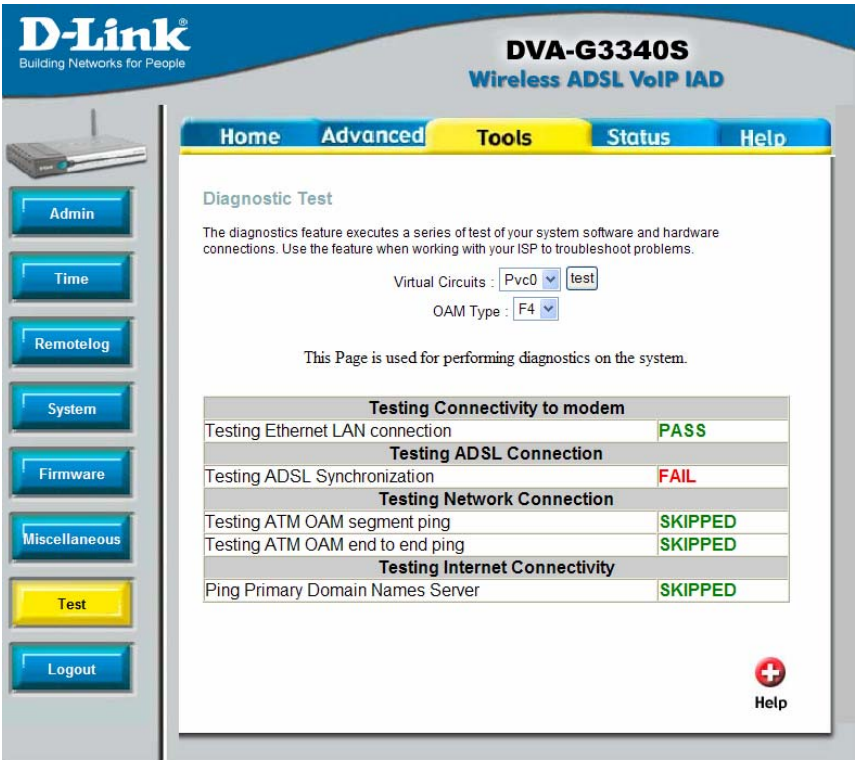
The Miscellaneous Configuration menu also allows you to enable IGMP forwarding. This is disabled by default. This setting will not allow IGMP (Internet Group Management Protocol) packets to be forwarded to the LAN. IGMP is used to manage multicasting on TCP/IP networks; most users will not need to enable this. Some ISPs

use IGMP to perform remote configuration for client devices, such as the Router. If you are unsure, check with your ISP. To enable IGMP service to the LAN interface, select Enabled and click the Apply button.

Test

Tools > Test

The Test menus are used to test connectivity of the Router. This diagnostics feature executes a series of test of your system software and hardware connections. Use this Diagnostic Test when working with your ISP to troubleshoot problems.



Diagnostic Test Menu

Status Information

Use the various read-only menus to view system information and monitor performance.

Device Information Display

Status > Device Info

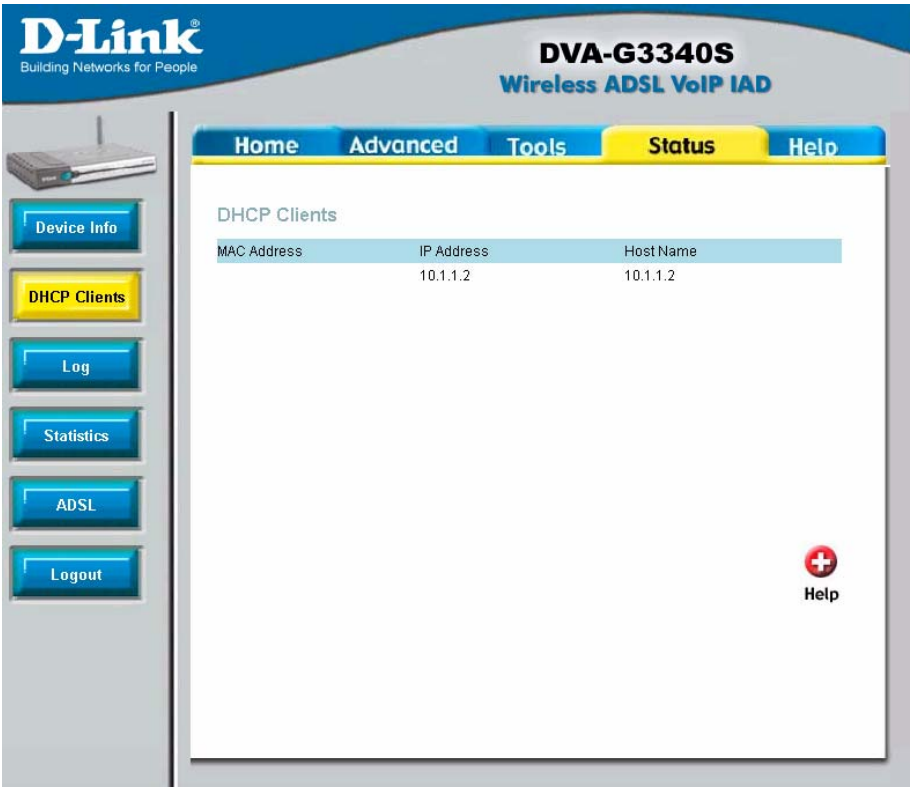
Use the **Device Information** window to quickly view basic current information about the LAN and WAN interfaces and device information including Firmware Version and MAC address.

Device Information display

DHCP Clients Info

Status > DHCP Clients

To view **DHCP clients** that are configured on the Router click DHCP Clients under the Status tab.



DHCP Client Info list

Log

Status > Log

The system log displays chronological event log data. Use the navigation buttons to view or scroll log pages. You may also save a simple text file containing the log to your computer. Click the Save Log button and follow the prompts to save the file.

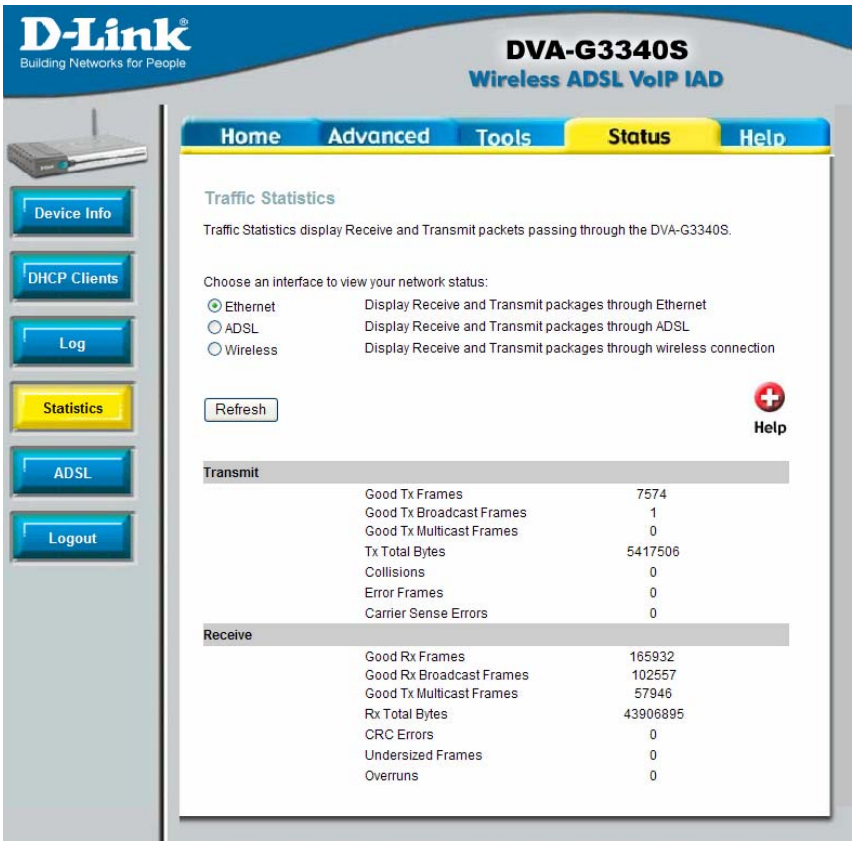
Log display

Click **Clear Log** delete the current log information.

Traffic Statistics

Status > Statistics

Use the Traffic Statistics window to monitor traffic on the Ethernet or ADSL Internet connection. When the Wireless Select the interface for which you want to view packet statistics and the information will appear below.



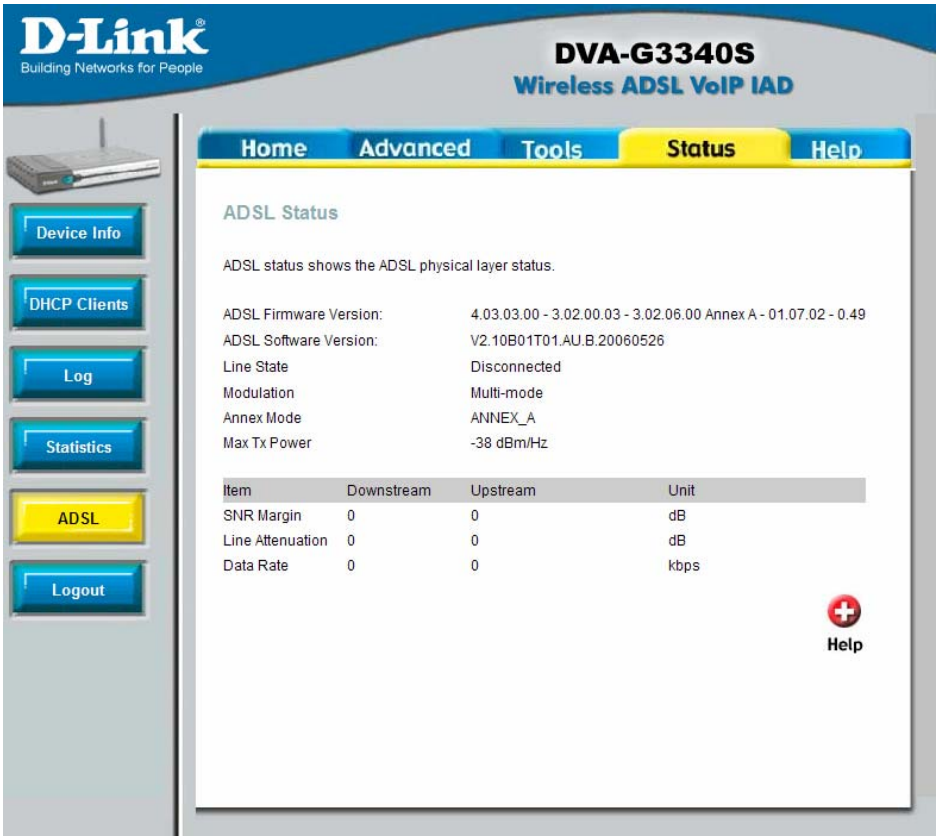
Traffic Statistics information

Click **Refresh** to view traffic information.

ADSL

Status > ADSL

Use the ADSL Status information and the Test page for troubleshooting the ADSL connection.



ADSL Status information

Technical Specifications

Key Component	Description
Network Processor and ADSL Chipset	TI AR7VWi
Voice Chipset	TI TNETV901

Product Feature	Description
Network Interface	
One ADSL port	RJ-11, inner pair (pin 2,3)
Standard Compliance	**ADSL Standards:** ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) AnnexA ITU G.992.2 (G.lite) Annex A ITU G.994.1 (G.hs) **ADSL2 Standards:** ITU G.992.3 (G.dmt.bis) Annex A ITU G.992.4 (G.lite.bis) Annex A **ADSL2+ Standards:** ITU G.992.5 Annex A
Line Rate	Downstream: up to 24Mbps Upstream : up to 1Mbps
Performance	Pass DSL Forum TR-067 Performance Criteria
LAN Interface	
Four Fast Ethernet ports	RJ-45, 10/100Mbps, MDI/MDIX Auto-sesnsing
Standard Compliance	IEEE802.3, IEEEE802.3u
USB Interface	
One USB port	Type B connector
Standard Compliance	USB Implementation Forum USB 1.1 Specification
Voice Interface	
Two ports for POTS connection	RJ-11, FXS interface Loop Start
One port for PSTN connection	RJ-11, FXO interface

Telephone dialing mode support	DTMF Dial Pulse (20pps/10pps)
Ringer Equivalency Number	REN=5
Line Impedance	600ohm
Wireless Access Point Embedded	
Standard Compliance	IEEE 802.11 IEEE 802.11b IEEE 802.11g
Radio and Modulation Type	IEEE 802.11b: DQPSK, DBPSK, DSSS, and CCK IEEE 802.11g: BPSK, QPSK, 16QAM, 64QAM, OFDM
Operating Frequency	2400 ~ 2484.5MHz ISM band
Channel Numbers	11 channels for United States 13 channels for European Countries 13 channels for Japan
Data Rate	IEEE 802.11b: 11, 5.5, 2, and 1Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps
Media Access Protocol	CSMA/CA with ACK
Form Factor and Interface	mini-PCI interface
Antenna type	One Built-in Diversity Antenna
Power	
External Switching Power Adapter	Input: Depends on specific country requirements Output: 12V DC, 1.25A
Device Power consumption	Maximum 12 watt
Reset Button	Reset to factory default

Product Feature	Description
Bridging / Routing	
Transparent bridging	
Dynamic Learning	Up to 1024 MAC addresses
Encapsulation	Bridged/Routed Ethernet over ATM (RFC1483/2684)

	Classical IP over ATM (RFC1577)
IPv4	TCP/UDP
	ARP
	ICMP
IP Routing	RIP v1 (RFC 1058), RIP v2 (RFC 1389)
	IP Static Routing
DHCP	DHCP Server (RFC2131)
	DHCP Client (RFC2131)
DNS	DNS Cache
	Dynamic DNS
IP multicast	IGMP Proxy
	IGMP Snooping
ATM / ADSL	
Multiple PVC	Support 8 PVCs
ATM Cell format	ITU-T Rec. I.361
ATM Adaptation Layer	AAL5
ATM signaling	ATM Forum UNI3.1/4.0
OAM support	F4/F5 Loopback
ATM QoS (Traffic Shaping)	UBR, CBR, VBR
PPP Support	
Point-to-Point Protocol	RFC1661
PPP over ATM	RFC2364
PPP over Ethernet	RFC2516
PPP Encapsulation	VC
	LLC
User Authentication	PAP (RFC 1334)
	CHAP (RFC 1994)
	Auto-detection of PAP/CHAP
NAT	
NAT/NAPT	
Port Forwarding	Static IP masquerade(1~65535)
	Entry Number: 32 entries

	Port Number Setting:- Possible to assign the range- Possible to set TCP/UDP/Both as the protocol
Pass Through	IPSec/L2TP/PPTP pass through
NAT ALGs	MSN MSGR
	FTP
	SIP (Video/ Audio/ White Board/ Remote Control) ICQ for File and Audio transfer
	NetMeeting 3/ 2.0 Video/Audio receive CUSEEME
Security	
MAC Filtering	Over 16 entries
	Only ARP Pass-through
	MAC Address and Ethernet type are configurable
IP Filtering	32 records
	Range Setting (IP Address, Port Number) In-bound/Out-bound Setting
SPI	Detection of Known Attacks
QoS	
Priority Queue	Voice over data
Wireless AP Functions	
ESS-ID Support	
MAC Address Filtering	Support Access Control List (ACL)
WEP Support	64/128/256 bits
WPA Support	
VoIP	
Call Control Protocol	SIP (RFC3261)
Codec	G.711µ-law/A-law
	G.726
	G.729A
Echo Canceller	G.168
Fax Relay	G.711

DTMF Relay	RFC2833
Country Tone Support	DT , RBT , BT，Howler／HST(future support)
Tone Detection	DTMF
	Modem/Fax: V.21,V.25
PSTN Life-line Function	Automatic fall back to PSTN in case of power failure PSTN line automatic selection (e.g. emergency Call 911) PSTN routing table support base on prefix number
Caller ID	BellCore, ETSI complaint
Life-line Backup	Making call to PSTN Receiving call from PSTN
RTP/RTCP	
Configuration / Management	
Access Administration	Username/Password control for Telnet, WEB configuration
WEB-based management	HTTP server
Ping	Support Ping test from Modem
SNTP	Simple Network Time Protocol
Factory Reset	Reset to factory default
UPnP 1.0	
Diagnostics	
Configuration Backup/Restore	

Product Feature	Description
Safety Requirement	
CSA International Mark	Including CSA950, UL1950, IEC60950, EN60950
EMC Specification	
FCC part15 class B	
PTT Test	
FCC part68	
Wireless Certification	
Wi-Fi certified	
Environmental Requirement	

Operating Temperature	0 °C to 40 °C
Storage Temperature	-20 °C to 70 °C
Operating Humidity Range	5% to 95% Non-condensing

Product Feature	Description
IP Address/Mask	10.1.1.1/255.0.0.0
VPI/VCI	8/35
ADSL Mode	Multi-mode
Connection Mode	PPPoE LLC
Web Interface User Name/Password	admin/admin

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link Australia
1 Giffnock Avenue, North Ryde,
NSW 2113
Sydney, Australia

TEL: 61-2-8899-1800
FAX: 61-2-8899-1868

Australia: 1300-766-868
New Zealand: 0800-900-900

URL:
www.dlink.com.au
www.dlink.co.nz

E-MAIL:
support@dlink.com.au
info@dlink.com.au

D-Link®
Building Networks for People