

# USER MANUAL

## DVA-G3340S

VERSION 1.10



**D-Link**<sup>®</sup>

**BROADBAND**

# Contents

<b>Package Contents</b> .....	4
<b>Introduction</b> .....	5
<b>Features</b> .....	8
<b>Using the Web Interface</b> .....	9
Home > Wizard .....	9
Home > Wireless .....	10
Home > Wireless > WEP .....	12
Home > Wireless > WPA .....	14
Home > Wireless > WPA-PSK .....	15
Home > WAN > PPPoE/PPPoA .....	16
Home > WAN > Dynamic IP Address .....	21
Home > WAN > Bridge Mode .....	24
Home > WAN > ATM .....	29
Home > WAN > ATM VC Settings .....	31
Home > WAN > Multiple PVC Settings .....	33
Home > LAN .....	34
Home > DHCP .....	35
Home > DNS .....	38
Home > Dynamic DNS .....	39
Home > Voice > Server .....	40
Home > Voice > User Agent .....	42
Home > Voice > Peer to Peer .....	44
Home > Voice > Telephony .....	46
Home > Voice > ACR .....	49
<b>Advanced Settings</b> .....	50
Advanced > UPnP .....	50
Advanced > Virtual Server .....	51
Advanced > SNMP .....	53
Advanced > TR069 .....	54
Advanced > Filters .....	55
Advanced > Bridge Filters .....	57
Advanced > Lan Clients .....	59
Advanced > Routing .....	60

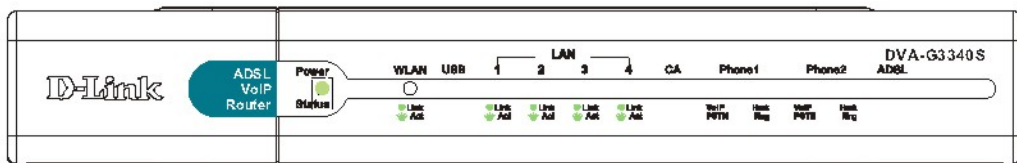
Advanced > DMZ .....	62
Advanced > Firewall.....	63
Advanced > RIP .....	65
Advanced > PPP .....	66
Advanced > ADSL.....	67
Advanced > ATM VCC .....	68
Advanced > QoS.....	69
Advanced > Wireless Management .....	70
Advanced > Wireless Performance .....	72

<b>Tools.....</b>	<b>73</b>
Tools > Admin .....	73
Tools > Time.....	75
Tools > Remotelog .....	76
Tools > System .....	77
Tools > Firmware.....	79
Tools > Miscellaneous.....	80
Tools > Test.....	82

<b>Status Information .....</b>	<b>83</b>
Status > Device Info.....	83
Status > DHCP Clients.....	84
Status > Log .....	85
Status > Statistics.....	86
Status > ADSL.....	87

<b>Technical Specifications .....</b>	<b>88</b>
---------------------------------------	-----------

# Package Contents



## Contents of Package:

- D-Link DVA-G3340S High-Speed 2.4GHz Wireless ADSL VoIP Router
- Power Adapter - AC 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.

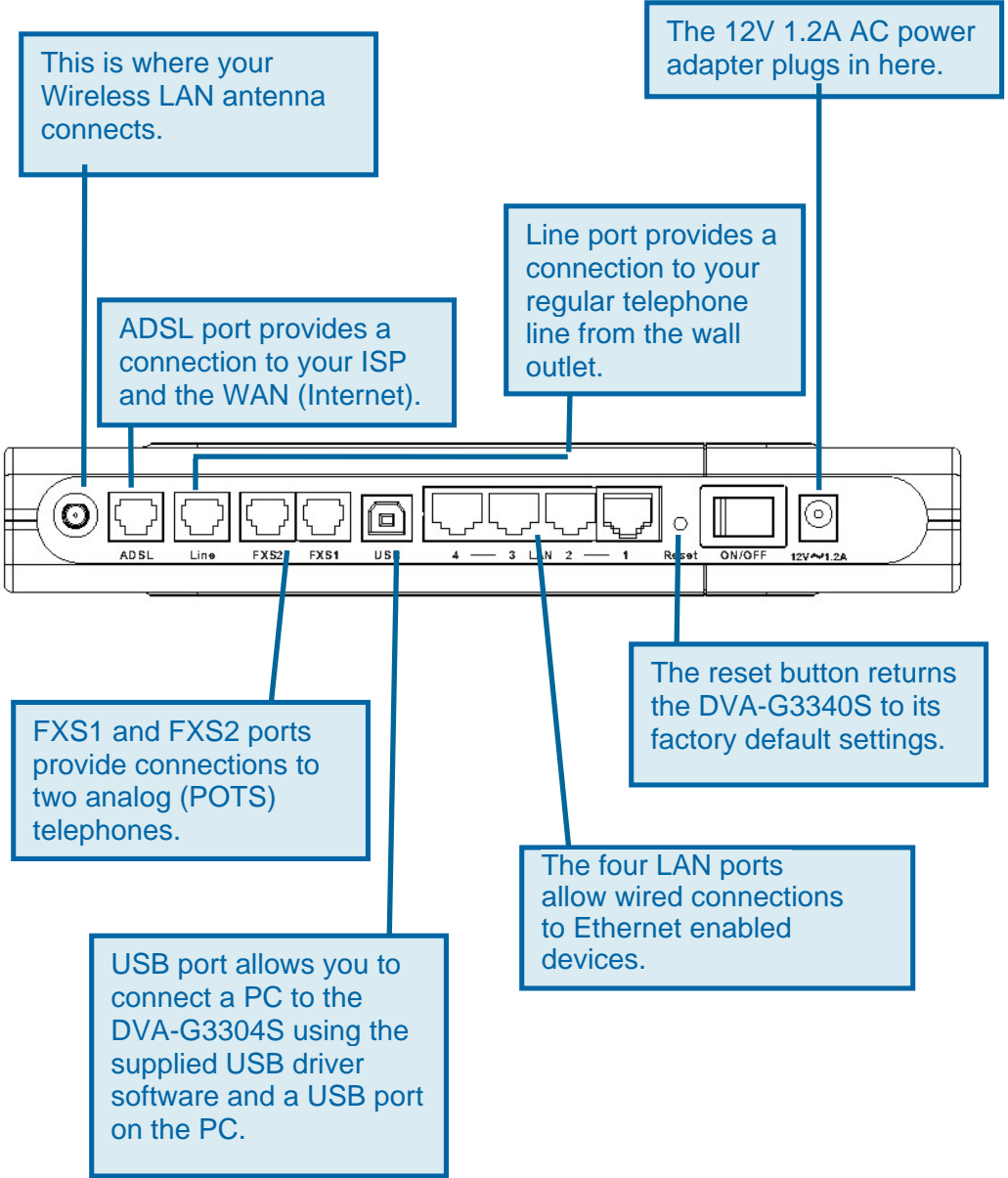
Unlike most routers, the DVA-G3340S provides data transfers at up to 5X (compared to the standard 11 Mbps) when used with other D-Link AirPlus G products. The 802.11 g standard is backwards compatible with 802.11 b products. This means that you do not need to change your entire network to maintain connectivity. 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

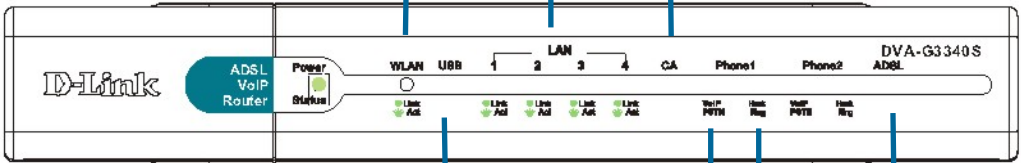


# LEDs

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.

LAN – These LEDs will be lit green when a LAN connection is detected. They 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:

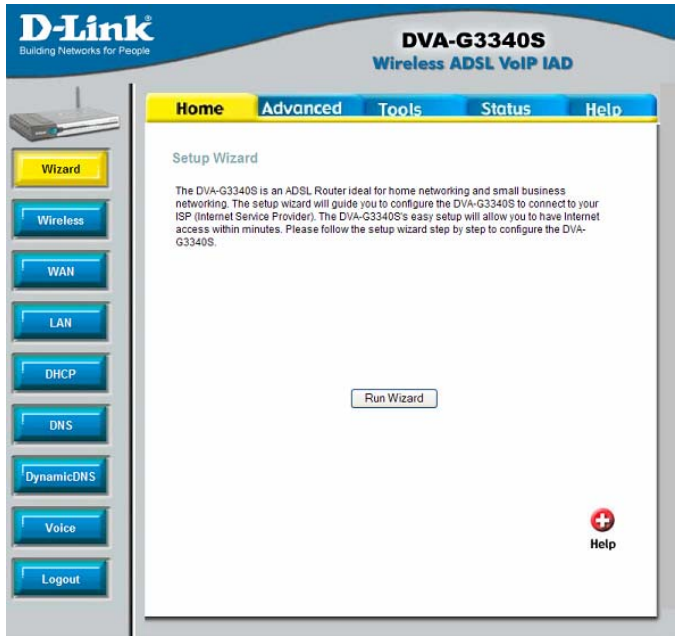
- Open your web browser
- Type in the IP Address of the Router (<http://10.1.1.1>)

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.



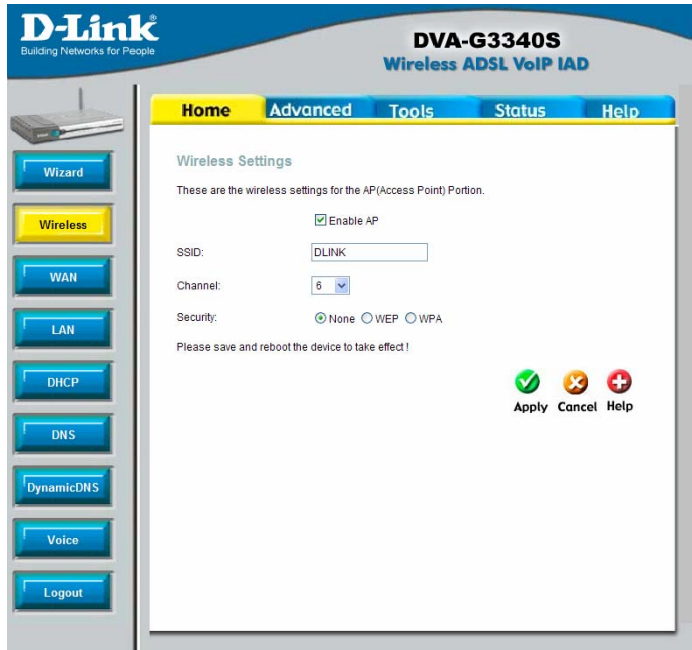
These buttons appear on most of the configuration screens in this section. Please click on the appropriate button at the bottom of each screen after you have made a configuration change.



# 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.

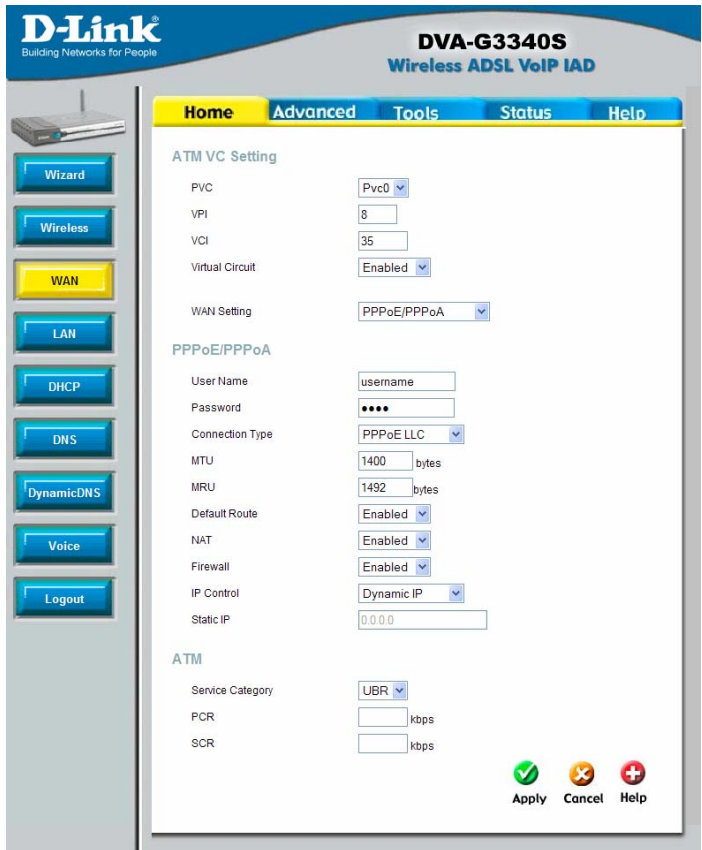
Click the **Apply** button to put the changes into effect. Remember to save the settings using the System Settings menu.

# Configuring the WAN Connection

Home > WAN > PPPoE/PPPoA



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 (*PcvO* 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 PPPoE 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 given an IP address for your 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
<b>User Name</b>	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.
<b>Password</b>	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.
<b>Connection Type</b>	This specifies the protocol (PPPoE or PPPoA) and the encapsulation method (LLC or VC-MUX) used for your connection. The options available are <i>PPPoE LLC</i> , <i>PPPoA LLC</i> or <i>PPPoA VC-MUX</i> .

<p><b>MTU</b></p>	<p>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.</p>
<p><b>MRU</b></p>	<p>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.</p>
<p><b>Default Route</b></p>	<p>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.</p>
<p><b>NAT</b></p>	<p>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.</p>
<p><b>Firewall</b></p>	<p>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.</p>
<p><b>IP Control</b></p>	<p>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 <i>Dynamic IP</i>. Some users will be given a specific IP address for the WAN interface. In this case you need to change this setting to <i>Static IP</i>. When Static IP is selected in the IP Control menu, you need to type in</p>

	<p>the global IP address provided to you by your ISP. The <i>IP Unnumbered</i> 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.</p>
<b>Static IP</b>	<p>If you have selected the <i>Static IP</i> 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.</p>

# 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.

The screenshot shows the D-Link DVA-G3340S router's configuration interface. The top navigation bar includes 'Home', 'Advanced', 'Tools', 'Status', and 'Help'. The left sidebar contains buttons for 'Wizard', 'Wireless', 'WAN', 'LAN', 'DHCP', 'DNS', 'DynamicDNS', 'Voice', and 'Logout'. The 'WAN' button is highlighted in yellow. The main content area is titled 'DVA-G3340S Wireless ADSL VoIP IAD' and shows the 'Dynamic IP' settings under the 'Advanced' tab. The 'ATM VC Setting' section includes: PVC (Pvc0), VPI (8), VCI (35), Virtual Circuit (Enabled), and WAN Setting (Dynamic IP Address). The 'Dynamic IP' section includes: Connection Type (1483 Bridged IP LLC), Cloned MAC Address (00:00:20:32:00:AB), Cloned MAC Address (Clone MAC Address), MTU (bytes), NAT (Enabled), and Firewall (Enabled). The 'ATM' section includes: Service Category (UBR), PCR (kbps), and SCR (kbps). At the bottom right, there are three buttons: 'Apply' (green checkmark), 'Cancel' (orange X), and 'Help' (red plus).

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 (*Pvc0* 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 be 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
<b>Connection Type</b>	This specifies the connection type and encapsulation method used for your Dynamic IP Address connection. The options available are <i>Bridged IP LLC</i> or <i>Bridged IP VC-MUX</i> .
<b>Cloned MAC Address</b>	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 <b>Clone MAC Address</b> 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

	<p>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.</p>
<b>MTU</b>	<p>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.</p>
<b>NAT</b>	<p>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.</p>
<b>Firewall</b>	<p>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.</p>

# 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 be 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.

The screenshot shows the configuration interface for a D-Link DVA-G3340S Wireless ADSL VoIP IAD. The page is titled "Static IP" and is part of the "WAN" settings. The interface includes a navigation menu on the left with buttons for Wizard, Wireless, WAN (highlighted), LAN, DHCP, DNS, DynamicDNS, Voice, and Logout. The main content area is divided into sections: "ATM VC Setting" and "Static IP".

**ATM VC Setting**

- PVC: Pvc0
- VPI: 8
- VCI: 35
- Virtual Circuit: Enabled
- WAN Setting: Static IP Address

**Static IP**

- Connection Type: 1483 Bridged IP LLC
- IP Address: [ ]
- Subnet Mask: [ ]
- Gateway Address: [ ]
- Primary DNS Address: [ ]
- Secondary DNS Address: [ ]
- MTU: 1400 bytes
- NAT: Enabled
- Firewall: Enabled

**ATM**

- Service Category: UBR
- PCR: [ ] kbps
- SCR: [ ] kbps

At the bottom right, there are three buttons: Apply (green checkmark), Cancel (orange X), and Help (red plus).

## 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 <i>Bridged IP LLC</i> , <i>Bridged IP VC-MUX</i> , <i>Routed IP LLC</i> , <i>Routed IP VC-MUX</i> or <i>IPoA</i> .

<b>IP Address</b>	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.
<b>Subnet Mask</b>	This is the Subnet mask for the WAN interface. Get this from your ISP.
<b>Gateway Address</b>	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.
<b>ARP Server Address</b> (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.
<b>Primary DNS Address</b>	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.
<b>Secondary DNS Address</b>	This is the second choice for a DNS server. Get this IP address from your ISP.
<b>MTU</b>	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.
<b>MRU</b>	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**

Service Category

PCR  kbps

SCR  kbps

**ATM Settings for WAN connection (PPPoE/PPPoA menu)**

Additional ATM settings for PPPoE or PPPoA connections:

ATM QoS Parameters	Description
<p><b>Service Category</b></p>	<p>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.</p> <p>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.</p> <p>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.</p> <p><i>UBR</i> – 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</p>

	<p>desirable to specify the PCR.</p> <p><i>CBR</i> – Constant Bit Rate, usually used in circumstances where very low packet loss and very low Cell Delay Variable (CDV) are desirable.</p> <p><i>VBR</i> – 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.</p>
<b>PCR</b>	<p>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.</p>
<b>SCR</b>	<p>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).</p>































































































































