

Advanced Wireless – Advanced Settings

To access Advanced Settings, point to the **Advanced Wireless** on the left window and click **Advanced Settings** submenu, or click the **Advanced Settings** button in the Wireless Settings window.

In this page, you can configure more advanced settings of 802.11g wireless radio. However, it is recommended to remain as default unless your ISP requests to change it.

ADVANCE WIRELESS

These options are for users that wish to change the behavior of their 802.11g wireless radio from the standard setting. D-Link does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

ADVANCED WIRELESS SETTINGS

Transmission Rate :	Auto	▼
Multicast Rate :	Auto	▼
Transmit Power :	100%	▼
Beacon Period :	100	(20 ~ 65535)
RTS Threshold :	2347	(0 ~ 2347)
Fragmentation Threshold :	2346	(256 ~ 2346)
DTIM Interval :	1	(1~255)
User Isolation :	Off	▼
Enable Wireless Guest Network 1:	<input type="checkbox"/>	
Guest SSID 1:	Guest01	

Note: It is strongly recommended that you configure wireless security for Guest SSID once you enable it.

Apply Cancel

Advanced Wireless – MAC Filtering

To access MAC Filtering, point to the **Advanced Wireless** on the left window and click **MAC Filtering** submenu, or click the **MAC Filtering** button in the Wireless Settings window.

This page can help you to allow or deny certain MAC addresses to pass through or block out.

Click **Add** at the bottom of the window to enter MAC address.
Click **Apply** at the bottom of the page to add the MAC address to the wireless MAC filtering list.

Select **Enable Wireless MAC Filter** and click the **only ALLOW computers listed to access wireless network** or **only DENY computers listed to access wireless network** of the filtering policy. Click **Apply** to save the settings. Go to **Maintenance -> System** and click **Reboot** to restart the device and let the new settings take effect.

WIRELESS MAC FILTERING

Enter the MAC address and click "Add" to add the MAC address to the wireless MAC address filters.

Wireless MAC Filtering Policy:

Enable Wireless MAC Filtering

Only **ALLOW** computers listed to access wireless network.

Only **DENY** computers listed to access wireless network.

Apply Cancel

WIRELESS MAC FILTERING LIST

MAC Address

Add

Note: Go to [MAINTENANCE -> System](#) and click the Reboot button to restart the device and let your new settings take effect!

Advanced Wireless – Wireless QoS

To access Wireless QoS, point to the **Advanced Wireless** on the left window and click **Wireless QoS** submenu, or click the **Quality of Service** button in the Wireless Settings window.

Select WMM to enable can control the transmitting of voice or video over wireless connection in order to provide better connection quality. Select WMM No Acknowledgement to enable could have more efficient throughout but higher error rates in a noisy Radio Frequency (RF) environment.

Click **Add** at the bottom of the window to see the Add Wireless QoS Classes section. Enter information in the section, and click **Apply**. Click **Apply WMM Settings** to save the settings. Go to **Maintenance -> System** and click **Reboot** to restart the device and let the new settings take effect.

WIRELESS QoS

This page lets you add, remove, enable, and disable wireless QoS.

WMM(WI-FI MULTIMEDIA) SETTINGS

WMM : Disabled ▼

WMM No Acknowledgement : Disabled ▼

Apply WMM Settings

WIRELESS QoS CLASSES

Name	Priority	Protocol	Src. IP/ Netmask	Src. Port	Dest. IP/ Netmask	Dest. Port
Add						

Note: Go to [MAINTENANCE -> System](#) and click the Reboot button to restart the device and let your new settings take effect!

Advanced – Port Forwarding

To access the Port Forwarding window, click the **Port Forwarding** button in the **Advanced** directory. Port Forwarding is used to redirect data to a single PC.

Click the **Add** button to set up a rule as follows.

Enter an IP address in the Private IP field, select a Protocol Type from the drop-down list, enter a range of ports in the Public Start Port and Public End Port fields, and then click the **Apply** button to see the customized rule in the ACTIVE PORT FORWARDING RULES table.

PORT FORWARDING					
This is the ability to open ports in your Router and re-direct data through those ports to a single PC on your network.					
Maximum number of entries which can be configured: 32					
ACTIVE PORT FORWARDING					
Private IP	Protocol Type	Public Start Port	Public End Port	Private Start Port	Connection
<input type="button" value="Add"/>					

Advanced – Port Triggering

To access the Port Triggering window, click the **Port Triggering** button in the **Advanced** directory.

Some applications require that the remote parties open specific ports in the Router's firewall for access. Port Trigger dynamically opens the Open Ports in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using Trigger Ports. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the Open Ports.

Applications such as games, video conferencing, and other remote access applications require that specific ports in the Router's firewall be opened for access by applications.

Click **Add** to see the Add Port Triggering section. You can configure the port settings on this window by clicking the **Select an application** radio button and then using the drop-down list to choose an existing application, or by clicking the **Custom application** radio button and entering your own Application Rule in the field provided. Click **Apply** when you are finished with the port setting configuration. The new Application Rule will appear in the Port Triggering table.

PORT TRIGGERING

Some applications require that the remote parties open specific ports in the Router's firewall for access. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'.

Some applications such as games, video conferencing, remote access applications, and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and clicking "Apply" to add it.

Maximum number of entries which can be configured: 32

PORT TRIGGERING

Application	Trigger		Open			
Name	Protocol	Port Range		Protocol	Port Range	
		Start	End		Start	End
<input type="button" value="Add"/>						

Advanced – DMZ

To access the DMZ (Demilitarized Zone) window, click the **DMZ** button in the **Advanced** directory.

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.

To designate a DMZ IP address, select **Enabled DMZ**, 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, deselect the **Enable DMZ** and click **Apply**. It will be necessary to save the settings and reboot the Router before the DMZ is activated.

DMZ SETTINGS

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the Router. If you have a computer that cannot run Internet applications successfully from behind the Router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

DMZ SETTINGS

Enable DMZ

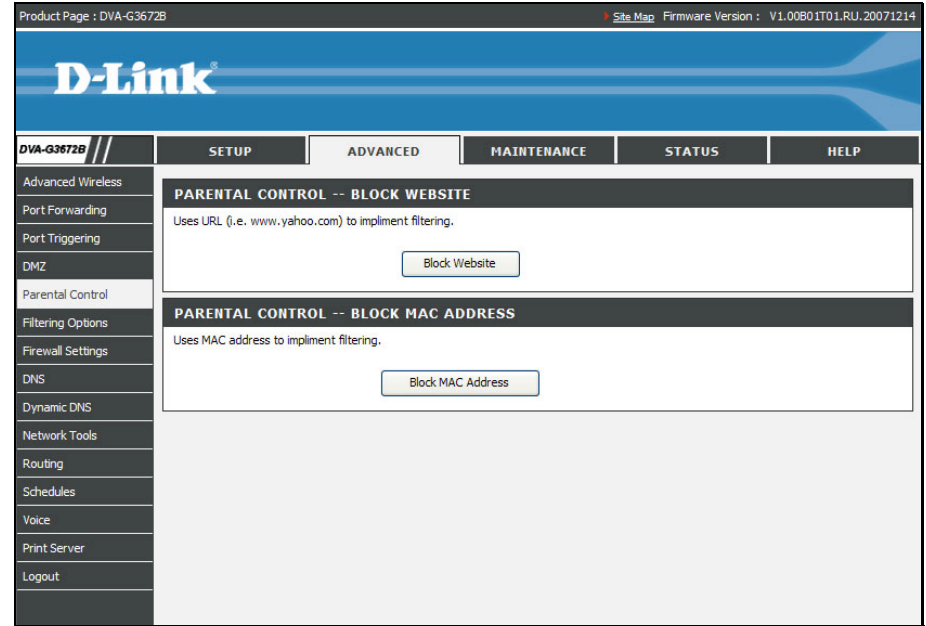
DMZ Host IP Address : <<

Note: Go to [MAINTENANCE -> System](#) and click the **Reboot** button to restart the device and let your new settings take effect!

Advanced – Parental Control

To access the Parent Control window, click the **Parent Control** button in the **Advanced** directory.

It has two subcategories: **Block Website** and **Block MAC Address**. You can either point to the **Parental Control** on the left window and click one of the submenus, or click one of the buttons in the Parental Control window.





Parental Control – Block Website

To access Block Website, point to the **Parental Control** on the left window and click **Block Website** submenu, or click the **Block Website** button in the Parental Control window.

Use this window to deny access to specified websites.

Click **Add** to see the **Add Block Website** section. URL (Uniform Resource Locator) is a specially formatted text string that uniquely defines an Internet website. This section will allow users to block computers on the LAN from accessing certain URLs. This may be accomplished by simply entering the URL to be blocked in the **URL** field.

To configure for URL blocking, enter the website's address into the **URL** field, click **Schedule Rule** or **Manual Schedule** radio button. For Schedule Rule, select a rule in the drop down list. Rules in the list can be configured in **Advanced** -> **Schedules**. For manual Schedule configure as follows. Use the radio buttons to click the desired **Day(s)**, either **All Week** or **Select Day(s)** (in which case you must tick the checkboxes for the desired individual days of the week), select the desired **Start Time** and **End Time** or tick the **All Day – 24 hrs** checkbox, and then click the **Block Website** button. Click the **Apply** button to see the configured URL blocking entry is displayed in the Block Website. To remove a Blocked URL entry in the table, click the corresponding  button. To modify a table entry, click the corresponding  button, make the desired changes, and then click the **Apply** button.

BLOCK WEBSITE

The Block Website allows you to set up a list of websites which users are not allowed to visit. If Block Website is enabled, all the websites in the list will be blocked. Each website in the list is associated with a Schedule Rule which is defined when to enable/disable this function for each website.



BLOCK WEBSITE

URL	Schedule Rule
<input type="button" value="Add"/>	

Parental Control – Block MAC Address

Use this window to deny access to specified MAC address.

Click **Add** to see the **Add Block MAC Address** section. MAC address is a specially formatted text string (xx:xx:xx:xx:xx:xx) that uniquely identification of a device. This section will allow users to block devices with certain MAC addresses on the LAN.

To configure for MAC address blocking, enter the username into the **Username** field, click **Current PC's Mac Address** to have MAC address of current computer, or click **Other MAC Address** and enter a MAC address manually. Click **Schedule Rule** or **Manual Schedule** radio button to configure the time schedule. For Schedule Rule, select a rule in the drop down list. Rules in the list can be configured in **Advanced** -> **Schedules**. For manual Schedule configure as follows. Use the radio buttons to click the desired **Day(s)**, either **All Week** or **Select Day(s)** (in which case you must tick the checkboxes for the desired individual days of the week), select the desired **Start Time** and **End Time** or tick the **All Day – 24 hrs** checkbox, and then click the **Block Website** button. Click the **Apply** button to see the configured URL blocking entry is displayed in the Block Website. To remove a Blocked URL entry in the table, click the corresponding  button. To modify a table entry, click the corresponding  button, make the desired changes, and then click the **Apply** button.

BLOCK MAC ADDRESS

The Block MAC Address allows you to set up a list of MAC addresses of LAN devices which will be restricted to access the Router. If the Block MAC address option is enabled, all the LAN devices with the MAC address in the list will not be allowed to access the Router. Each MAC address in the list is associated with a Schedule Rule which is defined when to enable/disable this function for each MAC address.

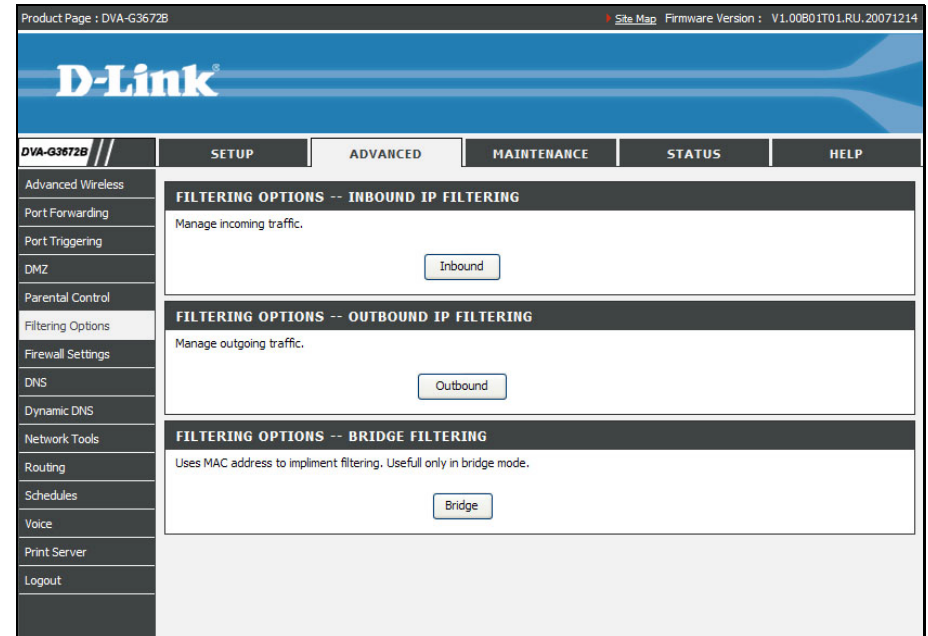
BLOCK MAC ADDRESS

Username	MAC Address	Schedule		
<input type="button" value="Add"/>				

Advanced – Filtering Options

To access the Filtering Options window, click the **Filtering Options** button in the **Advanced** directory.



It has three subcategories: **Inbound Filtering**, **Outbound Filtering** and **Bridge Filtering**. You can either point to the **Filtering Options** on the left window and click one of the submenus, or click one of the buttons in the Filtering Options window.



Filtering Options – Inbound Filtering

To access Inbound Filtering, point to the **Filtering Options** on the left window and click **Inbound Filtering** submenu, or click the **Inbound** button in the Filtering Options window.

The Inbound Filter allows you to create a filter rule to allow incoming IP traffic by specifying a filter name and at least one condition on this window. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. By default, all incoming IP traffic from the Internet is blocked when the firewall is enabled.

Click the **Add** button to see the Add Inbound IP Filtering section, enter the information in the section. Explanations of parameters are described below. Click the **Apply** button to add the entry in the Active Inbound IP Filtering table. To remove an entry in the table, click the corresponding  button. To modify a table entry, click the corresponding  button, make the desired changes, and then click the **Apply** button.

INCOMING IP FILTERING

The Inbound Filter allows you to create Filter Rules to allow the incoming traffic from Internet based on IP range and protocol. Each filter rule is specified by a filter name and at least one condition.

By default, all incoming IP traffic from the Internet is blocked when the firewall is enabled, but some IP traffic can be ACCEPTED by setting up filters.

ACTIVE INBOUND IP FILTERING



Name	Protocol	Source Address	Source Port	Dest. Address	Desc. Port	
<input type="button" value="Add"/>						

Filters Parameter	Description	
Filter Name	Enter a name for the new filter.	
Protocol	Select the transport protocol (TCP and UDP, TCP, UDP, ICMP or Any) that will be used for the filter rule.	
Select IP Range by	Select either IP Address or Netmask to show different items.	
	Source IP Address	Enter the start and end IP address for the range of IP addresses which you are creating the filter rule.
	Source IP Address & Source Subnet Mask	This is the IP address and their associated subnets for which you are creating the filter rule.
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.	
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.	

Filtering Options – Outbound Filtering

To access Outbound Filtering, point to the **Filtering Options** on the left window and click **Outbound Filtering** submenu, or click the **Outbound** button in the Filtering Options window.

The Outbound Filter allows you to create a filter rule to block outgoing IP traffic by specifying a filter name and at least one condition on this window. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Filters are used to allow or deny LAN or WAN users from accessing the Internet or your internal network.

Click the **Add** button to see the Add Outbound IP Filtering section, enter the information in the section. Explanations of parameters are described below. Click the **Apply** button to add the entry in the Active Outbound IP Filtering table. To remove an entry in the table, click the corresponding  button. To modify a table entry, click the corresponding  button, make the desired changes, and then click the **Apply** button.

OUTGOING IP FILTERING

The Outbound Filter allows you to create Filter Rules to deny the outgoing traffic to the Internet based on IP range and protocol. Each filter rule is specified by a filter name and at least one condition.

ACTIVE OUTBOUND IP FILTERING



Name	Protocol	Source Address	Source Port	Dest. Address	Desc. Port
<div style="text-align: right; margin-right: 10px;"> <input type="button" value="Add"/> </div>					

Filters Parameter	Description	
Filter Name	Enter a name for the new filter.	
Protocol	Select the transport protocol (TCP and UDP, TCP, UDP, ICMP or Any) that will be used for the filter rule.	
Select IP Range by	Select either IP Address or Netmask to show different items.	
	Source IP Address	Enter the start and end IP address for the range of IP addresses which you are creating the filter rule.
	Source IP Address & Source Subnet Mask	This is the IP address and their associated subnets for which you are creating the filter rule.
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.	
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.	

Filtering Options – Bridge Filtering

To access Bridge Filtering, point to the **Filtering Options** on the left window and click **Bridge Filtering** submenu, or click the **Bridge** button in the Filtering Options window.

Bridge filters are used to block or allow various types of packets through the WAN/LAN 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 losing the rules that have been configured.

Select Bridge Filtering Global Policy: **ALLOW all packets but DENY those matching any of the specific rules listed** or **DENY all packets but ALLOW those matching any of the specific rules listed** for the rules that configured below. Click the **Add** button to see the Add Bridge Filter section. Select a protocol (PPPoE, IPv4, IPv6, Apple Talk, IPX or IGMP) in the **Protocol Type** list, type in a Source MAC, a Destination MAC or both in the entry fields. Select a direction (LAN=>WAN, WAN=>LAN, or LAN<=>WAN) in the **Frame Direction** list. Click the **Apply** button to add the entry in the Active Bridge Filters table. To remove an entry in the table, click the corresponding  button. To modify a table entry, click the corresponding  button, make the desired changes, and then click the **Apply** button.

BRIDGE FILTERING

Bridge Filtering is only effective on ATM PVCs configured in Bridge mode. **ALLOW** means that all MAC layer frames will be **ALLOWED** except those matching with any of the specified rules in the following table. **DENY** means that all MAC layer frames will be **DENIED** except those matching with any of the specified rules in the following table.

The Active Bridge Filter allow you to Create a filter which is specified by the MAC layer frames and at least one condition. If multiple conditions are specified, all of them will take effect.

Bridge Filtering Global Policy:

ALLOW all packets but **DENY** those matching any of specific rules listed

DENY all packets but **ALLOW** those matching any of specific rules listed

ACTIVE BRIDGE FILTERS

Protocol	Destination MAC	Source MAC	Frame Direction
<input type="button" value="Add"/>			

Advanced – Firewall Settings

To access the Firewall Settings window, click the **Firewall Settings** button in the **Advanced** directory.

This page allows the Router to enforce specific predefined policies intended to protect against certain common types of attacks. Stateful Packet Inspection (SPI) is a packet inspection process that blocks unwanted and unrequested packets trying to reach PCs on your LAN. 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.

When you have selected the desired Firewall settings by ticking the corresponding check boxes for the various types of protection offered on this window, click **Apply**.

FIREWALL SETTINGS

The Router already provides a simple firewall by virtue of the way NAT works. By default NAT does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to Internet cyber-attackers.

FIREWALL SETTINGS

- Enable SPI**
- Enable DOS and Portscan Protection**
 - SYN/TCP reset attack
 - SYN/RST attack
 - SYN/FIN attack
 - Ping/Ping of Death attack
 - FIN/URG/PSH attack
 - Xmas attack
 - Null scanning attack

Apply Cancel

Advanced – DNS

To access the DNS window, click the **DNS** button in the **Advanced** directory.

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).

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 **Obtain DNS server address automatically** option. 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, click the **Use the following DNS server addresses** radio button and enter these IP addresses in the available entry fields for the Preferred DNS Server and the Alternative DNS Server. When you have configured the DNS settings as desired, click the **Apply** button.

The screenshot shows a web-based configuration window for DNS. At the top, there is a blue header with the text "DNS". Below this, a grey box contains the text "DNS server is used for translating a URL to an IP address." The main section is titled "DNS SERVER CONFIGURATION" in a dark grey header. It contains two radio button options: "Obtain DNS server address automatically" (which is selected) and "Use the following DNS server addresses". Under the second option, there are two input fields: "Preferred DNS Server" with the value "168.95.1.1" and "Alternate DNS Server" which is empty. At the bottom right of the window, there are two buttons: "Apply" and "Cancel".

Advanced – Dynamic DNS

To access the Dynamic DNS window, click the **Dynamic DNS** button in the **Advanced** directory.

The Router supports DDNS (Dynamic Domain Name Service). The Dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specified host from various locations on the Internet. This is enabled to allow remote access to a host by clicking a hyperlinked URL in the form hostname.dyndns.org. Many ISPs assign public IP addresses using DHCP, this can make it difficult to locate a specific host on the LAN using standard DNS. If for example you are running a public web server or VPN server on your LAN, this ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be setup with one of the supported DDNS providers.

Click **Add** to see the Add DDNS Settings section. Enter the required DDNS information, click the **Apply** button to see the entry in the Dynamic DNS List table. To remove an entry in the table, click the corresponding  button. To modify a table entry, click the corresponding  button, make the desired changes, and then click the **Apply** button.

DYNAMIC DNS

This page allows you to add a Dynamic DNS address.

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

DYNAMIC DNS LIST

Server Address	Hostname	Username or E-mail	Interface
<input type="button" value="Add"/>			

Advanced – Network Tools

To access the Network Tools window, click the **Network Tools** button in the **Advanced** directory. It has six subcategories: **Port Mapping**, **IGMP**, **QoS**, **UPnP**, **ADSL** and **SNMP**.

You can either point to the **Network Tools** on the left window and click one of the submenus, or click one of the buttons in the Network Tools window.

The screenshot shows the D-Link DVA-G3672B Advanced Network Tools configuration page. The page is titled "D-Link" and "DVA-G3672B //". The top navigation bar includes "SETUP", "ADVANCED", "MAINTENANCE", "STATUS", and "HELP". The left sidebar lists various configuration options, with "Network Tools" selected. The main content area displays six subcategories of Network Tools, each with a description and a button to access the configuration page:

- NETWORK TOOLS -- PORT MAPPING**: Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. Button: Port Mapping
- NETWORK TOOLS -- IGMP**: Transmission of identical content, such as multimedia, from a source to a number of recipients. Button: IGMP
- NETWORK TOOLS -- QoS**: Allows you to manually configure special routes that your network might need. Button: QoS
- NETWORK TOOLS -- UPnP**: Allows you to configure UPnP. Button: UPnP
- NETWORK TOOLS -- ADSL**: Allows you to configure Default Gateway used by WAN Interface. Button: ADSL
- NETWORK TOOLS -- SNMP**: Allows you to configure SNMP (Simple Network Management Protocol). Button: SNMP

Network Tools – Port Mapping

To access Port Mapping, point to the **Network Tools** on the left window and click **Port Mapping** submenu, or click the **Port Mapping** button in the Network Tools window.

Tick the **Enable Port Mapping** check box and select a PVC and its Priority assigning to the specific LAN port or wireless LAN. Click **Apply** to take effect.

PORT MAPPING

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network.

PORT MAPPING

Enable Port Mapping

LAN	Port Mapping PVC	Priority
Port 1	▼	Low ▼
Port 2	▼	Low ▼
Port 3	▼	Low ▼
Port 4	▼	Low ▼

Please set configuration for wireless port based QoS.

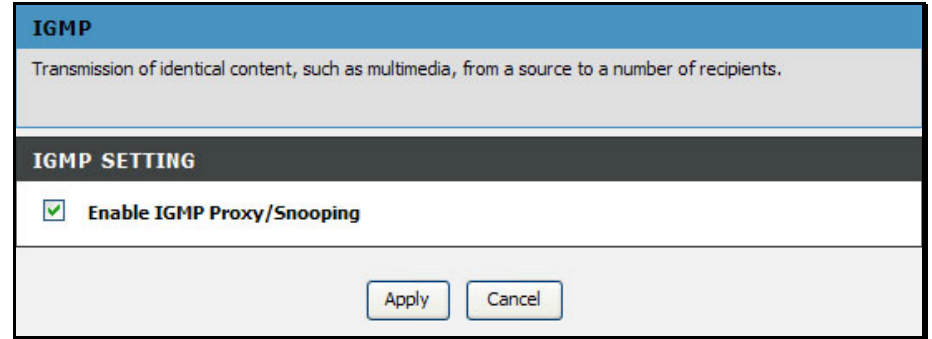
Wireless	▼
----------	---

Network Tools – IGMP

To access IGMP, point to the **Network Tools** on the left window and click **IGMP** submenu, or click the **IGMP** button in the Network Tools window.

IGMP (Internet Group Management Protocol) page is for identical content transmission.

When the **Enable IGMP Proxy/Snooping** check box is selected, Multicast packets are allowed to pass in both directions on the WAN interface. Most users will want to leave this on.



Network Tools – QoS

To access QoS, point to the **Network Tools** on the left window and click **QoS** submenu, or click the **QoS** button in the Network Tools window.

QoS or Quality of Service allows your Router to help prioritize the data packet flow in your Router and network. This is very important for time sensitive applications such as VoIP where it may help prevent dropped calls. Large amounts of non-critical data can be scaled so as not to affect these prioritized sensitive real-time programs.

Select one of the PVC connections for QoS. The Router allows you to manually configure Upstream Rate Limit or Classification Control. Tick **Enable Upstream Rate Limit** and select a number in the **Bandwidth** list to control the transmission rate. Tick the **Enable Classification Control** check box and you can choose ToS, Application or User Define classifications. The information in the table below the selection differs based on the classifications you select.

Tick the **Enable** check box for each queue configured and enter information in the corresponding fields. Some experimentation may be necessary to achieve the optimum results with your particular ISP's connection. When you are finished, click **Apply**. Go to **Maintenance -> System**, and click the **Reboot** button to let your new settings take effect.

QoS

You can set the Quality of Service on this web page. This should improve performance of Internet applications like games, video, voice, etc.

IP QoS

Please set configuration for IP based QoS.

PVC : PVCO ▼

Enable Upstream Rate Limit
 Bandwidth : 64 (kbps)

Enable Classification Control
 Classification : ToS ▼

Enable	Weight	Range (0~7)
<input type="checkbox"/>	0 %	0 ~ 0
<input type="checkbox"/>	0 %	0 ~ 0
<input type="checkbox"/>	0 %	0 ~ 0
<input type="checkbox"/>	0 %	0 ~ 0

Note: Go to [MAINTENANCE -> System](#) and click the Reboot button to restart the device and let your new settings take effect!

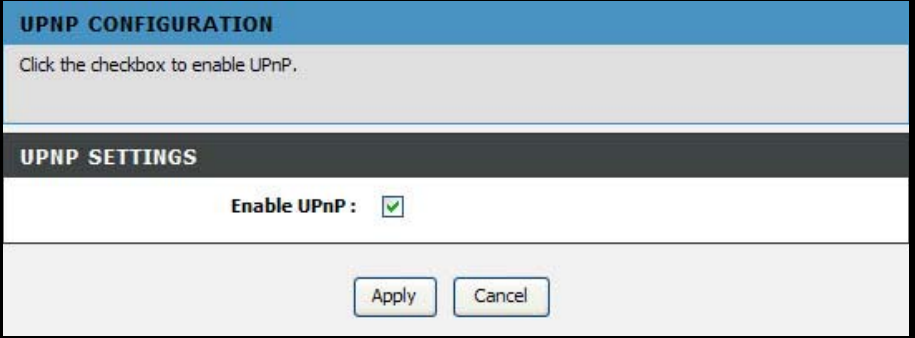
Apply
Cancel

Network Tools – UPnP

To access UPnP, point to the **Network Tools** on the left window and click **UPnP** submenu, or click the **UPnP** button in the Network Tools window.

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 is a protocol supported by diverse networking media including Ethernet, Firewire, phone line, and power line networking.

To enable UPnP for any available connection, tick the Enable UPnP check box, and click the **Apply** button.



UPNP CONFIGURATION

Click the checkbox to enable UPnP.

UPNP SETTINGS

Enable UPnP:

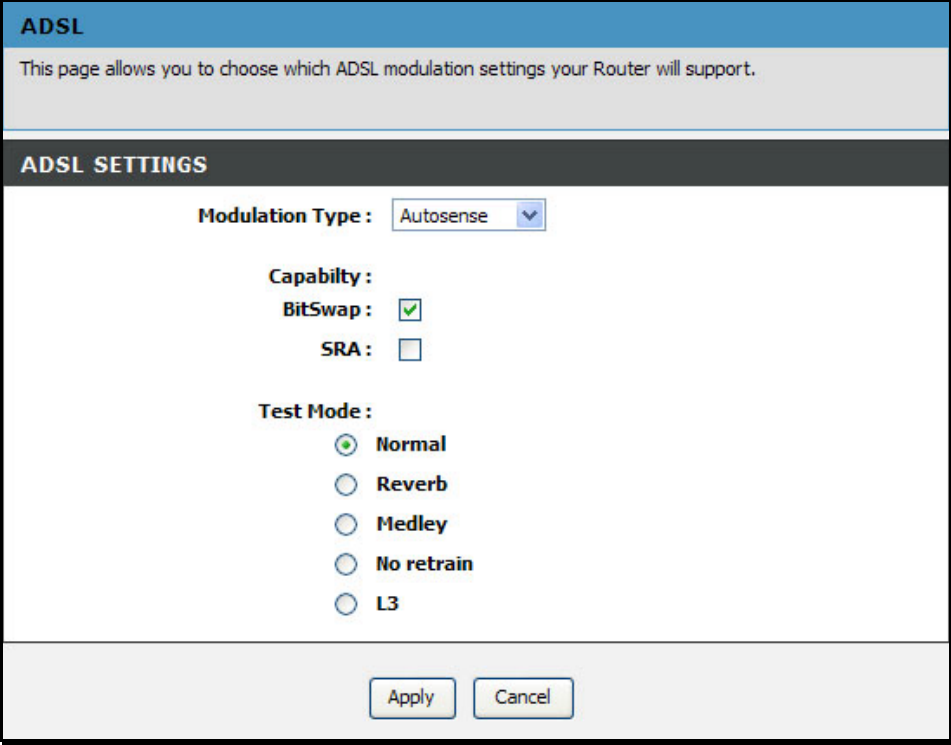
Apply Cancel

Network Tools – ADSL

To access ADSL, point to the **Network Tools** on the left window and click **ADSL** submenu, or click the **ADSL** button in the Network Tools window.

This window allows the user to set the configuration for ADSL protocols. For most ADSL accounts the default settings *Autosense* 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 from the **Modulation Type** drop-down list and click the **Apply** button.

Leave the Capability and Test Mode settings unchanged unless otherwise instructed by your ISP. Both BitSwap Enable and Seamless Rate Adaption (SRA) Enable deal with tests that determine the line condition between your Router and the ISP's Central office.



The screenshot shows the ADSL configuration interface. At the top, there is a blue header with the text "ADSL". Below the header, a grey box contains the text: "This page allows you to choose which ADSL modulation settings your Router will support." Underneath this is a dark grey section titled "ADSL SETTINGS". The main configuration area is white and contains the following settings:

- Modulation Type :** A dropdown menu currently set to "Autosense".
- Capability :**
 - BitSwap :** A checked checkbox.
 - SRA :** An unchecked checkbox.
- Test Mode :** A list of radio buttons with "Normal" selected.
 - Normal
 - Reverb
 - Medley
 - No retrain
 - L3

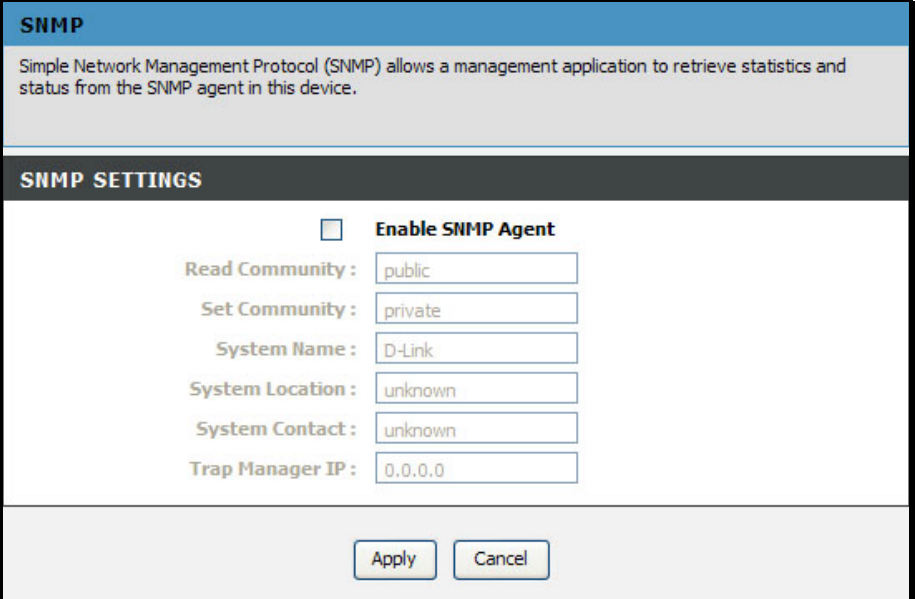
At the bottom of the window, there are two buttons: "Apply" and "Cancel".

Network Tools – SNMP

To access SNMP, point to the **Network Tools** on the left window and click **SNMP** submenu, or click the **SNMP** button in the Network Tools window.

Simple Network Management Protocol is a standard for internetwork and intranetwork management.

Tick the **Enable SNMP Agent** check box and configure the parameters for SNMP on this window and then click the **Apply** button.

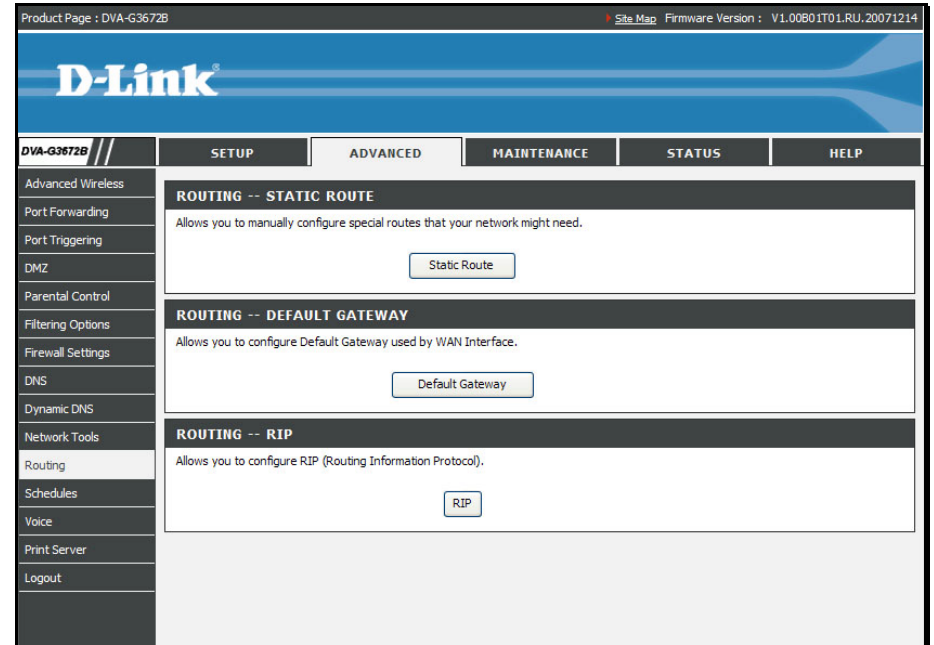


The image shows a configuration window titled "SNMP". At the top, there is a blue header with the text "SNMP". Below the header, a grey box contains the text: "Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device." Below this is a dark grey section titled "SNMP SETTINGS". In this section, there is a checkbox labeled "Enable SNMP Agent" which is currently unchecked. Below the checkbox are several input fields: "Read Community:" with the value "public", "Set Community:" with the value "private", "System Name:" with the value "D-Link", "System Location:" with the value "unknown", "System Contact:" with the value "unknown", and "Trap Manager IP:" with the value "0.0.0.0". At the bottom of the window, there are two buttons: "Apply" and "Cancel".

Advanced –Routing

To access the Routing window, click the **Routing** button in the **Advanced** directory.

It has three subcategories: **Static Route**, **Default Gateway** and **RIP**. You can either point to the **Routing** on the left window and click one of the submenus, or click one of the buttons in the Routing window.





Routing – Static Route

To access Static Route, point to the **Routing** on the left window and click **Static Route** submenu, or click the **Static Route** button in the Routing window.

The page allows you to manually enter the routing table.

To define a gateway and hop to route data traffic, complete the fields in the Add Static Route section. Click **Apply** to see the entry in the Active Static Route table. Go to **Maintenance -> System** and click **Reboot** to restart the device and let your changes take effect.

To add a static route to a specific destination IP, click **Add** to see the Add Static Route section. Enter a **Destination** IP address, **Netmask** and Gateway's IP address. Select a PVC in the **Connection** drop-down list. Click **Apply** to see the entry in the Active Static Route table. Go to **Maintenance -> System** and click **Reboot** to restart the device and let your changes take effect. To remove an entry in the table, click the corresponding  button. To modify a table entry, click the corresponding  button, make the desired changes, and then click the **Apply** button.

STATIC ROUTE

This page allows you to add a specific route interface. If you are not familiar with these Advanced Network settings, please read the help section.

ACTIVE STATIC ROUTE

Destination	Netmask	Gateway	Connection

Note: Go to [MAINTENANCE -> System](#) and click the Reboot button to restart the device and let your new settings take effect!