

Routing – Default Gateway

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

This page can either automatically assign a default gateway to the device or manually type in a default gateway or the device or interface. It is recommended to leave **Enable Automatic Assigned Default Gateway** ticked to automatically detect the Gateway IP address.

ROUTING -- DEFAULT GATEWAY

Default gateway is the default connection interface. This allows connection to the Internet by a default gateway. Basically, the Router will auto assign it, however, you also may set it by yourself.

DEFAULT GATEWAY

Enable Automatic Assigned Default Gateway

Use Default Gateway IP Address :

Use Interface :

Routing – RIP

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

The Router supports RIP version 1 and 2 used to share routing tables with other Layer 3 routing devices on your local network or remote LAN. The Operation setting refers to the RIP request. Select *Active* to allow RIP requests from other devices. Select *Passive* to instruct the Router to make RIP requests for routing tables from other devices.

To enable RIP, tick the **Enable Global RTP Mode** check box, select the Version (1, 2, or Both) and Operation (*Active* or *Passive*), and tick the Enable check box in the corresponding entry. Click the **Apply** button. Go to **Maintenance -> System** and click **Reboot** to restart the device and let your changes take effect.

RIP SYSTEM WIDE CONFIGURATION

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line.

ROUTING -- RIP CONFIGURATION

Enable Global RIP Mode

Interface	VPI/VCI	Version	Operation	Enable
br0	N/A	2 <input type="button" value="v"/>	Active <input type="button" value="v"/>	<input type="checkbox"/>
ppp_0_8_35_1	8/35	1 <input type="button" value="v"/>	Active <input type="button" value="v"/>	<input type="checkbox"/>

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

Advanced – Schedules

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

You can add schedules in this page and then apply them to Parental Control.

Click **Add** to see the Add Schedule Rule section. Enter a Name for the schedule. 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. Click **Apply** to see the entry in the Schedule Rule 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.

SCHEDULE

Schedule allows you to create scheduling rules to be applied for your firewall and Parental Control.

SCHEDULE RULE

Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	Stop Time		
<input type="button" value="Add"/>											

Advanced – Voice

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

You can set up the basic VoIP settings in this page. All information in this page should be obtained by your ISP.

Voice over Internet Protocol (VoIP) is a protocol that can transmit the voice through the Internet. Session Initiation Protocol (SIP) is a widely used signaling protocol of VoIP. To start using the VoIP service, select an interface in the Interface list for the VoIP service, and enter the Primary SIP Server IP and Primary SIP Server Port. The Secondary SIP Server, Outbound Proxy IP, Stun Server and SIP Service Domain are optional. Tick **Enable T38 Fax** for sending fax data through the network. Tick **Enable VAD** to disable silent packet and send other transmission. Select a DTMF type (Inband, RFC2833 or SIP Info) in the **DTMF relay** drop-down list. Tick one of forwarding call methods for All, No Answer or Busy calls, and then type a number that calls is forwarded to. Select a routing rule of the PSTN line (auto, Line1 or Line2) in the **PSTN Routing** drop-down list. Enter digits in the **PSTN Dialplan** field for transferring VoIP service to PSTN service.

You can also set up the codec priorities in Codec Settings section. In VoIP Setting section, you can configure the user name and password for registering to SIP VoIP service.

Click the **Apply** button, and go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.

VOICE SETTING

Voice settings allow you to set up the configuration for the SIP VoIP service. All this information should be provided by the service provider. The Primary SIP server IP and port number are mandatory, and the Secondary server and Stunt server are optional. PSTN Dialplan allows you to set up a prefix number. If you dial this number, the telephone line will be switching from VoIP to PSTN.

VOICE SETTINGS

Interface :	lan <input type="button" value="v"/>
Primary SIP Server IP :	<input type="text" value="192.168.1.1"/>
Primary SIP Server Port :	<input type="text" value="5060"/>
Secondary SIP Server IP :	<input type="text" value="0.0.0.0"/>
Secondary SIP Server Port :	<input type="text" value="5060"/>
Outbound Proxy IP :	<input type="text" value="0.0.0.0"/>
Outbound Proxy Port :	<input type="text" value="5060"/>
Stun Server IP :	<input type="text" value="0.0.0.0"/>
Stun Server Port :	<input type="text" value="3478"/>
SIP Service Domain :	<input type="text"/>
Locale selection :	NORTH_AMERICA <input type="button" value="v"/>
Enable T38 Fax :	<input checked="" type="checkbox"/>
Enable VAD :	<input checked="" type="checkbox"/>
DTMF relay :	INBAND <input type="button" value="v"/>
TX Gain :	0 dB <input type="button" value="v"/>
RX Gain :	0 dB <input type="button" value="v"/>
Call Forwarding :	<input type="checkbox"/> All <input type="checkbox"/> No Answer <input type="checkbox"/> Busy
Forwarding Number :	<input type="text"/>
PSTN Routing :	auto <input type="button" value="v"/>
PSTN Dialplan :	<input type="text"/>
Session Timer :	<input type="text" value="3600"/>

Advanced –Print Server

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

Tick the **Enable on-board print server** check box, enter a Printer Name and Model name in the fields, and click **Apply** to enable the printer server function.

The screenshot shows a web-based configuration window titled "PRINT SERVER SETTINGS". At the top, a blue header bar contains the title. Below the header, a light gray box contains the text: "This page allows you to enable / disable printer support." The main content area has a dark gray header bar with the title "PRINT SERVER SETTINGS". Below this, there is a checked checkbox labeled "Enable on-board print server". Underneath, there are two text input fields: "Printer Name" with the value "g3672b" and "Make and Model" with the value "DLink Print Server". At the bottom of the form, there are two buttons: "Apply" and "Cancel".

Maintenance – System

To access the System window, click the **System** button in the **Maintenance** directory.

When you configure the Router, you will need to restart the Router to take the settings effect. Click **Reboot** to restart the Router.

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 **Backup Settings** button. You will be prompted to select a location on your computer to put the file. The file type is bin 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 **Upload Settings** button to load the settings from your local hard drive. Confirm that you want to load the file when prompted. The Router will reboot and begin operating with the configuration settings that have just been loaded.

To reset the Router to its factory default settings, click the **Restore Default Settings** button. You will be prompted to confirm your decision to reset the Router. The Router will reboot with the factory default settings including IP settings (192.168.1.1) and Administrator password (admin).

The screenshot displays the D-Link web interface for the DVA-G3672B router. The top navigation bar includes 'Product Page : DVA-G3672B', 'Site Map', and 'Firmware Version : V1.0080IT01.RU.20071214'. The main menu has tabs for 'DVA-G3672B', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The 'MAINTENANCE' tab is selected, and the 'System' sub-tab is active. The left sidebar lists navigation options: System, Firmware Update, Access Controls, Diagnostics, System Log, and Logout. The main content area is titled 'SYSTEM SETTINGS' and contains the following sections:

- SYSTEM SETTINGS**: A text box stating, 'The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by the device can be uploaded into the unit.'
- SYSTEM -- REBOOT**: A text box stating, 'Click the reboot button to restart the device and let your new settings take effect!' with a 'Reboot' button below it.
- SYSTEM -- BACKUP SETTINGS**: A text box stating, 'Backup DSL Router configurations. You may save your Router configurations to a file on your PC. Note: Please always save the configuration file before viewing it.' with a 'Backup Settings' button below it.
- SYSTEM -- UPDATE SETTINGS**: A text box stating, 'Update DSL Router settings. You may update your Router settings using your saved files.' It includes a 'Settings File Name:' label, an input field, a 'Browse...' button, and an 'Update Settings' button below it.
- SYSTEM -- RESTORE DEFAULT SETTINGS**: A text box stating, 'Restore DSL Router settings to the factory defaults.' with a 'Restore Default Settings' button below it.

On the right side, there is a 'Helpful Hints...' section with text: 'The system page allows you to reboot your Router, as well as restore it to the factory default. You can also backup your settings at a point when you have completed all your changes. If you ever need to automatically reconfigure your Router, you can then use the saved file to restore to your favored settings automatically.' and a 'More...' link.

Maintenance – Firmware Update

To access the Firmware Update window, click the **Firmware Update** button in the **Maintenance** directory.

Use the Firmware Upgrade menu to load the latest firmware for the Router. Note that the Router configuration settings may return to the factory default settings, so make sure you save the configuration settings with the System menu described above. To upgrade firmware obtained from your ISP, click the **Browse** button to search for the file. Click the **Update Firmware** button to begin copying the file. The file will load and restart the Router automatically.

FIRMWARE UPDATE

Step 1: Obtain an updated firmware image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Firmware" button once to upload the new image file.

NOTE: The process will take about 2 minutes to complete, and your DSL Router will be rebooted. Please DO NOT power off your device before the process is completed.

FIRMWARE UPDATE

Current Firmware Version : V1.00B01T01.RU.20071214

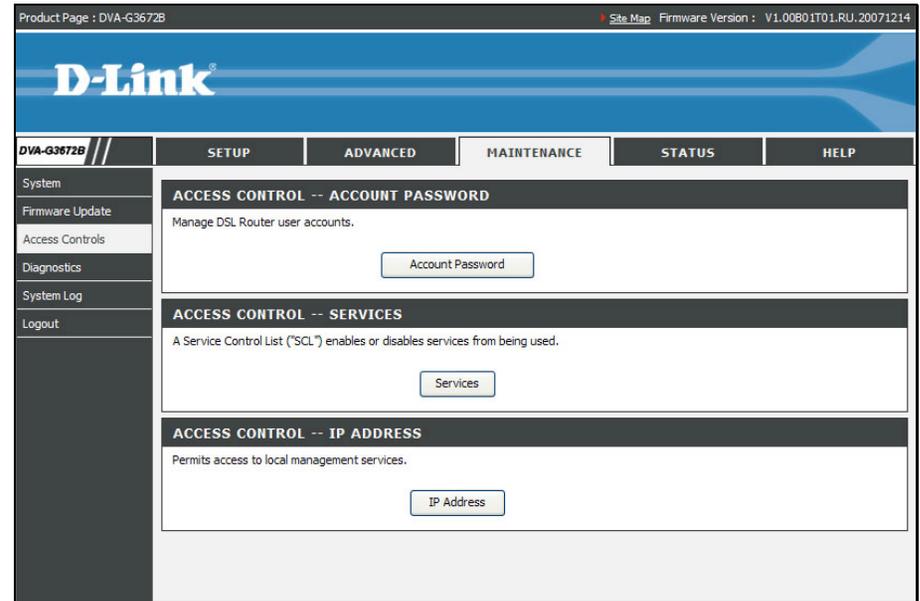
Current Firmware Date : Dec 14 2007

Firmware File Name :

Maintenance – Access Controls

To access the Access Controls window, click the **Access Controls** button in the **Maintenance** directory.

In this page, you can choose to change password, manage the service control or IP address control.



Access Controls – Account Password

To access Account Password, point to the **Access Controls** on the left window and click **Account Password** submenu, or click the **Account Password** button in the Access Controls window.

There are three different user names for different purpose. Support is for remote supporter to login from WAN and is able to adjust TR-069 settings. User and Admin is to login from LAN. Select a user name (Admin, User or Support), type the Current Password in the first field, the New Password in the second field, and enter the password again in the Confirm Password field to be certain you have typed it correctly.

You can configure the idle time between 5 and 30 minutes for the webpage asking you to logout. Click the **Apply** button. Go to **Maintenance -> System** and click **Reboot** to restart the device.

ACCOUNT PASSWORD

The 'admin', 'support', and 'user' accounts can access the management interface. The admin and support accounts have read/write access and can change passwords, while the user account has read-only access.

ADMINISTRATOR SETTINGS

Username :

Current Password :

New Password :

Confirm Password :

Login session times out if idle for minutes. (5~30)

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

Access Controls – Services

To access Services, point to the **Access Controls** on the left window and click **Services** submenu, or click the **Services** button in the Access Controls window.

This page lists out all the available services including Telnet, FTP, HTTP, ICMP, SNMP, SSH and TFTP that can enable at LAN, WAN or both. Tick to enable the services, or deselect to disable them.

Service	LAN	WAN
Telnet	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
FTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
HTTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
ICMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
SNMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
SSH	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
TFTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled

Access Controls – IP Address

To access IP Address, point to the **Access Controls** on the left window and click **IP Address** submenu, or click the **IP Address** button in the Access Controls window.

Click **Add** to see the Add IP Address section. Enter an IP address and click **Apply** in the section. The IP address will show in the table in the Remote Web and Telnet Management section. Tick the **Enable Access Control Mode** check box and click **Apply** in this section to enable the function.

The IP Address Access Control mode, if enabled, permits access to local management services from IP address contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Enter the IP address of the management station permitted to access the local management services, and click 'Apply.'

This is for Remote Web and Telnet Management.

Enable Access Control Mode

IP Address

Maintenance – Diagnostics

To access the Diagnostics window, click the **Diagnostics** button in the **Maintenance** directory.

This window is used to test connectivity of the Router. A Ping test may be done through the local or external interface to test connectivity to known IP addresses. The diagnostics feature executes a series of tests of your system software and hardware connections. Use this window when working with your ISP to troubleshoot problems.

DIAGNOSTIC TEST

The diagnostics feature executes a series of tests for your system software and hardware connections. Use this function to examine the connections between the Router and your ISP to troubleshoot problems.

WAN Connection : PVC0 ▾ Test With OAM F5 Test With OAM F4

TESTING CONNECTIVITY TO MODEM

Testing Ethernet Connection	PASS
Testing Wireless Connection	PASS

TESTING ADSL CONNECTION

Testing ADSL Synchronization	FAIL
------------------------------	-------------

TESTING NETWORK CONNECTION

Testing ATM OAM F5 Segment Ping	FAIL
Testing ATM OAM F5 End to End Ping	FAIL

TESTING INTERNET CONNECTIVITY

Test PPP Server Session	FAIL
Test Authentication with ISP	FAIL
Ping Default Gateway	FAIL
Ping Primary Domain Names Server	FAIL
Ping Primary Domain Names Server	FAIL

Maintenance – System Log

To access the System Log window, click the **System Log** button in the **Maintenance** directory.

The system log allows you to configure local and remote logging, and to view the logs that have been created.

To generate a system log, tick the **Enable Remote Log** check box. Select the **Log Level** and **Display Level** from the drop-down lists. The levels available are the same for each type of level: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debugging. Click the **Apply** button to allow your new settings to take effect.

SYSTEM LOG

The system Log allows you to configure local, remote, and email logging, and to view the logs that have been created.

REMOTE LOG SETTINGS

Enable Remote Log

Log Level : Debugging

Display Level : Error

Mode : Local

Apply Cancel View System Logs

Status – Device Info

Use the Device Information window to quickly view basic current information about the Wireless, WAN and local network interfaces, and device information including Model Name, Time and Date, and Firmware.

Product Page : DVA-G3672B Site Map Firmware Version : V1.00801T01.RU.20071214

D-Link

DVA-G3672B // SETUP ADVANCED MAINTENANCE STATUS HELP

Device Info

Wireless Clients

DHCP Clients

Logs

Statistics

Routing Info

Logout

Helpful Hints...

All of your device's Information, WLAN, WAN, and LAN status, and details are shown here.

Details include firmware version, Modem MAC address, Default gateway, WLAN SSID, WLAN security type, Modem IP, etc.

[More..](#)

DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

SYSTEM INFO

Model Name: DVA-G3672B

Time and Date: Jan 01, 2000 23:16:04

Firmware Version: V1.00801T01.RU.20071214

INTERNET INFO

WAN Connection: Pvc0 (Auto PVC)

Internet Connection Status: **ADSL LINK DOWN**

Internet Connection Up Time: 0 hours, 0 minutes, 0 seconds

Downstream Line Rate (Kbps):

Upstream Line Rate (Kbps):

Enabled WAN Connections :

Name	VPI/VCI	Connection Type	Firewall	NAT	IGMP	QoS	IP Address
PVC 0	8/35	PPPoE LLC	Enabled	Enabled	Enabled	Disabled	N/A

Default Gateway: N/A

Preferred DNS Server: N/A

Alternate DNS Server: N/A

WIRELESS INFO

MAC Address: 00:50:BA:11:22:3D

Status: Enabled

Network Name (SSID): D-Link DVA-G3672B

Visibility: Visible

Security Mode: open

LOCAL NETWORK INFO

Status – Wireless Clients

To access the Wireless Clients window, click the **Wireless Clients** button in the **Status** directory.

The Wireless Clients window lists out the active Wireless connection when the Wireless function is on.

WIRELESS MANAGEMENT		
The page shows the associated stations.		
ASSOCIATED STATIONS		
BSSID	Associated	Authorized
<input type="button" value="Refresh"/>		

Status – DHCP Clients

To access the DHCP Clients window, click the **DHCP Clients** button in the **Status** directory.

The Connected LAN Clients list displays active DHCP clients when the Router is acting as a DHCP server.

DHCP CLIENTS		
This page shows all the currently connected wireless and LAN computers or PCs.		
CONNECTED LAN CLIENTS		
Host Name	MAC Address	IP Address
No DHCP Clients Available		
<input type="button" value="Refresh"/>		

Status – Logs

To access the Logs window, click the **Logs** button in the **Status** directory.

This page displays the event logs of the Router. Click **Clear Log** to delete all the records. Click **Save Log** to save the records as a *.sys file.

VIEW LOG

Use this option to view the Router logs. You can define what types of events you want to view and the event levels to view.

LOG FILES

[First Page](#) [Last Page](#) [Previous](#) [Next](#) [Clear Log](#) [Save Log](#)

Page 1 Of 1

Time	Message
Jan 1 21:15:07	kernel: eth1 Link DOWN.
Jan 1 21:15:09	kernel: eth1 Link UP.
Jan 1 23:09:12	kernel: OAM loopback response not received on PORT/VPI/VCI 0/8/35.
Jan 1 23:09:14	kernel: OAM loopback response not received on PORT/VPI/VCI 0/8/35.

Status – Statistics

To access the Statistics window, click the **Statistics** button in the **Status** directory.

Use this window to monitor traffic on the Local Network & Wireless, Internet or ADSL connections. This window also displays information concerning ADSL status.

TRAFFIC STATISTICS

Traffic Statistics display Receive and Transmit packets passing through the Device.

LOCAL NETWORK & WIRELESS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	1821783	17852	0	0	743377	16246	0	0
Wireless	0	0	0	0	409288	4880	0	0

INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
nas_0_8_35	8/35	PPPoE	0	0	0	0	0	0	0	0

ADSL

Mode:	Autosense	
Type:	Fast	
Line Coding:	Trellis	
Status:	DOWN	
	Downstream	Upstream
SNR Margin (dB):	0.0	0.0
Attenuation (dB):	0.0	0.0
Output Power (dBm):	N/A	N/A
Attainable Rate (Kbps):	0	0
Rate (Kbps):		
D (interleaver depth):	0	0
Delay (msec):	0	0
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total ES:	0	0

Status – Routing Info

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

This page displays all the routing rules information.

ROUTE TABLE

Routing table is used to direct forwarding by matching destination addresses to the network paths used to reach them.

ROUTING TABLE LISTS

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0

Help

To access the Help window, click the **Help** directory.

The screenshot displays a web-based help menu with the following structure:

- HELP MENU**
 - [SETUP](#)
 - [ADVANCED](#)
 - [MAINTENANCE](#)
 - [STATUS](#)
- SETUP HELP**
 - [Wizard](#)
 - [Internet Setup](#)
 - [Wireless Settings](#)
 - [Wireless Basics](#)
 - [Wireless Security](#)
 - [Local Network](#)
 - [Time and Date](#)
- ADVANCED HELP**
 - [Advanced Wireless](#)
 - [Advanced Settings](#)
 - [MAC Filtering](#)
 - [Wireless QoS](#)
 - [Port Forwarding](#)
 - [Port Triggering](#)
 - [DMZ](#)
 - [Parental Control](#)
 - [Block Website](#)
 - [Block MAC Address](#)
 - [Filtering Options](#)
 - [Inbound Filtering](#)
 - [Outbound Filtering](#)
 - [Bridge Filtering](#)
 - [Firewall Settings](#)
 - [DNS](#)
 - [Dynamic DNS](#)
 - [Network Tools](#)
 - [Port Mapping](#)
 - [IGMP](#)
 - [QoS](#)
 - [UPnP](#)
 - [ADSL](#)
 - [SNMP](#)
 - [Routing](#)
 - [Static Route](#)
 - [Default Gateway](#)
 - [RIP](#)
 - [Schedules](#)
 - [Voice](#)
- MAINTENANCE HELP**
 - [System](#)
 - [Firmware Update](#)
 - [Access Control](#)
 - [Account Password](#)
 - [Services](#)
 - [IP Address](#)
 - [Diagnostics](#)
 - [System Log](#)
- STATUS HELP**
 - [Device Info](#)
 - [Wireless Clients](#)
 - [DHCP Clients](#)
 - [Logs](#)
 - [Statistics](#)
 - [Routing Info](#)

FCC Notices

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

CAUTION: Change or modification not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance."