Wireless

DSL Modem

Model #: GT724WGR

User Manual

Ver 1.0
# Table of Contents

1 Introduction 1
   Minimum System Requirements 1
   Features 2
   Getting to Know the Modem 3

2 Performing a Quick Setup 7
   Accessing Quick Setup Screens 7
   Changing the Password 9

3 Viewing the Modem’s Status 11
   Broadband Connection Status 11
   Network Status 14

4 Configuring Wireless Settings 15
   Accessing Wireless Setup 15
   Basic Wireless Setup 17
   Wireless Advanced Settings 17
   Wireless Status 23

5 Configuring Advanced Setup Options 25
   Accessing the Advanced Setup Options 25
   DSL Settings 27
   DHCP Settings 28
   LAN IP Address 30
   WAN IP Address 31
   QoS Settings Upstream 33
   QoS Settings Downstream 35
   QoS Status 36
   Remote Management 36
   Telnet Timeout Setting 37
   Dynamic Routing 38
   Static Routing 38
   UPnP (Universal Plug and Play) 39
   Time Zone 39
   Remote Syslog Capture 40
6 Configuring Security Settings 41
  Accessing Wired Security Screens 41
  Admin User Name and Password 42
  Firewall 43
  Port Forwarding 47
  DMZ Hosting 49
  NAT (Network Address Translation) 50

7 Configuring Internet Access Controls 51
  Accessing Internet Access Control Screens 51
  Services Blocking 52
  Website Blocking 53
  Schedule Rules 54

8 Configuring the Modem’s Utilities 57
  Accessing the Utilities Screens 57
  Restore Default Settings 59
  Upgrade Firmware 59
  Web Activity Log 60
  System Log 61
  OAM Ping Test 62
  Ping Test 62
  Reboot 63

9 Troubleshooting 65
  Troubleshooting 65
  Frequently Asked Questions 67

A Specifications 73
  General 73
  Wireless Operating Range 74
  LED Indicators 74
  Environmental 74

B Setting up Static IP on a Computer 75
  Windows 2000 75
  Windows XP 80
  Windows Vista 83

C Service Acronyms 87
  Service Acronym Definitions 87

D Glossary 91

Notices 95
  Regulatory Compliance Notices 95
  Modifications 95

Limited Warranty 97
Introduction

Thank you for purchasing the Actiontec Wireless DSL Modem. The Modem is the simplest way to connect computers to a high-speed broadband connection. This easy-to-use product is perfect for the home office or small business. If you want to take your computing to the next level, the Wireless DSL Modem is sure to be one of the keys to your success.

Minimum System Requirements

- Active DSL service
- Computer with a 10 Mbps or 10/100 Mbps Ethernet connection
- Microsoft Windows 2000, XP, Vista
  Mac OS 7.1+, 8.0+, 9.0+, OS X+
- Internet Explorer 4.0 or higher (5.x+ recommended) or Netscape Navigator 4.0 or higher (4.7+ recommended)
- TCP/IP network protocol installed on each computer
Features

- ADSL WAN port (RJ-11)
- Full-rate ANSI T1.413 Issue 2, ITU G.992.1 (G.dmt) and G.992.2 (G.lite) standard compliance
- Auto-handshake for different ADSL services
- Bridged Ethernet over ATM, PPP over ATM, PPP over Ethernet
- Precise ATM traffic shaping
- IP packet routing and transparent bridge
- RIP-1, RIP-2, and static routing protocol support
- Built-in NAT, DHCP server
- DNS relay support
- PAP/CHAP authentication, administrative passwords through Telnet
- 64-, 128-, and 256-bit WEP/WPA wireless LAN security
- IEEE 802.3 Ethernet standard compliance
- 10/100 Base-T Ethernet ports (4)
- Fast Ethernet flow control support
- Web-based configuration setup
- FTP firmware upgradeable
- Web download support
- 802.11b/g support
Getting to Know the Modem

This section contains a quick description of the Modem’s lights, ports, etc. The Modem has several indicator lights (LEDs) on its front panel and a series of ports on its rear panel.

Front Panel

The front panel of the Modem features eight lights: Power, DSL, Internet, Ethernet (4), and Wireless.

![Modem Front Panel Diagram]

**Power Light**

The Power light displays the Modem’s current status. If the Power light glows steadily green, the Modem is receiving power and fully operational. When the Power light is rapidly flashing, the Modem is initializing. If the Power light glows red when the Power cord is plugged in, the Modem has suffered a critical error and technical support should be contacted.

**DSL Light**

The DSL light illuminates when the Modem is connected to a DSL line and the unit is able to synchronize to the DSL signal from the ISP. When it flashes, the Modem’s built-in DSL modem is training for the DSL service.
Internet Light
When the Internet light glows steadily, the Modem is connected to the DSL provider.

Ethernet Lights
The Ethernet lights illuminate when the Modem is connected to one or more computers via its yellow Ethernet ports.

Wireless Light
The Wireless light illuminates when the Modem’s wireless radio is turned on.

Rear Panel
The rear panel of the Modem contains six ports (Ethernet [4], Line, and Power), as well as Reset and Power switches.

Ethernet Ports
The Ethernet ports are used to connect computers to the Modem via Ethernet cable. The Ethernet ports are 10/100 Mbps auto-sensing ports, and either a straight-through or crossover Ethernet cable can be used when connecting to the ports.

Line Port
The Line port is used to connect the Modem to a DSL (Digital Subscriber Line) connection.
Chapter 1 Introduction

Reset Switch
Depressing the Reset switch restores the Modem’s factory default settings. To reset the Modem, depress and hold the Reset switch for five to seven seconds. The reset process will start after releasing the switch, during which the Power light will turn from green to orange.

Power Port
The Power port is used to connect the Power cord to the Modem.

⚠️ Warning: Do not unplug the Power cord from the Modem during the reset process. Doing so may result in permanent damage to the Modem.

Power Switch
The Power switch is used to power the Modem on and off.
This page left intentionally blank.
Performing a Quick Setup

This chapter is a guide through a quick set up of the Modem, including how to connect the Modem to the ISP.

To complete the quick setup, have the Welcome Letter or ISP Worksheet handy. If the document is not available, contact the ISP immediately.

Accessing Quick Setup Screens

To access the Quick Setup screens:

1. Open a Web browser. In the “Address” text box, type: http://192.168.0.1 then press Enter on the keyboard.

3. Follow the instructions in the “Welcome to the Quick Setup” screen, then click Next.

4. At the top of the next window, select the type of connection used by the ISP.

4a. If PPPoA or PPPoE was selected in step 4, the default user name and password are entered in the appropriate text boxes. If “RFC1483 via DHCP” was selected, go to step 5.
5. Click **Apply** at the bottom of the screen.

6. Read the instructions on the next screen. The Modem is successfully configured.

The Power light flashes rapidly while the Modem restarts, then glows steadily green when fully operational. The Internet light will also glow steadily green. The Modem is now configured and users can start surfing the Internet.

If an error appears, stating the Web browser was unable to connect to the Internet, check the configuration settings. Ensure all the information required by the ISP is entered correctly.

### Changing the Password

To create or change the password allowing access to the Modem’s Web Configuration screens, follow these instructions:

1. From the “Home” screen, select **Security**.

2. The “Security” screen appears. Select “Admin User Name and Password.”

3. The “Change Admin Username/Password” screen appears. Enter a new Username in the “Admin User Name” text box, then enter a new password in the “Admin Password” text box. Make sure to write down the user name and password and keep it in a secure location. They will be needed to access the Modem’s Web Configuration screens in the future.
4. Click **Apply** at the bottom of the screen.

5. Read the instructions on the next screen. The user name and password are successfully changed.

Once the Modem has rebooted, the new user name and password are active. To access the Modem’s Web Configuration screens, the new user name and password must be entered.
Viewing the Modem’s Status

After configuring the Modem, the Modem’s connection and network status can be viewed. The Internet connection status is viewed in the “Broadband Connection Status” screen, while the network status is viewed in the “My Network” screen.

**Broadband Connection Status**

To view the Modem’s connection statistics, select **Status** from the strip of icons at the top of any Gateway GUI screen. The “Broadband Connection Status” screen appears. There are three sections in this screen: General Statistics, PPP Status, and DSL Status.

⚠️ **Note:** No settings (other than connecting or disconnecting from the Internet by clicking on **Connect** or **Disconnect**) can be changed from the Broadband Connection Status screen.

**General Statistics**

The top section of the Broadband Connection Status screen displays general statistics regarding the Modem, including model number, firmware version, IP address, and gateway IP address.

<table>
<thead>
<tr>
<th>Broadband Connection Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model:</td>
</tr>
<tr>
<td>Firmware Version:</td>
</tr>
<tr>
<td>Gateway MAC Address:</td>
</tr>
<tr>
<td>WAN IP Address:</td>
</tr>
<tr>
<td>Subnet Mask:</td>
</tr>
<tr>
<td>Gateway IP Address:</td>
</tr>
<tr>
<td>DNS Address #1:</td>
</tr>
<tr>
<td>DNS Address #2:</td>
</tr>
</tbody>
</table>
**PPP Status**

The middle section of the Broadband Connection Status screen displays the status of the Modem’s PPP connection, including user name, authentication failures, and packets sent and received.

```
<table>
<thead>
<tr>
<th>PPP Status</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status:</td>
<td>Not Connected</td>
</tr>
<tr>
<td>User Name:</td>
<td></td>
</tr>
<tr>
<td>LCP State:</td>
<td>down</td>
</tr>
<tr>
<td>IPCP State:</td>
<td>down</td>
</tr>
<tr>
<td>Authentication Failures:</td>
<td></td>
</tr>
<tr>
<td>Session Time:</td>
<td>0</td>
</tr>
<tr>
<td>Packets Sent:</td>
<td></td>
</tr>
<tr>
<td>Packets Received:</td>
<td></td>
</tr>
</tbody>
</table>
```

**DSL Status**

The bottom section of the Broadband Connection Status screen displays the status of the Modem’s DSL connection, including mode settings, connection status, and number of discarded packets. Click **Reset** to refresh all statistics on this screen.

```
<table>
<thead>
<tr>
<th>DSL Status</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VPI:</td>
<td>0</td>
</tr>
<tr>
<td>VCI:</td>
<td>35</td>
</tr>
<tr>
<td>DSL Mode Setting:</td>
<td>HHMODE</td>
</tr>
<tr>
<td>DSL Negotiated Mode:</td>
<td>NOT TRAINED</td>
</tr>
<tr>
<td>Connection Status:</td>
<td>Idle</td>
</tr>
<tr>
<td>Speed (down/up):</td>
<td>0 / 0 kbps</td>
</tr>
<tr>
<td>ATM QoS class:</td>
<td>UBR</td>
</tr>
<tr>
<td>Near End CRC Errors:</td>
<td>0 / 0</td>
</tr>
<tr>
<td>Far End CRC Errors:</td>
<td>0 / 0</td>
</tr>
<tr>
<td>Near End CRC(Within last 30 mins):</td>
<td>0 / 0</td>
</tr>
<tr>
<td>Far End CRC(Within last 30 mins):</td>
<td>0 / 0</td>
</tr>
<tr>
<td>Near End RS FEC:</td>
<td>0 / 0</td>
</tr>
<tr>
<td>Far End RS FEC:</td>
<td>0 / 0</td>
</tr>
<tr>
<td>Near End FEC(Within last 30 mins):</td>
<td>0 / 0</td>
</tr>
<tr>
<td>Far End FEC(Within last 30 mins):</td>
<td>0 / 0</td>
</tr>
<tr>
<td>Discarded Packets(Within last 30 mins):</td>
<td>0</td>
</tr>
<tr>
<td>SNR Margin (Downstream/Upstream):</td>
<td>0 / 0</td>
</tr>
<tr>
<td>Attenuation (Downstream/Upstream):</td>
<td>0 / 0</td>
</tr>
</tbody>
</table>
```
In the menu on the left side of the Broadband Connection Status screen, there are two other options available to view: NAT Table and Routing Table. Click to generate the option of choice.

**NAT Table**

Selecting **NAT Table** generates the “NAT Table” screen. This screen displays an overview of the current list of open connections through NAT (Network Address Translation) the Modem supports between the networked computers and the Internet.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Timeout</th>
<th>SRC IP</th>
<th>SRC Port</th>
<th>DST IP</th>
<th>DST Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Routing Table**

Selecting **Routing Table** generates the “Routing Table” screen. This screen displays an overview of the Modem’s network routes.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Valid</th>
<th>Destination</th>
<th>Netmask</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>192.168.0.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>192.168.0.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>
Network Status

To view the Modem’s network status, select My Network from the strip of icons at the top of any Modem GUI screen. The “My Network” screen appears, listing all devices connected to the network. From this screen, various settings can be accessed, including Website blocking, Schedule Rules, and Enable Application.

![Diagram of network status with options]

To view the network status of a particular device, click View Device Details for the device. An overview of the device's network status appears.

![Device status overview]

**DAD-MOM PC**
- IP Address: 192.168.1.2
- IP Address Allocation: DHCP
- Hardware Address: 00:0E:0D:11:11:11
Configuring Wireless Settings

This chapter explains how to set up the Modem’s wireless network capabilities, including setting up wireless security and viewing the wireless connection status.

Accessing Wireless Setup

To access the Wireless Settings configuration screens, follow these instructions:

1. Open a Web browser. In the “Address” text box, type: 
   \[ \text{http://192.168.0.1} \]
   then press \textbf{Enter} on the keyboard.

2. The Main screen appears. Click \textbf{Wireless Setup}.
3. A login window appears. Enter the user name and password in the appropriate text boxes, then click OK.

Note: The default user name is “admin.” The default password is “password.”

4. The “Wireless Basic Settings” screen appears, which guides the user through a basic set up of the Modem’s wireless networking capabilities.
Chapter 4 Configuring Wireless Settings

Basic Wireless Setup
To perform a basic setup of a wireless network using the Modem:

1. In the “Wireless Basic Settings” screen, turn the Modem’s wireless radio on by selecting On.

2. Create a name for the wireless network and enter it in the “ESSID” text box.

3. Select a channel from the “Channel” drop-down menu. In the United States, use channels 1-11.

4. Activate WPA-PSK (Wi-Fi Protected Access w/ Pre-Shared Key) to secure the wireless network by selecting WPA-PSK.

5. Enter eight alphanumeric characters in the “Pre-Shared Key (PSK) for Home Network” text box.

6. Click Save to save the wireless settings.

Wireless Advanced Settings
To access the Modem’s wireless advanced settings screens, select Advanced Settings from the menu on the left side of the “Wireless Basic Settings” screen.

<table>
<thead>
<tr>
<th>Wireless Advanced Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1</strong>: Securing your wireless traffic as it transmits through the air.</td>
</tr>
<tr>
<td>OFF</td>
</tr>
<tr>
<td>WPA (allows you to enable a pre-shared key for a local network or more advanced security for an enterprise network)</td>
</tr>
<tr>
<td>WEP (Recommended)</td>
</tr>
<tr>
<td>WEP + 802.1x (For enterprise networks only)</td>
</tr>
</tbody>
</table>

| **Level 2**: Stop your DSL Gateway from broadcasting your Wireless Network Name (ESSID) |
| ESSID Broadcast (Allows you to prevent users who do not know your ESSID name to access your DSL Gateway wirelessly.) |

| **Level 3**: Limit access to certain wireless devices |
| Wireless MAC Authentication (Allows you to limit access to your wireless network by allowing only those devices with specific MAC addresses.) |

<table>
<thead>
<tr>
<th>Other Advanced Wireless Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b/g Mode (Allows you to limit access to your wireless network based on the type of technology.)</td>
</tr>
</tbody>
</table>

This generates the “Wireless Advanced Settings” screen. In this screen, the security of the wireless network can be activated and fortified.
Wireless Security

The first section of the Wireless Advanced Settings screen involves wireless security (securing wireless traffic as it transmits through the air). The Modem offers three types of wireless security: WPA WEP, and WEP+802.1x.

WPA

Activating WPA (Wi-Fi Protected Access) in the Wireless Advanced Settings screen generates the “Wireless WPA Settings” screen.

There are two levels of WPA. “Pre-Shared Key (PSK) for Home Network” is for home network security. To set up a PSK (Pre-Shared Key), enter 8-63 alphanumeric characters in the text box. All wireless-enabled devices must support WPA and know the PSK to join the network.

The “Group Key Interval,” “Server IP Address,” “Port,” and “Secret” text boxes are enterprise network specific, and should only be accessed by an information systems professional. See “WEP+802.1x” on the previous page for more information.

When finished with this screen, click Apply to save all changes. To return to the Wireless Advanced Settings screen, click Back.
Chapter 4 Configuring Wireless Settings

WEP
Selecting WEP in the Wireless Advanced Settings screen generates the “WEP Key” screen. Here, the authentication type, encryption level, and WEP keys are entered to activate WEP (Wired Equivalent Privacy) security encryption for the wireless network.

![WEP Key Screen]

**Authentication Type** - There are three authentication types: Open, Shared, and Both. Open authentication allows any wireless-enabled device to recognize the network, even if the WEP key is invalid. Shared allows only wireless-enabled devices with the correct WEP key to recognize the network.

**64-bit WEP** - 64-bit WEP requires one or more keys, each key comprising five hexadecimal pairs. One key (Key 1) is automatically generated by the Modem at start-up, based on the Modem’s MAC address. This key is also displayed on a sticker on the bottom of the Modem. A hexadecimal digit consists of an alphanumeric character ranging from 0-9 or A-F. An example of a 64-bit WEP key is: 4E-A3-3D-68-72. To create a new set of 64-bit WEP keys, activate one or more keys by clicking in the appropriate circles, then enter five hexadecimal digit pairs in each activated Key text box (Key 1-, Key 2-, Key 3-, Key 4-). After activating 64-bit WEP, a computer with wireless capability can join the network only if these same keys are entered in the computer’s wireless encryption scheme.

**128-bit WEP** - 128-bit WEP requires one or more keys, each key comprising 13 hexadecimal pairs. A hexadecimal digit consists of an alphanumeric character ranging from 0-9 or A-F. An example of a 128-bit WEP key is: 3D-44-FE-6C-A1-EF-2E-D3-C4-21-74-5D-B1. To create a 128-bit WEP key, activate Key 1 by clicking in the appropriate circle, select “128 bit” from the drop-down list on the right, then enter 13 hexadecimal digit pairs in the Key text box. After activating 128-bit, a computer with wireless capability can join the network only if this key is entered in the computer’s wireless encryption scheme.
**256-bit WEP** - 256-bit WEP requires one or more keys, each key comprising 29 hexadecimal pairs. A hexadecimal digit consists of an alphanumeric character ranging from 0-9 or A-F. To create a 256-bit WEP key, activate Key 1 by clicking in the appropriate circle, select “256 bit” from the drop-down list on the right, then enter 29 hexadecimal digit pairs in the Key text box. After activating 256-bit WEP, a computer with wireless capability can join the network only if this key is entered in the computer’s wireless encryption scheme.

**Note:** Not all wireless PC Cards support 128- or 256-bit WEP. Ensure all PC Cards installed in the networked computers support 128- or 256-bit WEP before activating.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

**WEP+802.1x**

Activating **WEP+802.1x** in the Wireless Advanced Settings screen generates the “WEP+802.1x” screen. This setting is for enterprise networks only, and should be accessed by an experienced information systems specialist.

![WEP+802.1x](image)

To set up WEP+802.1x security, enter the IP address of the RADIUS server in the “Server IP Address” text box, and the “Secret” key (for communication between the RADIUS server and the Modem) in the “Secret” text box. The “Port” and “Group Key Interval” values should remain the same.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.
Chapter 4 Configuring Wireless Settings

ESSID Broadcast

Selecting **ESSID Broadcast** in the Wireless Advanced Settings screen generates the “ESSID Broadcast” screen.

To prevent unwanted computers from joining the Modem’s wireless network by using an ESSID of “Any,” select **Disable** in the ESSID Broadcast screen. To broadcast the wireless network’s ESSID, select **Enable**.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

Wireless MAC Authentication

Selecting **Wireless MAC Authentication** in the Wireless Advanced Settings screen generates the “Wireless MAC Authentication” screen.
This feature allows the user to control the wireless LAN network by denying or allowing wireless access by specifying the MAC address of the wireless client(s) allowed or denied access on the wireless network. To do this, follow the instructions on-screen.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

### 802.11b/g Mode

Selecting **802.11b/g Mode** in the Wireless Advanced Settings screen generates the “802.11b/g Mode” screen.

Access to the Modem’s network can be restricted to wireless clients using either the 802.11b or 802.11g wireless adapters. Click on the down arrow next to the drop-down menu and select the desired option. We recommend using the “Mixed” mode (the default option), which enables both 802.11b and 802.11g wireless clients to join the network.

**Note:** If Mixed is chosen and 802.11b wireless clients join the network, some 802.11g wireless clients may connect at 802.11b speeds (11 Mbps) to accommodate the slower adapters.

When finished with this screen, click **Apply** to save all changes.
Wireless Status

To view the Modem’s wireless status and settings, select **Wireless Status** from the menu on the left side of the “Wireless Basic Settings” screen.

![Wireless Status Screen]

The “Wireless Status” screen appears, which displays all of the settings of the Modem’s wireless network settings.
This page left intentionally blank.
Configuring Advanced Setup Options

This chapter explains how to configure the Modem’s advanced setup options, such as Remote Management, DHCP settings, and Quality of Service (QoS).

Accessing the Advanced Setup Options

To access the “Advanced Setup” options, follow these instructions:

1. Open a Web browser. In the “Address” text box, type:
   
   `http://192.168.0.1`

   then press Enter on the keyboard.
2. The Main screen appears. Click Advanced Setup.

![Advanced Setup Screen](image)

3. A login window appears. Enter the user name and password in the appropriate text boxes, then click OK.

![Login Window](image)

☞ Note: The default user name is “admin.” The default password is “password.”
4. The “Advanced Setup” screen appears. To modify a specific configuration, click on its name in the menu bar on the left, or from the list in the middle of the screen.

**DSL Settings**

To access DSL Settings, select DSL Settings from the “Advanced Setup” screen. The Modem’s VPI, VCI, Mode, and QoS (Quality of Service) settings can be changed from this screen. We recommend not changing these values without first consulting the ISP.
DHCP Settings

Selecting **DHCP Settings** in the “Advanced Setup” screen generates the “DHCP Settings” screen. The Modem has a built-in DHCP (Dynamic Host Configuration Protocol) server that automatically assigns a different IP address to each computer on the network, eliminating IP address conflicts.

The factory default setting is **On**. To disable the DHCP Server, select **Off**, then click **Apply**.

We strongly recommend leaving the DHCP Server option **On**. If the DHCP Server option is **Off**, ensure the IP addresses of the networked computers are on the same subnet as the IP address of the Modem. For more information, see “DHCP Server Configuration.”

**DHCP Server Configuration**

Clicking in the check box labeled “I would like to adjust the DHCP server settings” activates the text boxes at the bottom of the DHCP Settings screen. Change the IP address range and DNS server information in these text boxes.

**Beginning IP Address**

This is the IP address at which the DHCP server starts assigning IP addresses. We recommend keeping the factory default setting (192.168.0.2).
Ending IP Address
This is the IP address at which the DHCP server stops assigning IP addresses. We recommend keeping the factory default settings (192.168.0.254).

The beginning and ending IP addresses define the IP address range of the Modem. If the default values are left intact, the Modem supplies a unique IP address between 192.168.0.2 and 192.168.0.254 to each computer on the network. Note that the first three groups of numbers of the addresses are identical; this means they are on the same subnet. The IP address of the Modem must be on the same subnet as the IP address range it generates. For instance, if the Modem’s IP address is changed to 10.33.222.1, set the beginning IP address to 10.33.222.2, and the ending IP address to 10.33.222.254.

Subnet Mask
Enter the IP address of the DHCP server’s subnet mask here.

Lease Time
This value represents the amount of time (in seconds) the DHCP server holds onto a specific IP address.

Domain Name
This is the domain name provided by the ISP. If the ISP provided domain name information, enter it here. If not, leave the text box intact.

DNS (Dynamic or Static)
This is the type of DNS server provided by the ISP. If ISP provided DNS server information, select the type here. If not, leave as is.

DNS Server 1
This is the primary DNS server provided by the ISP. If the ISP provided DNS server information, enter it here. If not, leave the text box intact.
**DNS Server 2**

This is the secondary DNS provided by the ISP. If the ISP provided secondary DNS server information, enter it here. If not, leave the text box intact.

When finished in this screen, click **Apply** to activate any changes made.

---

**LAN IP Address**

Selecting **LAN IP Address** in the “Advanced Setup” screen causes a warning screen to appear.

Read the on-screen warning, then click **Yes** to continue.

The “LAN IP Address” screen appears.

The values in the “Modem IP Address” and “Modem Subnet Mask” text boxes are the IP and subnet mask address of the Modem as seen on the network. These values can be modified for your LAN network, but we recommend keeping the default factory settings (IP address 192.168.0.1; subnet mask address 255.255.255.0).

**Note:** If the Modem’s LAN IP Address is modified, verify that the DHCP Server range is within the same subnet. For more information, see “DHCP Server Configuration.”

When finished in this screen, click **Apply** to activate any changes made.
Chapter 5 Configuring Advanced Setup Options

WAN IP Address

Selecting WAN IP Address in the “Advanced Setup” screen causes a warning screen to appear.

Read the on-screen warning, then click Yes to continue.

The “WAN IP Address” screen appears.
WAN IP Address allows manual set up of the IP address of the Modem. To do this:

*Note:* Some DSL providers use PPPoE to establish communication with an end user. Other types of broadband Internet connections (such as fixed point wireless) may use either DHCP or static IP address. If unsure which connection is present, check with the ISP before continuing.

1. Select the type of connection the ISP uses. If PPP Auto Connect is being used, click in the appropriate check box.

2. If using PPPoA or PPPoE was selected in step 1, enter the user name and password in the appropriate text boxes. If the ISP requires no user name or password, click in the “My ISP does not require a username and password” check box.

3. Select the IP type. If “Single Static IP Address” was selected, enter the IP address in the “Single Static IP” text box. If “Block of Static IP Addresses” was selected, enter the designated gateway IP address and subnet mask address in the “Modem Address” and “Subnet Mask” text boxes, respectively. Also, “VIP Mode” can be activated by clicking in the appropriate check box.

4. Select the DNS type. If static DNS address was selected, enter the primary DNS address and, optionally, the secondary DNS address in the appropriate text boxes.

When finished in this screen, click **Apply** to activate any changes made.
QoS Settings Upstream

Selecting QoS Settings Upstream from the “Advanced Setup” screen causes the “QoS Upstream Settings” screen to appear.

QoS (Quality of Service) allows the prioritization of certain types of data traffic (such as VoIP traffic) over other types of traffic (such as standard data). Both upstream (data coming into the network) and downstream (data going out of the network) traffic can be prioritized using QoS.

Enable QoS

Clicking in this check box activates/deactivates QoS.

Trusted Mode

If “Trusted Mode” is activated, all data traffic set to an IP precedence level of 5 will be recognized as high priority traffic, regardless of IP or MAC address rule settings (used for VoIP only).
Total Available Bandwidth
Displays the total amount of available bandwidth (in kilobits per second).

High Priority Bandwidth
Enter the amount of high priority bandwidth to be used by the prioritized traffic type (cannot exceed total available bandwidth).

Priority
Always set to “High” and cannot be changed.

Protocol
Select the data type being configured. Options: TCP, UDP, ICMP.

Source
Identify the source device here, using the device’s IP or MAC address, then enter appropriate value in text box. If IP is used, enter the netmask address, if applicable. A priority port range can also be defined, using the “Port Range” text boxes.

Destination
Identify the destination device here, using the device’s IP address, then enter appropriate value in text box. Enter the netmask address, if applicable. A priority port range can also be defined, using the “Port Range” text boxes.

Rule List
After finishing the configuration of the QoS settings, click Add to save the settings in the Rule List menu box. This collection of QoS settings can then be reused at a future time. If deleting a QoS rule list, highlight it, then click Remove.

When finished, click Apply to activate any changes made.
Chapter 5 Configuring Advanced Setup Options

QoS Settings Downstream


The “QoS Downstream Settings” screen is identical to the “QoS Upstream Settings” screen, with the exception of the “Trusted Mode” and “Set IP Precedence” options. Use this screen to configure QoS for data going out of the network.

When finished in this screen, click Apply to activate any changes made.
QoS Status

Selecting **QoS Status** from the “Advanced Setup” screen causes the “QoS Status” screen to appear. This screen displays the status of QoS upstream and downstream traffic, and differentiates both streams into high priority and normal priority traffic.

**Remote Management**

Selecting **Remote Management** in the “Advanced Setup” screen generates the “Remote Management” screen. Remote management allows access to the Modem through the Internet via another computer. The Modem will be vulnerable to other users on the Internet if Remote Management is activated.

To access the Modem remotely:

1. Enter a user name and password in the appropriate text boxes.
2. Enter a port number through which the Modem will be accessed. Port 80 is the default port number.
Chapter 5 Configuring Advanced Setup Options

3. Activate Remote Management by selecting the appropriate **On** radio button.

4. Write down the WAN IP address of the Modem (see “WAN IP Address”).

5. On a computer outside of the network, open a Web browser and enter the Modem’s WAN IP address in the Address text box. The Modem’s Home screen (or a password prompt, if a password has been set) appears in the browser window.

   **Note:** If the default port (80) of the Modem has been changed, the user may need to enter the WAN IP, a colon (:) and the new port number. For example, if the WAN IP is 71.251.176.63, and the port has been changed to 8081, enter **http://71.251.176.63:8081** to remotely access the Modem.

When finished in this screen, click **Apply** to activate any changes made.

---

**Telnet Timeout Setting**

Selecting **Telnet Timeout Setting** in the “Advanced Setup” screen generates the “Telnet Timeout Setting” screen. Select a period of time from the choices available, and the Telnet session will automatically terminate at that time. If no automatic termination is needed, select “No idle disconnect timeout.”

![Telnet Timeout Setting](image)

When finished in this screen, click **Apply** to activate any changes made.
Dynamic Routing

Selecting Dynamic Routing in the “Advanced Setup” screen generates the “Dynamic Routing” screen.

If another gateway or router is set up behind the Modem in the network configuration, consult the documentation that came with the Gateway or Router to see what kind of Dynamic Routing is required, then select the needed option.

When finished in this screen, click Apply to activate any changes made.

Static Routing

Selecting Static Routing in the “Advanced Setup” screen generates the “Static Routing” screen. Enter the static route addresses in their respective text boxes, then click Add. The address will appear in the “Static Routing Table.” To remove an address, highlight it by clicking on it in the Static Routing Table, then click Remove.

When finished in this screen, click Apply to activate any changes made.
**Chapter 5 Configuring Advanced Setup Options**

**UPnP (Universal Plug and Play)**

Selecting UPnP in the “Advanced Setup” screen generates the “UPnP” screen. In this screen, the Universal Plug and Play option is turned on or off by activating the appropriate circle.

![UPnP Screen]

Universal Plug and Play is a zero-configuration networking protocol that allows hardware and software (such as Netmeeting) to operate more efficiently. If Netmeeting is not running properly, activate UPnP.

**Note:** Activating UPnP presents a slight security risk. After finishing with the hardware or software using UPnP, we recommend deactivating UPnP.

When finished in this screen, click **Apply** to activate any changes made.

---

**Time Zone**

Selecting Time Zone in the “Configuring the Advanced Settings” screen generates the “Time Zone” screen. In this screen, select the time zone in which the Modem is being used. Click in the “Day Light Saving” check box if Daylight Saving Time is currently in effect where the Modem is being used.

![Time Zone Screen]

When finished in this screen, click **Apply** to activate any changes made.
Remote Syslog Capture

Selecting **Remote Syslog Capture** in the “Advanced Setup” screen generates the “Remote Syslog Capture” screen. In this screen, the user can configure the Modem to allow a remote computer to access the Modem’s system activity logs.

When finished in this screen, click **Apply** to activate any changes made.
Configuring Security Settings

This chapter explains how to configure the Modem’s wired security capabilities, including firewall settings, DMZ hosting, and network address translation.

Accessing Wired Security Screens

To access the Wired Security configuration screens, follow these instructions:

1. Open a Web browser. In the “Address” text box, type:
   http://192.168.0.1
   then press Enter on the keyboard.

3. A login window appears. Enter the user name and password in the appropriate text boxes, then click OK.

Note: The default user name is “admin.” The default password is “password.”

4. The “Security” screen appears. To modify a specific configuration, click on its name in the menu bar on the left, or from the list in the middle of the screen.

Admin User Name and Password
See “Changing the Password” on page 9.
Firewall

Selecting Firewall in the Security screen generates the “Firewall Settings” screen. Select the level of security needed for the network.

Note: If VPN connections need to made through the Modem, the Firewall must be set to Off. No VPN connections can be made if the Firewall setting is at Custom, High, Medium, or Low. Also note that DMZ hosting, Port Forwarding, and Application Level Modem settings are active only when the Firewall is Off.

Custom

If Custom is selected in the “Firewall Security Level” screen, the user can select which of the services listed in the window can pass through the firewall (both in and out) the services listed at the bottom of the screen. Remember that checking a box opens the service; a blank check box indicates that the service is blocked. Only experienced network administrators should select and use the Custom Firewall option.
**High**

If **High** is selected in the “Firewall Security Level” screen, the services with a check mark beside them will remain open (either incoming, outgoing, or both, depending on the checkmarks), as shown in the figure below. These settings can be modified to customize the firewall settings.

![Firewall Settings Table]

When finished with this screen, click **Apply** to save the changes.
Medium

If Medium is selected in the “Firewall Security Level” screen, the services with a check mark beside them will remain (either incoming, outgoing, or both, depending on the checkmarks), as shown in the figure below. These settings can be modified to customize the firewall settings.

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>In</th>
<th>Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>20,21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TELNET</td>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NNTP</td>
<td>119</td>
<td></td>
<td></td>
</tr>
<tr>
<td>REAL A/V</td>
<td>7000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS23</td>
<td>1720</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TFTP</td>
<td>1600</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMAP</td>
<td>143</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP/0</td>
<td>443</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMAP/0</td>
<td>993</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POP3/0</td>
<td>995</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When finished with this screen, click Apply to save the changes.
Low

If **Low** is selected in the “Firewall Security Level” screen, the services with a check mark beside them will remain open (either incoming, outgoing, or both, depending on the checkmarks), as shown in the figure below. These settings can be modified to customize the firewall settings.

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>In</th>
<th>Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>20.21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TELNET</td>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NNTP</td>
<td>119</td>
<td></td>
<td></td>
</tr>
<tr>
<td>REAL A/V</td>
<td>7070</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M122</td>
<td>122</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T120</td>
<td>1503</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSMTP</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMAP</td>
<td>143</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP7</td>
<td>993</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POP30</td>
<td>995</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Figure: Firewall Settings]

Note: If a check appears in a box, that service is open (or allowed). An empty box signifies the service is closed (or blocked).

Off

If **Off** is selected in the “Firewall Security Level” screen, firewall filtering is based solely on the basic NAT firewall. At this setting, VPN connections can be made, and DMZ hosting, Port Forwarding, and Application Level Modem settings are active.

*Note: See “Service Acronyms,” for a description of the services listed in the Firewall Security Level screens.*
Port Forwarding

Selecting Port Forwarding in the Security screen generates the “Port Forwarding” screen.

This screen allows certain programs to bypass the Modem’s built-in firewall, allowing access to parts of the network (for hosting a Web or ftp server, for example). To use, select the name of a computer on the network from the “PC Name” drop-down list, then click Add. Next, select a “Category” by clicking the appropriate radio button. In the “Available Rules” list box, select a game, application, server, etc., then click Add>>. The selected item appears in the “Applied Rules” list box. Repeat for each item needed.

To remove an item from the Applied Rules list, highlight it, then click Remove.

To view an item’s rules (forwarded ports, etc.), highlight it, then click View Rule. When finished with this screen, click Apply to save the changes.

Note: Port Forwarding is active only when the Firewall is set to Off.
Rule Management

To create a custom set of rules, click the “User” radio button, then click **New**. The “Rule Management” screen appears.

In this screen, the user can create a custom rule not defined in the programming. To do this (using a single port):

1. Enter the rule name in the “Rule Name” text box. The name is usually based on the application or game title.

2. Set “Protocol” to “TCP.”

3. Enter the port number in the “Port Start,” “Port End,” and “Port Map Start” text boxes. For example, if a server is running on port 8080, enter “8080” in all three text boxes.

4. Click **Apply**.

5. Change Protocol to “UDP.”

6. Enter the port number again, as in step 3.

7. Click **Apply** again. The rule’s TPC and UDP mapping appear at the bottom of the screen.

8. Click **Back**.

9. Select the computer on which to open the ports, then click **User**.

10. Select the rule, then click **Add** to move the rule to the “Applied Rule” text box.

11. Click **Apply**.
For multiple ports:

1. Enter the rule name in the “Rule Name” text box. The name is usually based on the application or game title.

2. Set “Protocol” to “TCP.”

3. Enter the starting port number of the port range in the “Port Start” and “Port Map Start” text boxes, and the last port of the range in the “Port End” text box. For example, if the port range is 5000 to 6000, enter “5000” in the “Port Start” and “Port Map Start” text boxes, and “6000” in the “Port End” text box.

4. Click Apply.

5. Change Protocol to “UDP.”

6. Enter the port numbers again, as in step 3.

7. Click Apply again. The rule’s TPC and UDP mapping appear at the bottom of the screen.

8. Click Back.

9. Select the computer on which to open the ports, then click User.

10. Select the rule, then click Add to move the rule to the “Applied Rule” text box.

11. Click Apply.

**DMZ Hosting**

Selecting **DMZ Hosting** in the “Security” screen generates the “DMZ Hosting” screen. To use DMZ hosting, select the computer on the network to be used as a DMZ host in the “DMZ Host PC Name” drop-down menu, then click **On**.
DMZ hosting is used to support online gaming and Internet conferencing services. These programs usually require multiple open ports, making the network accessible from the Internet. DMZ hosting symbolically places the DMZ host computer outside of the Modem’s network. We recommend activating DMZ hosting only as long as necessary.

When finished with this screen, click **Apply** to save the changes.

**Warning**: The DMZ Host computer will be vulnerable to computer hackers on the Internet while in DMZ mode.

---

**NAT (Network Address Translation)**

Selecting **NAT** in the “Security” screen generates the “NAT” screen. The Modem’s basic firewall security is based on NAT. Disabling NAT allows the computers connected to the Modem to be accessed by outside parties, and can cause the loss of Internet connectivity. Do not turn NAT off unless instructed to do so by the ISP.

When finished, click **Apply** to save the changes.
Configuring Internet Access Controls

This chapter explains how to configure the Internet access controls of the Modem, such as services blocking, Web site blocking, and schedule rules.

Accessing Internet Access Control Screens

To access the Internet Access Control configuration screens, follow these instructions:

1. Open a Web browser. In the “Address” text box, type:

   http://192.168.0.1

   then press Enter on the keyboard.

2. The Main screen appears. Click Internet Access Control.
3. A login window appears. Enter the user name and password in the appropriate text boxes, then click OK.

![Login Window](image)

**Note:** The default user name is “admin.” The default password is “password.”

4. The “Internet Access Control” screen appears. To modify a specific setting, click on its name in the menu bar on the left, or from the list in the middle of the screen.

**Services Blocking**

Selecting **Services Blocking** in the Internet Access Control screen generates the “Services Blocking” screen.

![Services Blocking](image)

To modify Internet privileges (Web, FTP, Newsgroups, etc.) for the computers on the network:

1. Select the computer’s network name from the “PC Name” drop-down menu.
2. Select the Internet service(s) to be blocked by clicking in the appropriate check box.

3. Click **Apply** to block the selected service from the selected computer.

---

**Website Blocking**

Selecting **Website Blocking** in the Internet Access Control screen generates the “Website Blocking” screen. This feature enables the Modem to block Web sites to any or all computers on the network. To block a Web site, select the computer name from the “PC Name” drop-down menu. Then, enter the address of the Web site to be blocked in the “Website” text box and click **Add**. The blocked Web site address will be displayed in the “Blocked Website List” text box, and will not be available to the selected computer on the network. To block the Web site from another computer on the network, repeat the process. To remove a blocked Web site, click on it in the “Blocked Website List,” then click **Remove**. When finished, click **Apply**.

Any changes made in this screen may take up to five minutes to be applied.
Schedule Rules

Selecting Schedule Rules in the Internet Access Control screen generates the “Schedule Rules” screen. Schedule rules allow computers on the network to access the Internet at scheduled times only.

To set up schedule rules for a computer on the network:

1. Select the computer’s network name from the “PC Name” drop-down menu.

2. Click View/Edit Access Details. The computer’s “Allowed Application and Times” screen appears.

3. To schedule Internet access at the same time every day, select “Daily” by clicking the appropriate radio button. If creating different access schedules on a day-to-day basis, select “Weekly.”
4a. If “Daily” was selected in step 3, create a period of Internet access (or rule) by selecting a beginning time (from the “From” drop-down menu) and ending time (from the “To” drop-down menu). If allowing Internet access to a particular computer from 6 p.m. to 8 p.m., for example, select “18 (6 pm)” from the From drop-down menu, and “20 (8 pm)” from the To drop-down menu. Click Add to add the access period to the “Rules” list box. Additional access periods can be added by repeating this step (9 a.m. through 12 p.m., for example), and adding it to the Rules list box. Once the rules are applied in the Daily screen, Internet access will be granted every day at the times listed in the Rules list box.

Note: When using “Daily” scheduling, an access period cannot include 12 a.m. (midnight). To create an access period that includes midnight, create two access periods, one that ends at 12 a.m., and one that begins at 12 a.m.

4b. If “Weekly” was selected in step 3, periods of Internet access can be scheduled at different times on different days (6 p.m. to 8 p.m. on Friday, and 1 p.m. to 4 p.m. on Saturday, for example). To do this, select the day of the week by clicking in the appropriate check box, then create a period (or rule), as explained in step 4a. Click Add for each separate time period. All access periods created will appear in the Rules list box. Once the rules are applied in the Weekly screen, Internet access will be granted to a particular computer at the days and times selected on a weekly basis.

Allowed Application and Times

Notes: Only a Daily or Weekly web browsing option can be set. Setting Daily and Weekly options together will not apply. Once you have set a rule, it will take up to 5 minutes for the rule to take effect.

Web Browsing

- Daily
- Weekly

Notes: A checked box signifies Internet access is allowed. An empty box signifies Internet access is not allowed.

<table>
<thead>
<tr>
<th>Sunday</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Saturday</th>
</tr>
</thead>
</table>

Time

From: 9:00 AM

To: 9:00 AM

Add

Remove

ADD
Note: When using “Weekly” scheduling, an access period cannot include 12 a.m. (midnight). To create an access period that includes midnight, create two access periods, one that ends at 12 a.m. on one day, and one that begins at 12 a.m. on the following day.

5. When finished with all scheduling, click Apply to save the changes to the Modem.

Removing a Schedule Rule

To remove a scheduled rule, select it from the Rules list box, then click Remove. The schedule rule will disappear from the Rules list box.
Configuring the Modem’s Utilities

This chapter explains how to use the Modem’s utilities, including how to restore default settings, upgrade the Modem’s firmware, and perform a ping test.

Accessing the Utilities Screens

To access the Utilities configuration screens, follow these instructions:

1. Open a Web browser. In the “Address” text box, type:
   
   http://192.168.0.1

   then press Enter on the keyboard.

2. The “Home” screen appears. Click Utilities.
3. A login window appears. Enter the user name and password in the appropriate text boxes, then click OK.

Note: The default user name is “admin.” The default password is “password.”

4. The “Utilities” screen appears. To modify a specific configuration, click on its name in the menu bar on the left, or from the list in the middle of the screen.
Chapter 8 Configuring the Modem’s Utilities

Restore Default Settings

To restore the Modem to its factory default settings, select Restore Default Settings from the Utilities screen. When the “Restore Default Settings” screen appears, click Restore Default Settings. Any changes made to the Modem’s settings will be lost and the factory default settings restored. During this process, the Modem’s Power light flashes and the Modem is disabled.

⚠️ Warning: Do not unplug the Power cord from the Modem during the Restore Default Settings process. Doing so may result in permanent damage to the Modem.

When the Power Light stops flashing and glows steadily green, the Modem is fully operational.

---

Upgrade Firmware

Selecting Upgrade Firmware in the Utilities screen generates the “Upgrade Firmware” screen. Firmware upgrades are periodically released to enhance the Modem’s capabilities. Follow the instructions on-screen to upgrade the Modem’s firmware.

---

59
Web Activity Log

The Web Activity Log provides information about the Web sites each computer on the Modem’s network has visited. To access the Web Activity Log, select Web Activity Log from the Utilities screen.

Auto Refresh

To set the Web Activity Log screen to automatically refresh at certain intervals, activate the circle next to “Auto Refresh Every” at the bottom of the Web Activity Log screen, then enter a time value (in seconds) in the text box, or click on the down arrow and select a time value from the menu that appears. The Web Activity Log will refresh at the selected interval.

Manual Refresh

To set the Web Activity Log screen to manually refresh, activate the circle next to “Manual Refresh” at the bottom of the Web Activity Log screen. To refresh the Web Activity Log screen, click Refresh.
Chapter 8 Configuring the Modem’s Utilities

System Log

The System Log provides information about the Modem’s activity. To access the System Log, select **System Log** from the Utilities screen.

**System Log (Size)**

Select the size of the system log displayed here. The smaller the size, the shorter the length of the system log saved.

**Display**

View other saved logs by selecting a log from this drop-down list.

**Apply**

Pressing this button saves any changes to the System Log screen and causes the Save and Restart screen to appear.

**Save Log As**

Pressing this button allows the user to save a log as a file.
OAM Ping Test

Selecting **OAM Ping Test** from the Utilities screen generates the “OAM Ping Test” screen, which is used to check whether the Modem is properly connected to the network. Follow the on-screen instructions to perform the test.

---

### OAM Ping Test

This test can be used to check whether your DSL Gateway is properly connected to the Network. This test may take a few seconds to complete. To perform the test, select your “Test Type” from the list and press the Test button.

<table>
<thead>
<tr>
<th>Connection</th>
<th>VPI</th>
<th>VCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test</td>
<td>0</td>
<td>35</td>
</tr>
</tbody>
</table>

**Test Type**: PS End 3x  
**Test Result**: Waiting for Test

**OAM Statistics**
- Near End F4 Loop Back Count: 0
- Near End F5 Loop Back Count: 0
- Far End F4 Loop Back Count: 0
- Far End F5 Loop Back Count: 0

---

Ping Test

Selecting **Ping Test** from the Utilities screen generates the “Ping Test” screen, which is used to check whether the Modem is properly connected to the Internet. Follow the on-screen instructions to perform the test.

---

### Ping Test

This test can be used to check whether your DSL Gateway is properly connected to the Internet. This test may take a few seconds to complete. To perform the test, insert the URL or IP Address that you would like to ping and click the Test button.

**URL or IP Address:** 192.168.1.1

**Number of Pings:** 1

---

PING 192.168.1.1 (192.168.1.1): 64 data bytes
72 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.0 ms
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0%
Chapter 8 Configuring the Modem’s Utilities

Reboot

Selecting Reboot from the Utilities screen generates the “Reboot” screen. From this screen, the Modem can be rebooted. To do this:

1. From the first Reboot screen, click Reboot.

![Reboot screen]

2. A confirmation window appears. Click OK.

![Confirmation window]

3. The Modem reboots. Read the onscreen information in the screen that appears.

![Onscreen information]

When the Modem’s Power light stops flashing, the Modem has rebooted.
This page left intentionally blank.
Troubleshooting

This chapter contains a list of problems that may be encountered while using the Modem, and techniques to try and overcome the problem. Note that these techniques may not solve the problem. This chapter also includes a list of frequently asked questions.

**Troubleshooting**

**LAN Connection Failure**

- Ensure the Modem is properly configured, the LAN connections are correct, and the power is on.
- Confirm the computer and Modem are on the same network segment. If unsure, let the computer get the IP address automatically by initiating the DHCP function (see “DHCP Server” in chapter 3), then verify the computer is using an IP address within the default range (192.168.0.2 through 198.168.0.254). If the computer is not using an IP address within the range, it will not connect to the Modem.
- Ensure the Subnet Mask address is set to 255.255.255.0 by clicking Status in the “Main Menu” screen.

**Cannot Connect to the Internet**

- Make sure the phone line is connected to the Line port of the modem and the DSL light glows solid green.
- Make sure the Internet light glows solid green.
- If the DSL light is blinking, contact TDS for a line test, as DSL connectivity has been lost.
- If the Internet light glows red, try power cycling the unit (turning it off, then on). A red Internet light indicates the rejection of username\password by the ISP.
- Ensure both ends of the power cord and all network cables are properly connected.
• Ensure the Subnet Mask address is set to 255.255.255.0 by clicking Status in the “Main Menu” screen.

• Verify the Modem’s settings are the same as the computer by clicking Status in the “Main Menu” screen.

• If running Windows 2000, or XP, check the computer’s TCP/IP settings. Select Start, Run, enter
  
  `CMD`
  in the “Open” text box, then press OK. A “DOS” window appears, with a blinking cursor (prompt). Enter
  
  `ipconfig`
  at the cursor, then press Enter on the keyboard.
  
The IP address of the Ethernet adapter should appear in the DOS window. Ensure the IP address in the 192.168.0.x network (with “x” defining a range from 2 through 255).

If the Ethernet adapter is showing an incorrect IP address, enter

  `ipconfig /release`

at the cursor, then press Enter on the keyboard, which sets all values back to 0 (zero). Next, enter

  `ipconfig /renew`

at the cursor, then press Enter on the keyboard (this process may take a few seconds). The renewed IP address should be on the 192.168.0.x network.

If an error occurs, or the IP address renews with an address outside the 192.168.0.x network, contact the ISP immediately

• Ensure the browser is set to “Never dial a connection” and there are no previous LAN settings.
  
  To check this, go to Start, Settings, Control Panel. In the Control Panel, double-click Internet Options. When the “Internet Properties” window appears, ensure that the “Never dial a connection” option is activated, then click LAN Settings. When the “Local Area Network (LAN) Settings” window appears, ensure that no settings are activated. If there are settings activated, deactivate them.

• Shutdown and restart the computer. After the computer restarts, unplug the power cord from the Modem and plug it back in. When the lights glow solid green, try accessing the Internet.
Time out error occurs when entering a URL or IP Address

- Verify all the computers are working properly.
- Ensure the IP settings are correct.
- Ensure the Modem is on and connected properly.
- Verify the Modem’s settings are the same as the computer by clicking Status in the “Main Menu” screen.
- Check the cable/DSL modem by attempting to connect to the Internet.

Frequently Asked Questions

This section includes a list of questions concerning the Modem, and answers to those questions.

General

I have run out of Ethernet ports on my Modem. How do I add more computers?

Plugging in an Ethernet hub or switch expands the number of ports on the Modem. Run a standard Ethernet cable from the “Uplink” port of the new hub or switch to an Ethernet port on the Modem.

Which protocols does the Modem support?

The internal LAN connections support multiple protocols (e.g. TCP/IP, NetBEUI, IPX/SPX, and AppleTalk). The External WAN connection supports only TCP/IP.

Which connection speeds does the Modem support?

The LAN connections on the Modem support 10/100 Mbps. The WAN connection supports 8 Mbps, because of the physical restrictions placed on broadband connections. The 802.11g wireless connection supports up to 54 Mbps connection speeds (depending on signal quality, environmental factors, and physical distance).
**Will my Xbox work with the Modem?**

Yes, the Modem is compatible with the Xbox. You need to set a static IP on the Xbox in the Xbox live network settings, and forward ports 3074 (both UDP and TCP), 53 (both UDP and TCP), and 88 (UDP) if you run into DSL resolution errors.

**Is the Modem flash-upgradeable? How do I do it?**

Yes, the firmware is upgradeable. You can find a link to the firmware site under Utilities in the Web-based configurator. We recommend contacting the ISP for assistance to avoid any issues running firmware upgrades, and to confirm you have the correct firmware before upgrading the unit.

**Does the Modem function as a DSL modem?**

Yes, the Modem has a built-in DSL Modem.

**Wireless**

**Can I use an 802.11b wireless card to connect to the Modem?**

Yes, the Modem can handle 802.11b cards or 802.11g cards. The 802.11g standard is backward compatible with the 802.11b standard. The Modem can be setup to handle just “g” wireless cards, just “b” wireless cards, or both.

**If I install several Modems in different locations in my building, will they be able to talk to each other? Will I be able to stay connected as I move between them?**

The Modem does not communicate with other access points, since it functions as a single access point system. If you installed several Modem devices and were to move between coverage areas, your wireless device would have to reconnect to a separate network.

**Which wireless cards will work with the Modem?**

The Modem connects with any wireless card supporting the 802.11g/802.11b wireless standards.
**Can my wireless signal pass through floors, walls, and glass?**

The physical environment surrounding the Modem can have a varying effect on signal strength and quality. Generally, the more dense the object (a concrete wall compared to a plaster wall, for example), the greater the interference. Concrete or metal-reinforced structures will experience a higher degree of signal loss than those made of wood, plaster, or glass.

**I have an Apple computer that uses the Airport wireless device. Is this device compatible with the Modem?**

While Apple Airport cards should work with the Modem, newer Apple systems may have patches installed that will not allow them to accept WEP keys. If you use new Apple Airport cards and have issues with WEP, set the Modem encryption to WPA (see “WPA” on page 18).

**Network**

**I use my laptop at work and at home. Is there something special I need to do to make it work in both places?**

Yes. Reconfigure your network setting (Workgroup, Domain, Password, User name, IP addressing or any other specific settings used by your company). You may also use third party software like NetSwitcher to automatically switch between different configurations.

**What is the valid IP range I can use for my home network?**

The valid IP range for the Modem is 192.168.0.2 to 192.168.0.254 by default.

**How do I find out what IP address my computer is using?**

Windows 2000 and XP - Select **Start, Run** and type “cmd.” Press **Enter.** When the command screen appears, type “ipconfig” and press **Enter.**
I used DHCP to configure my network. Do I need to restart my computer to refresh my IP address?

No. Follow these steps to refresh your IP address:

Windows 2000 - Select Start, Run, type “cmd,” and press Enter. At the DOS prompt, type “ipconfig /release,” then type “ipconfig /renew.”

Windows XP - Unplug the Ethernet cable or wireless card and plug it back in.

Can I run an application located on another computer over the network?

Yes, if the application is designed to run over a network.

Can I play games between computers on my network, or on the Internet?

Yes, if the games were designed for multi-player or LAN play. For specific information about whether a game is capable of Internet or LAN play, refer to the game documentation. Some games require ports to be forwarded to host or join games over the Internet.

I have an FTP or Web server on my network. How can I make it available to users on the Internet?

For a Web server, enable port forwarding for port 8088 to the IP address of the server and set up the Web server to receive on that port, as well. (Configuring the server to use a static IP address is recommended.)

For an FTP server, enable port forwarding for port 21 to the IP address of the server. (Configuring the server to use a static IP address is recommended.)

Connections

How many computers can be connected through the Modem?

The Modem is capable of 254 connections, but it is recommended to have no more than 45 connections. As you increase the number of connections, you decrease the available speed for each computer.
Chapter 9 Troubleshooting

Security

What is the default username for the Modem?
The default username for the router is “admin” and the default password is “password” (all lower case, no quotation marks). To activate the password to protect the Modem, change the default password. Remote management will not be available on the Modem until the default password is changed.

Does the Modem function as a firewall?
Yes. The Modem provides its security through the use of NAT firewall, which acts as a physical barrier between your network and the Internet.

What is NAT and how does it protect my network?
NAT (Network Address Translation) is a type of security that masks the private IP addresses of the computers on your network with a single public IP address. With NAT, the private IP address of the computers on your network is never transmitted over the Internet.

Which Virtual Private Networking (VPN) protocols are supported?
The Modem supports pass-through for PPTP, L2TP, and IPSec.
This page left intentionally blank.
Specifications

General

Model Number

GT724WGR (Wireless DSL Modem)

Standards

IEEE 802.3 (10BaseT)
IEEE 802.3u (100BaseTX)
IEEE 802.11g (Wireless)
G.dmt
G.lite
t1.413
RFC 1483, 2364, 2516

Protocol

LAN - CSMA/CD
WAN - PPP, DHCP, Static IP

WAN

Full-rate ADSL Interface

LAN

10/100 RJ-45 switched ports

Speed

LAN Ethernet: 10/100 Mbps auto-sensing
Wireless: 802.11g 54 Mbps optimal (see “Wireless Operating Range” for details)

Cabling Type

Ethernet 10BaseT: UTP/STP Category 3 or 5
Ethernet 100BaseTX: UTP/STP Category 5
Wireless Operating Range

Indoors
Up to 91M (300 ft.) @ 54 Mbps

Outdoors
Up to 457M (1500 ft.) @ 54 Mbps

Topology
Star (Ethernet)

LED Indicators
Power, DSL, Internet, Ethernet (4), Wireless

Environmental

Power
External, 12V DC, 600mA

Certifications
FCC Class B, FCC Class C (part 15, 68), CE Mark Commercial, UL

Operating Temperature
0° C to 40° C (32°F to 104°F)

Storage Temperature
-20°C to 70°C (-4°F to 158°F)

Operating Humidity
10% to 85% non-condensing

Storage Humidity
5% to 90% non-condensing
Setting up Static IP on a Computer

To communicate with the Modem from a computer on the network (to use the Modem’s GUI, for example), the user may have to switch the IP address settings from DHCP-enabled to static IP on the computer, so that the computer and the Modem are on the same subnet.

To set up static IP on a computer, select the operating system and follow the instructions provided in this chapter.

Note: The following instructions are based on the Modem’s factory default IP address. If the Modem’s IP address has been changed, enter the new IP address when instructed to enter an IP address.

Windows 2000

1. From the desktop, click on the Start button in the lower left corner.

2. From the menu that appears, select Settings.
3. Another menu appears. Select **Control Panel**.

4. When the “Control Panel” window appears, double-click **Network and Dial-up Connections**.
5. In the “Network and Dial-up Connections” window, double-click **Local Area Connection**. A number may be displayed after the Local Area Connection. If there is more than one Local Area Connection listed, locate the one that corresponds to the network card installed in the computer by finding the name of the network card in the “Device Name” column.

![Network and Dial-up Connections window](image)

6. The “Local Area Connection Status” window appears. Select **General**, then click **Properties**.

![Local Area Connection 2 Status window](image)

7. The “Local Area Connection Properties” window appears. Click **General**.
8. In the “Components checked are used by this connection” list box, double-click Internet Protocol (TCP/IP).


10. In the General tab, make sure the radio button next to “Obtain an IP Address automatically” is active (contains a black dot). If the radio button is already active, leave it alone.

11. Enter the following numbers in the “IP Address” text box:

   192.168.0.2

   Press the space bar on the keyboard to add the periods between the numbers.
12. Enter the following numbers in the “Subnet mask” text box:
   \[ 255.255.255.0 \]

   Press the space bar on the keyboard to add the periods between the numbers.

13. Enter the following numbers in the “Default gateway” text box:
   \[ 192.168.0.1 \]

   Press the space bar on the keyboard to add the periods between the numbers.


15. In the “Local Area Connection Properties” window, click OK. The Local Area Connection Properties window disappears.

16. Click Close in the Local Area Connection Status window. The window disappears.

17. Close the Network and Dial-up Connections window by clicking on the “x” button at the upper right corner of the window.

   The computer is now set up with a static IP address, allowing the user to access the Modem’s GUI.
Windows XP

1. From the desktop, click **Start** button in the lower left corner.

2. From the menu that appears, select **Control Panel**.

3. When the “Control Panel” window appears, double-click **Network Connections**.
4. In the “Network Connections” window, double-click Local Area Connection. A number may be displayed after the Local Area Connection. If more than one Local Area Connection is listed, locate the one that corresponds to the network card installed in your computer by finding the name of the network card in the “Device Name” column.

5. The “Local Area Connection Properties” window appears. Select General.

6. In the “This connection uses the following items” list box, double-click Internet Protocol (TCP/IP).

8. In the General tab, make sure the radio button next to “Use the following IP Address” is active (contains a black dot). If the radio button is already active, leave it alone.

9. Enter the following address in the “IP Address” text box:  
   192.168.0.2  
   Enter the periods in the address by pressing the space bar on the keyboard.

10. Enter the following address in the “Subnet mask” text box:  
    255.255.255.0  
    Enter the periods in the address by pressing the space bar on the keyboard.

11. Enter the following address in the “Default gateway” text box:  
    192.168.0.1  
    Enter the periods in the address by pressing the space bar on the keyboard.

12. Click OK. The Internet Protocol (TCP/IP) Properties window disappears.

13. In the Local Area Connection Properties window, click Close. The Local Area Connection Properties window disappears.

14. Click Close in the Local Area Connection Status window. The window disappears.
15. Close the Network and Dial-up Connections window by clicking on the “x” button at the upper right corner of the window.

The computer is now set up with a static IP address, allowing the user to access the Modem’s GUI.

Windows Vista

1. From the desktop, click Start button in the lower left corner.

2. From the menu that appears, select Control Panel.

3. When the “Control Panel” window appears, double-click Network and Internet.
4. The “Network and Internet” window appears. Click **Network and Sharing Center**.

5. The “Network and Sharing Center” screen appears. From the menu on the left, click **Manage network connections**.
6. The “Network Connections” screen appears. Double-click **Local Area Connection**.

![Network Connections Screen]

7. The “Local Area Connection Properties” window appears. In the “This connection uses the following items” list box, double-click **Internet Protocol (TCP/IP)**.

![Local Area Connection Properties Window]

![Internet Protocol Version 4 (TCP/IPv4) Properties window]

9. In the **General** tab, make sure the circle next to “Use the following IP Address” is selected. When active, a black dot appears in the circle. If the circle already contains a black dot, leave it alone.

10. Enter the following address in the “IP Address” text box:
    
    192.168.0.2

    Enter the periods in the address by pressing the space bar on the keyboard.

11. Enter the following address in the “Subnet mask” text box:
    
    255.255.255.0

    Enter the periods in the address by pressing the space bar on the keyboard.

12. Enter the following address in the “Default gateway” text box:
    
    192.168.0.1

    Enter the periods in the address by pressing the space bar on the keyboard.

13. Click **OK**. The Internet Protocol (TCP/IP) Properties window disappears.

14. In the Local Area Connection Properties window, click **Close**. The Local Area Connection Properties window disappears.

15. Click **Close** in the Local Area Connection Status window. The window disappears.

16. Close the rest of the open windows by clicking on the “x” button at the upper right corner of the window.

The computer is now set up with a static IP address.
Service Acronyms

The following information is related to the Firewall options (Custom, High, Medium, and Low) section in the “Configuring Security Settings” chapter of this manual. This appendix explains the meaning of the service acronyms included with the various levels of firewall security, and the UDP and TCP ports used by each service.

Service Acronym Definitions

**DNS**
Domain Name System. A data query system used to translate host names into Internet addresses (i.e., www.somewebsite.com translates to 888.999.000.111). Uses UDP 53 and TCP 53.

**EPMAP**
EndPoint Mapper. Uses UDP 135 and TCP 135.

**FTP**
File Transfer Protocol. A protocol used to transfer files over the Internet. Uses TCP 20 and 21.

**HTTP**
HyperText Transfer Protocol. This protocol delivers information over the Internet, and is used when a computer connects to a Web site via an Internet browser. Uses TCP 80.

**HTTPS**
HyperText Transfer Protocol using Secure Socket Layer. A secure version of the protocol that delivers information over the Internet. Uses UDP 443 and TCP 443.
IMAP, IMAPv3
Internet Message Access Protocol. Protocols for retrieving E-mail messages. IMAP uses TCP 143; IMAPv3 uses TCP 220.

IPSEC IKE, IPSEC ESP
IP Security. Protocols which support the secure exchange of packets at the IP layer. Uses UDP 500.

LDAP

MICROSOFT-DS, -GC
-DS uses UDP 445 and TCP 445; -GC uses TCP 3268.

NETBIOS-NS, -DGM, -SSN
Network Basic Input Output System. Three types of DOS BIOS augmentation which add functions for local area networks (LANs). -NS uses UDP 137 and TCP 137; -DGM uses UDP 138; -SSN uses TCP 138.

NNTP
Network News Transfer Protocol. A protocol used to distribute and retrieve news articles over the Internet. Uses TCP 119.

POP3
Post Office Protocol 3. Another protocol used to transfer E-mail between computers. Usually employs a pop3 server, and is used to receive mail only. Uses TCP 110.

PROFILE
Uses TCP 136.
**SMTP**

Simple Mail Transfer Protocol. A protocol used to transfer E-mail between computers over the Internet. Can be used to send and receive mail. Uses TCP 25.

**SNMP**

This page left intentionally blank.
**Access Point**
A device that allows wireless clients to connect to one another. An access point can also act as a bridge between wireless clients and a “wired” network, such as an Ethernet network. Wireless clients can be moved anywhere within the coverage area of the access point and remain connected to the network. If connected to an Ethernet network, the access point monitors Ethernet traffic and forwards appropriate Ethernet messages to the wireless network, while also monitoring wireless traffic and forwarding wireless client messages to the Ethernet network.

**ATM (Asynchronous Transfer Mode)**
A networking technology based on transferring data in fixed-size packets.

**Client**
A desktop or mobile computer connected to a network.

**DHCP (Dynamic Host Configuration Protocol)**
A protocol designed to automatically assign an IP address to every computer on your network.

**DNS (Domain Name System) Server Address**
Allows Internet host computers to have a domain name and one or more IP addresses. A DNS server keeps a database of host computers and their respective domain names and IP addresses so that when a user enters a domain name into a Web browser, the user is sent to the proper IP address. The DNS server address used by computers on the home network corresponds to the location of the DNS server the ISP has assigned.

**DSL (Digital Subscriber Line) Modem**
A modem that uses existing phone lines to transmit data at high speeds.

**Encryption**
A method to allow wireless data transmissions a level of security.

**ESSID (Extended Service Set Identifier)**
A unique identifier for a wireless network. Also known as “SSID.”
Ethernet Network

A standard wired networking configuration using cables and hubs.

Firewall

A method preventing users outside the network from accessing and/or damaging files or computers on the network.

Gateway

A central device that manages the data traffic of your network, as well as data traffic to and from the Internet.

IP (Internet Protocol) Address

A series of four numbers separated by periods identifying a unique Internet computer host.

ISP Gateway Address

An IP address for the Internet router. This address is only required when using a cable or DSL modem.

ISP (Internet Service Provider)

A business that allows individuals or businesses to connect to the Internet.

LAN (Local Area Network)

A group of computers and devices connected together in a relatively small area (such as a house or an office). A home network is considered a LAN.

MAC (Media Access Control) Address

The hardware address of a device connected to a network.

NAT (Network Address Translation)

A method allowing all of the computers on a home network to use one IP address, enabling access to the Internet from any computer on the home network without having to purchase more IP addresses from the ISP.

PC Card

An adapter that inserts in the PCMCIA slot of a computer, enabling the communication with a device.
Appendix D Glossary

**PPPoE (Point-To-Point Protocol over Ethernet)/ PPPoA (Point-To-Point Protocol over ATM)**

Methods of secure data transmission.

**Router**

A central device that manages the data traffic of your network.

**Subnet Mask**

A set of four numbers configured like an IP address used to create IP address numbers used only within a particular network.

**SSID**

See “ESSID.”

**TCP/IP (Transmission Control Protocol/Internet Protocol)**

The standard protocol for data transmission over the Internet.

**WAN (Wide Area Network)**

A network that connects computers located in separate areas, (i.e., different buildings, cities, countries). The Internet is a WAN.

**WECA (Wireless Ethernet Compatibility Alliance)**

An industry group that certifies cross-vender interoperability and compatibility of IEEE 802.11b wireless networking products and promotes the standard for enterprise, small business, and home environments.

**WLAN (Wireless Local Area Network)**

A group of computers and other devices connected wirelessly in a small area.
This page left intentionally blank.
Notices

Regulatory Compliance Notices

Class B 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 implementing one or more of the following measures:

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

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Actiontec Electronics, Inc., may void the user’s authority to operate the equipment.

Declaration of conformity for products marked with the FCC logo – United States only.

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;
2. This device must accept any interference received, including interference that may cause unwanted operation.

\textbf{Note:} To comply with FCC RF exposure compliance requirements, the antenna 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.

For questions regarding your product or the FCC declaration, contact:

\textit{Actiontec Electronics, Inc.}
760 North Mary Ave.
Sunnyvale, CA 94086
United States
Tel: (408) 752-7700
Fax: (408) 541-9005
Limited Warranty

Hardware: Actiontec Electronics, Inc., warrants to the end user (“Customer”) that this hardware product will be free from defects in workmanship and materials, under normal use and service, for twelve (12) months from the date of purchase from Actiontec Electronics or its authorized reseller.

Actiontec Electronics’ sole obligation under this express warranty shall be, at Actiontec’s option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, Actiontec Electronics may, in its sole discretion, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of Actiontec Electronics, Inc. Replacement products may be new or reconditioned. Actiontec Electronics warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

Software: Actiontec Electronics warrants to Customer that each software program licensed from it will perform in substantial conformance to its program specifications, for a period of ninety (90) days from the date of purchase from Actiontec Electronics or its authorized reseller. Actiontec Electronics warrants the media containing software against failure during the warranty period. The only updates that will be provided are at the sole discretion of Actiontec Electronics and will only be available for download at the Actiontec Web site, www.actiontec.com. Actiontec Electronics’ sole obligation under this express warranty shall be, at Actiontec Electronics’ option and expense, to refund the purchase price paid by Customer for any defective software product, or to replace any defective media with software which substantially conforms to applicable Actiontec Electronics published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. Actiontec Electronics makes no warranty or representation that its software products will meet Customer’s requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third-party products listed in the Actiontec Electronics software product documentation or specifications as being compatible, Actiontec Electronics will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a “bug” or defect in the third party’s product or from use of the software product not in accordance with Actiontec Electronics published specifications or user guide.
THIS ACTIONTEC ELECTRONICS PRODUCT MAY INCLUDE OR BE BUNDLED WITH THIRD-PARTY SOFTWARE, THE USE OF WHICH IS GOVERNED BY A SEPARATE END-USER LICENSE AGREEMENT.

THIS ACTIONTEC ELECTRONICS WARRANTY DOES NOT APPLY TO SUCH THIRD-PARTY SOFTWARE. FOR THE APPLICABLE WARRANTY, PLEASE REFER TO THE END-USER LICENSE AGREEMENT GOVERNING THE USE OF SUCH SOFTWARE.

Obtaining Warranty Service: Customer may contact Actiontec Electronics Technical Support Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from Actiontec Electronics or its authorized reseller may be required. Products returned to Actiontec Electronics must be pre-authorized by Actiontec Electronics with a Return Merchandise Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. The repaired or replaced item will be shipped to Customer, at Actiontec Electronics’ expense, not later than thirty (30) days after Actiontec Electronics receives the defective product.

Return the product to:
(In the United States)
Actiontec Electronics, Inc.
760 North Mary Avenue
Sunnyvale, CA 94085

Actiontec Electronics shall not be responsible for any software, firmware, information, memory data, or Customer data contained in, stored on, or integrated with any products returned to Actiontec Electronics for repair, whether under warranty or not.

WARRANTIES EXCLUSIVE: IF AN ACTIONTEC ELECTRONICS’ PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER’S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT ACTIONTEC ELECTRONICS’ OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, TERMS OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. ACTIONTEC ELECTRONICS
NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

ACTIONTEC ELECTRONICS SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER’S OR ANY THIRD PERSON’S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPT TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OTHER HAZARDS, OR ACTS OF GOD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, ACTIONTEC ELECTRONICS ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCT, EVEN IF ACTIONTEC ELECTRONICS OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT ACTIONTEC ELECTRONICS’ OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Disclaimer: Some countries, states or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

Dispute Resolution: The customer may contact the Director of Technical Support in the event the Customer is not satisfied with Actiontec Electronics’ response to the complaint. In the event that the Customer is still not satisfied with the response of the Director of Technical Support, the Customer is instructed to contact the Director of Marketing. In the event that the Customer is still not satisfied with the response of the Director of Marketing, the Customer is instructed to contact the Chief Financial Officer and/or President.
**Governing Law:** This Limited Warranty shall be governed by the laws of the State of California, U.S.A., excluding its conflicts of laws and principles, and excluding the United Nations Convention on Contracts for the International Sale of Goods.