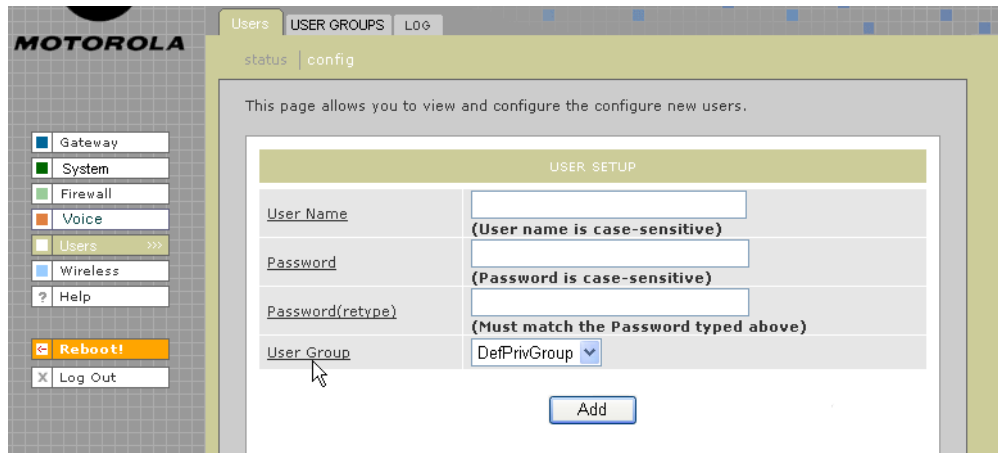


Users > USERS — config

Use this page to configure new users.

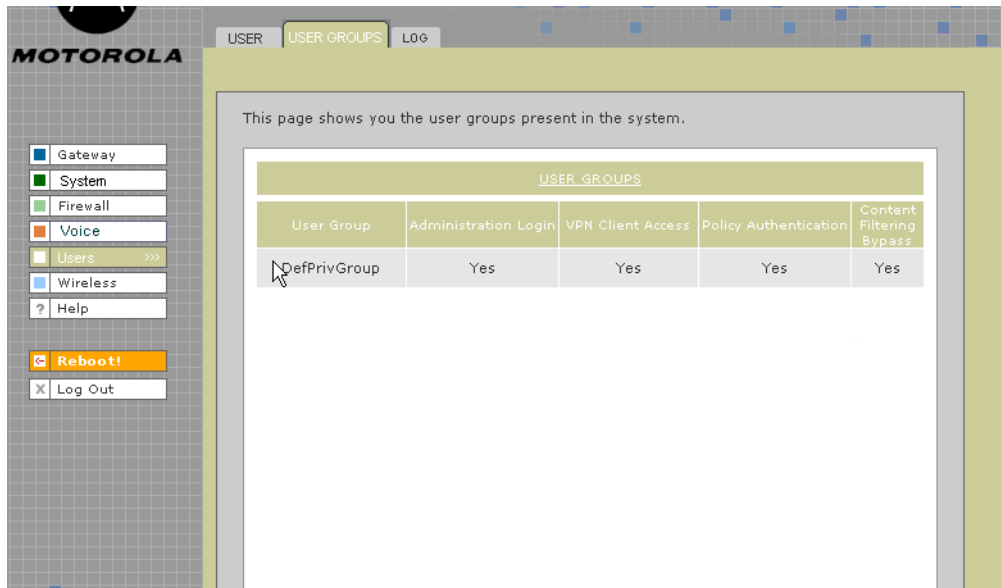


Users > USERS — config page fields

Field	Description
USER SETUP	
User Name	Type the user name as it will be entered by the user to log on to the network.
Password	Type at least four characters for the user's password.
Password (retype)	Retype the user's password.
User Group	Select a user group from the list. The user is given all the privileges assigned to that group. See Users > USER GROUPS for more information about user groups.
Add (button)	Click Add when you finish entering user setup information. The user name is added to the USERS list on the Firewall > FIREWALL — advanced page.

Users > USER GROUPS

Use this page to configure user groups to which users belong.



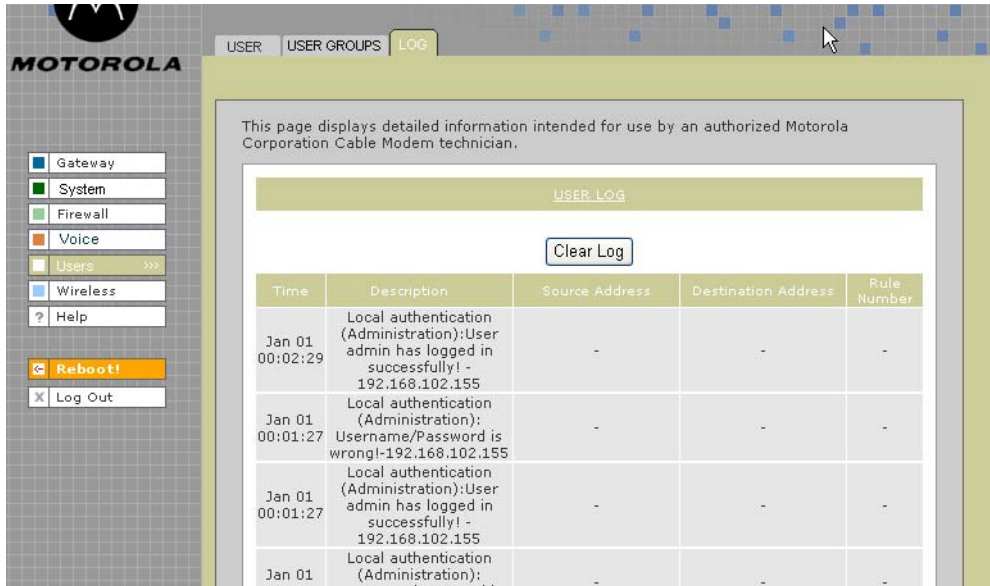
Users > USER GROUPS page fields

Field	Description
USER_GROUPS	Will this page include a way to create user groups?
User Group	Help screens not provided
Administration Login	
VPN Client Access	
Policy Authentication	
Content Filtering Bypass	

NOTE: page 25 of spec says the product supports VPN pass through for IPSEC, PPTP, and L2TP.

Users > LOG

Use this page to view a log of user activity:

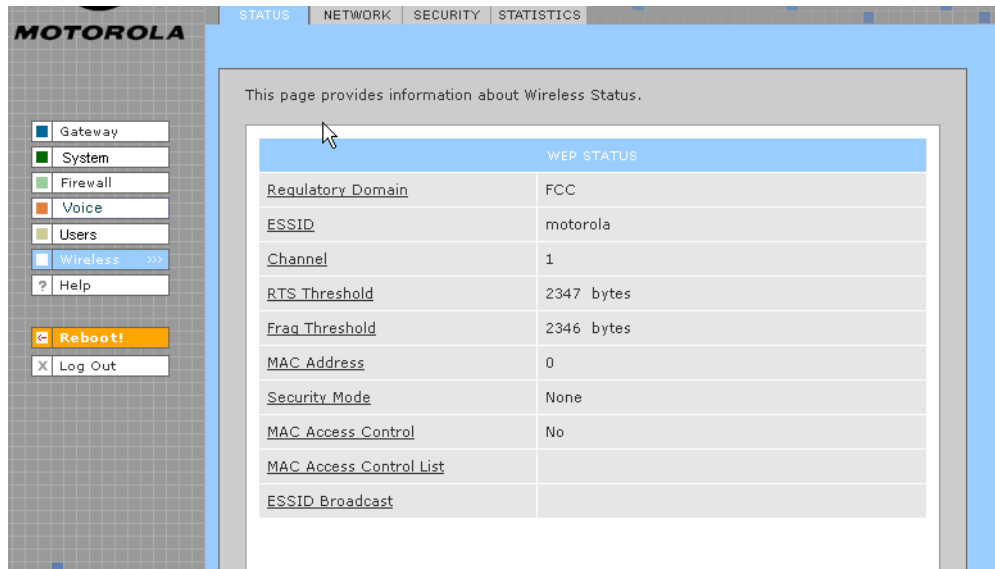


Users > LOG page fields

Field	Description
USER LOG	
Clear Log (button)	Clears all entries in the log.
Time	The time frame that a user accessed a particular destination address.
Description	The URL or Web page accessed.
Source Address	The source IP address of the inbound or outbound message.
Destination Address	The destination IP address of the inbound or outbound message.
Rule Number	The firewall profile rule applicable to this user. Refer to Firewall > FIREWALL — advanced for more information about firewall rules.

Wireless > STATUS

This page provides wireless status information.



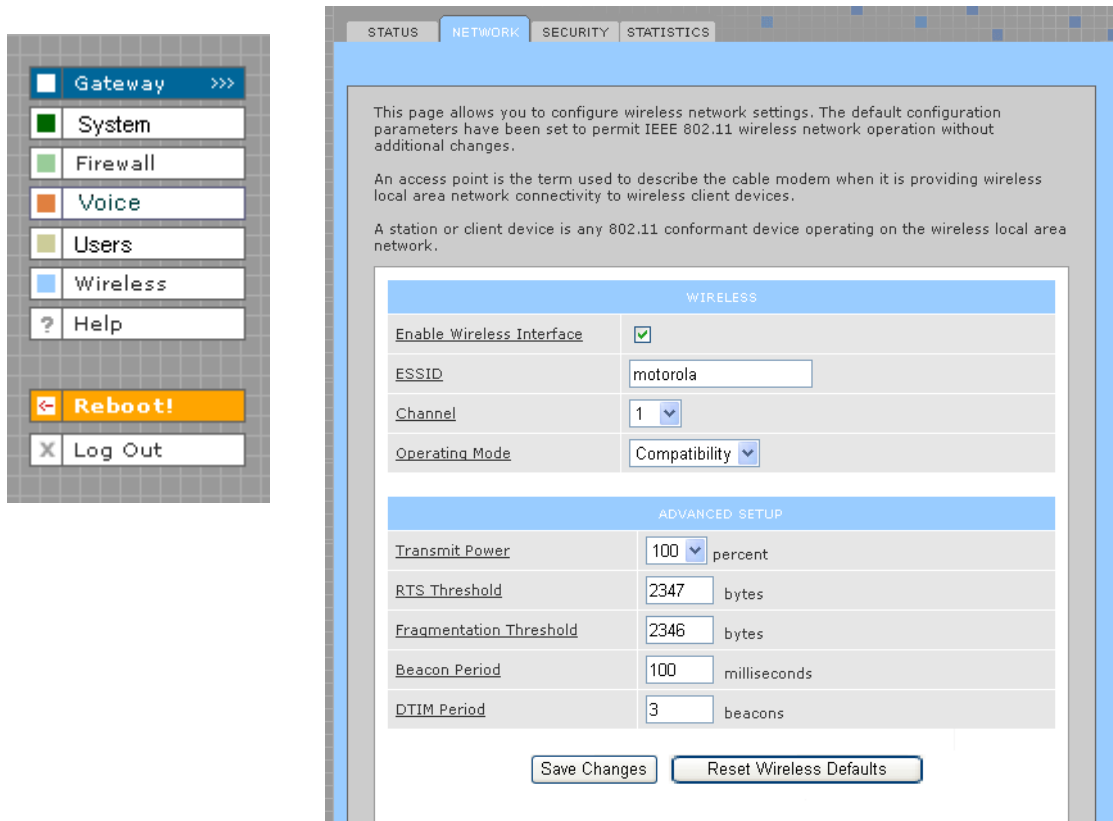
The screenshot shows the Motorola configuration interface. On the left is a navigation menu with options: Gateway, System, Firewall, Voice, Users, Wireless (selected), and Help. Below the menu are buttons for Reboot! and Log Out. The main content area has tabs for STATUS, NETWORK, SECURITY, and STATISTICS. A message states: "This page provides information about Wireless Status." Below this is a table titled "WEP STATUS" with the following data:

WEP STATUS	
<u>Regulatory Domain</u>	FCC
<u>ESSID</u>	motorola
<u>Channel</u>	1
<u>RTS Threshold</u>	2347 bytes
<u>Frag Threshold</u>	2346 bytes
<u>MAC Address</u>	0
<u>Security Mode</u>	None
<u>MAC Access Control</u>	No
<u>MAC Access Control List</u>	
<u>ESSID Broadcast</u>	

Refer to "[Setting Up Your Wireless LAN \(WLAN\)](#)" for a description of each field, or mouse-over the underlined field name and right-click to view a general description in a Help window.

Wireless > NETWORK

This page allows you to configure wireless network settings. The default configuration parameters are set to permit IEEE 802.11 wireless network operation without additional changes. Any 802.11 conforming device may operate on the network.



STATUS NETWORK SECURITY STATISTICS

This page allows you to configure wireless network settings. The default configuration parameters have been set to permit IEEE 802.11 wireless network operation without additional changes.

An access point is the term used to describe the cable modem when it is providing wireless local area network connectivity to wireless client devices.

A station or client device is any 802.11 conformant device operating on the wireless local area network.

WIRELESS

Enable Wireless Interface	<input checked="" type="checkbox"/>
ESSID	motorola
Channel	1
Operating Mode	Compatibility

ADVANCED SETUP

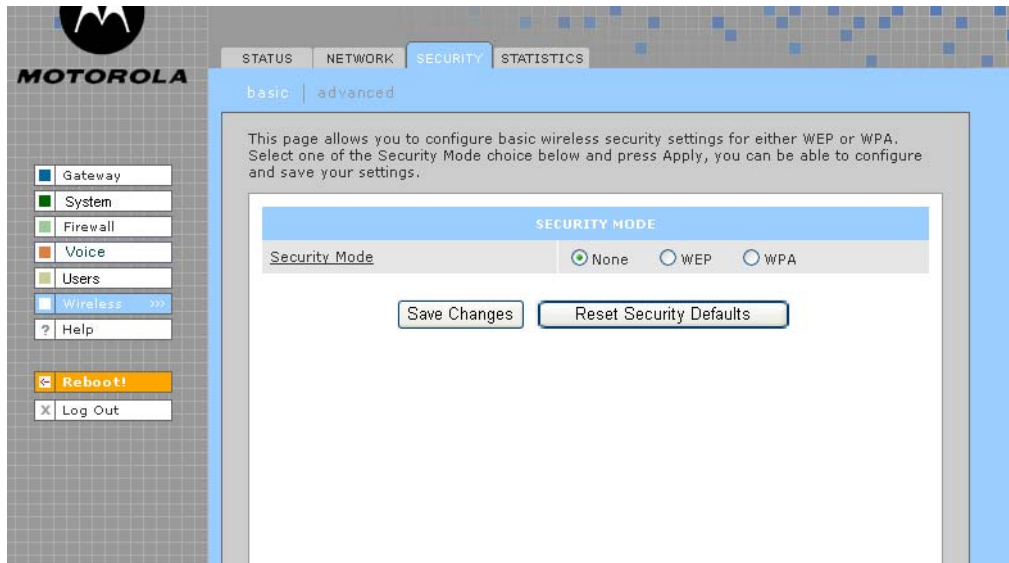
Transmit Power	100	percent
RTS Threshold	2347	bytes
Fragmentation Threshold	2346	bytes
Beacon Period	100	milliseconds
DTIM Period	3	beacons

Save Changes Reset Wireless Defaults

Refer to "[Setting Up Your Wireless LAN \(WLAN\)](#)" for a description of each field, or mouse-over the underlined field name and right-click to view a general description in a Help window.

Wireless > SECURITY – basic

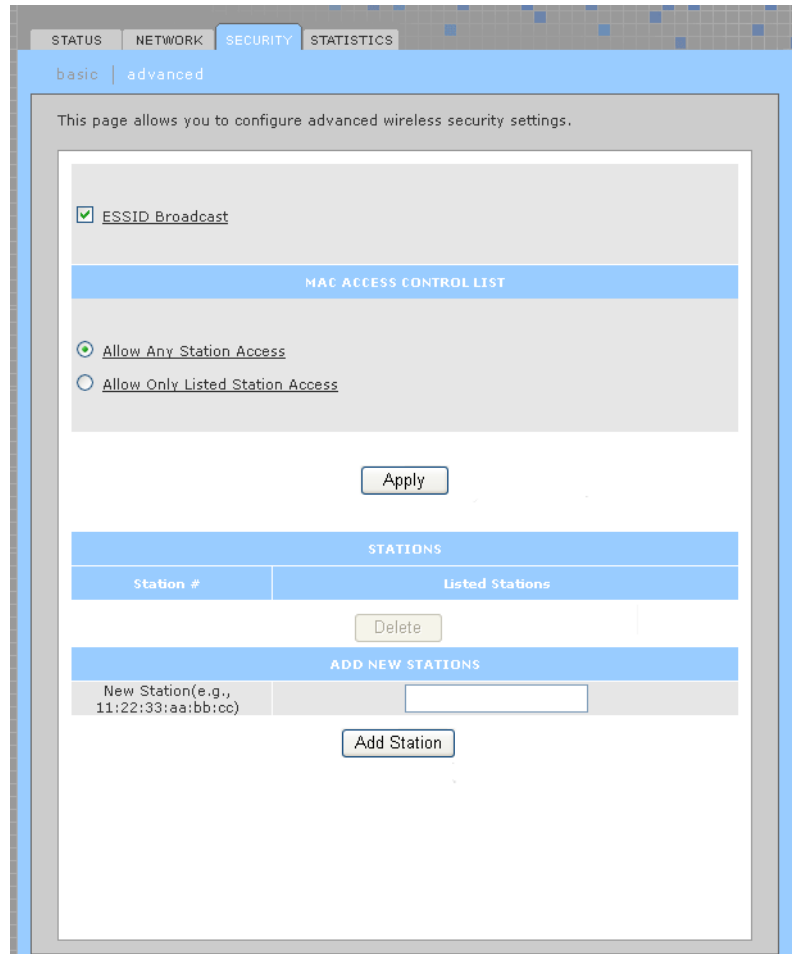
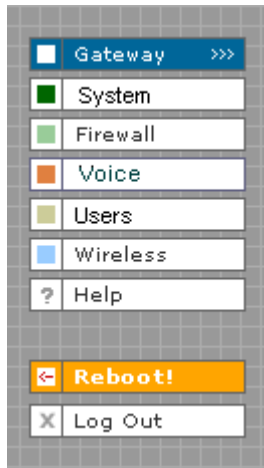
This page allows you to configure basic wireless security settings for WEP or WPA.



Refer to [“Configuring WPA on the VT2500”](#) or [“Configuring WEP on the VT2500”](#) under [“Setting Up Your Wireless LAN \(WLAN\)”](#) for a description of each field. Or, mouse-over the underlined field name and right-click to view a general description in a Help window.

Wireless > SECURITY – advanced

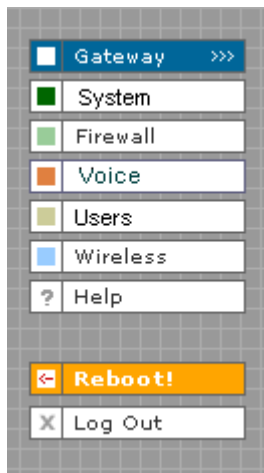
This page allows you to configure advanced wireless security settings.



Refer to “[Setting Up Your Wireless LAN \(WLAN\)](#)” for a description of each field, or mouse-over the underlined field name and right-click to view a general description in a Help window.

Wireless > STATISTICS

This page provides information about wireless statistics.



STATUS NETWORK SECURITY **STATISTICS**

This page provides information about Wireless Stats.

WIRELESS STATISTICS	
<u>Transmitted Fragment Count</u>	1263
<u>Multicast Transmitted Fragment Count</u>	1262
<u>Failed Count</u>	1
<u>Retry Count</u>	0
<u>Multiple Retry Count</u>	0
<u>Frame Duplicate Count</u>	1
<u>Request to Send Success Count</u>	3341
<u>Request to Send Failure Count</u>	1996
<u>Acknowledge Failed Count</u>	0
<u>Received Fragment Count</u>	11
<u>Multicast Received Fragment Count</u>	11
<u>Frame Check Sequence Error Count</u>	10155
<u>Transmitted Frame Count</u>	1265
<u>WEP Undecryptable Count</u>	0

Refresh

Refer to "[Setting Up Your Wireless LAN \(WLAN\)](#)" for a description of each field, or mouse-over the underlined field name and right-click to view a general description in a Help window.

❖ Configuring TCP/IP

You must be sure all client computers are configured for [TCP/IP](#) (a protocol for communication between computers). Perform *one* of these:

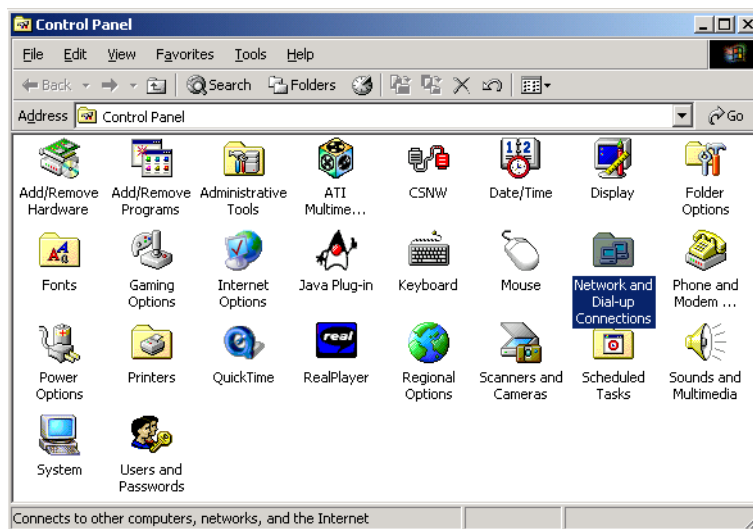
- [Configuring TCP/IP in Windows 95, Windows 98, or Windows Me](#)
- [Configuring TCP/IP in Windows 2000](#)
- [Configuring TCP/IP in Windows XP](#)
- Follow the instructions in your Macintosh or UNIX user manual

After configuring TCP/IP, perform *one* of the following to verify the [IP address](#):

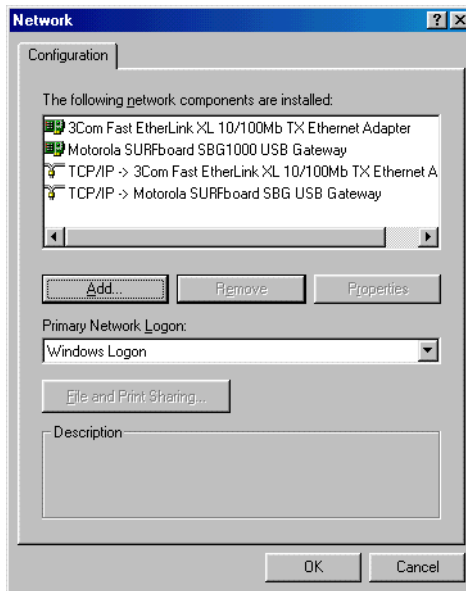
- [Verifying the IP Address in Windows 95, Windows 98, or Windows Me](#)
- [Verifying the IP Address in Windows 2000 or Windows XP](#)
- Follow the instructions in your Macintosh or UNIX user manual

Configuring TCP/IP in Windows 95, Windows 98, or Windows Me

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Settings** and then **Control Panel** from the pop-up menus to display the Control Panel window:

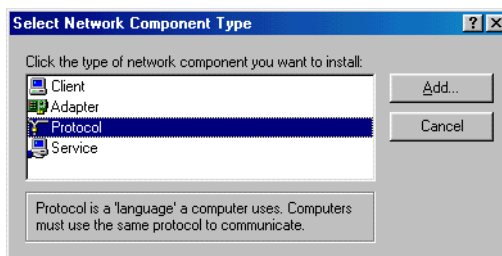


- 3 Double-click the **Network** icon to display the Network window:

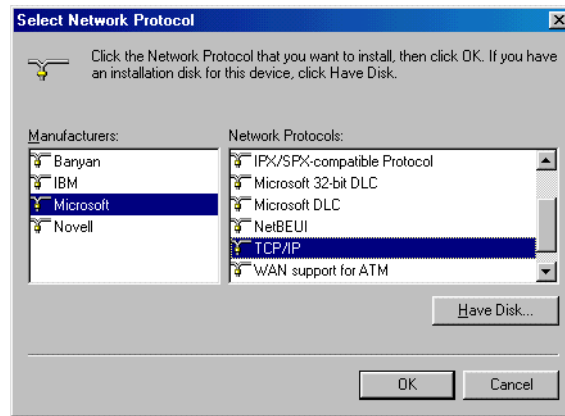


Although your VT model number may be different than in the images in this guide, the procedure is the same.

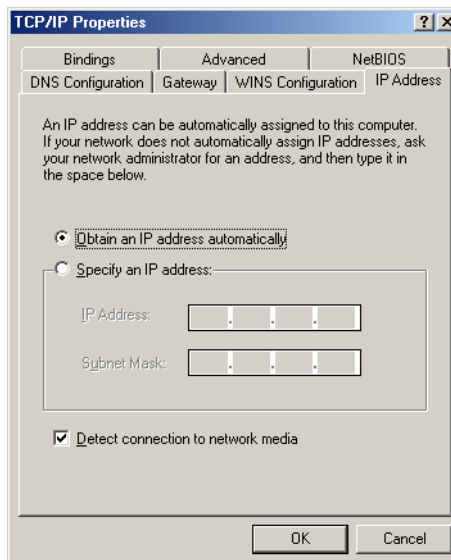
- 4 Select the **Configuration** tab.
- 5 Verify that TCP/IP is installed for the adapter used to connect to the VT2500. If TCP/IP is installed, skip to step 10. If TCP/IP is not installed for the adapter, continue with step 6.
- 6 Select the adapter to use for the VT2500 connection and click **Add**. The Select Network Component Type window is displayed:



- 7 Click **Protocol** and click **Add**. The Select Network Protocol window is displayed:



- 8 Click **Microsoft** in the Manufacturers section and click **TCP/IP** in the Network Protocols section.
- 9 Click **OK**.
- 10 Click **TCP/IP** on the Network window. If there is more than one TCP/IP entry, choose the one for the Ethernet card or USB port connected to the VT2500.
- 11 Click **Properties**. The TCP/IP Properties window is displayed:

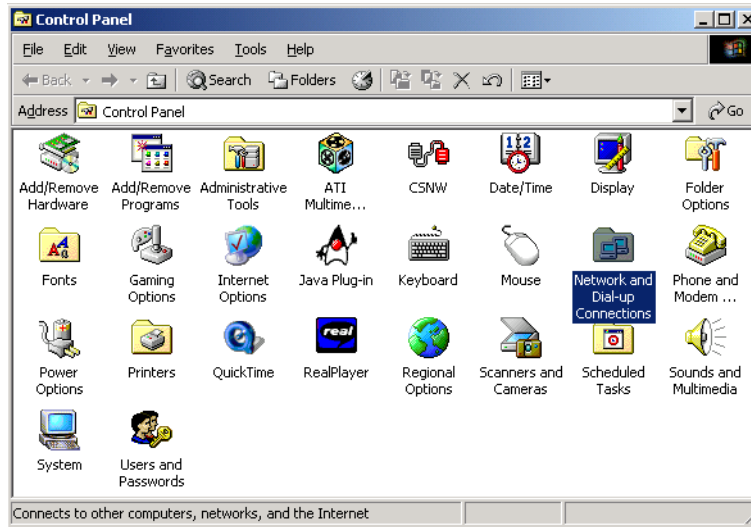


- 12 Click the **IP Address** tab.
- 13 Click **Obtain an IP address automatically**.
- 14 Click **OK** to accept the TCP/IP settings.
- 15 Click **OK** to close the Network window.
- 16 Click **OK** when prompted to restart the computer and click **OK** again.

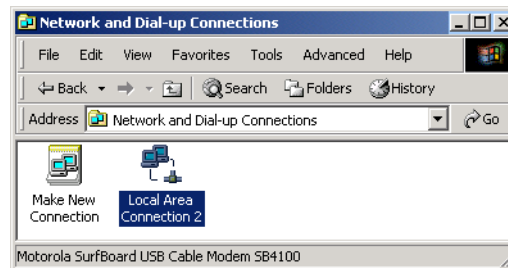
When you complete TCP/IP configuration, go to [“Verifying the IP Address in Windows 95, Windows 98, or Windows Me”](#).

Configuring TCP/IP in Windows 2000

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Settings** and then **Control Panel** from the pop-up menus to display the Control Panel window:

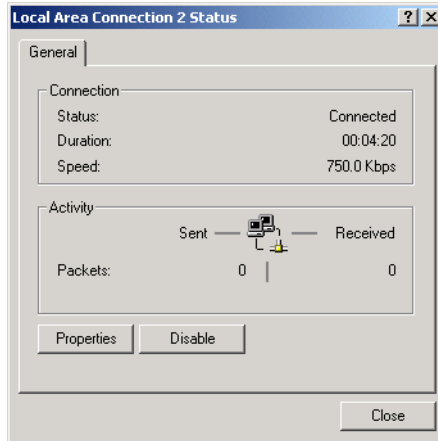


- 3 Double-click the **Network and Dial-up Connections** icon to display the Network and Dial-up Connections window:

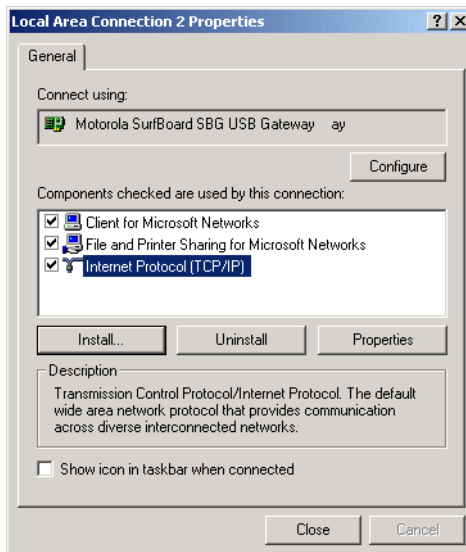


In the steps that follow, a connection *number* like 1, 2, 3, etc., is a reference that is displayed on computers with multiple network interfaces. Computers with only one network interface may only see the label: Local Area Connection.

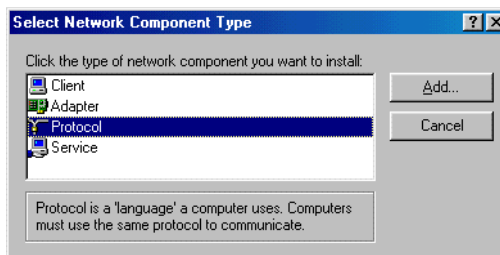
- 4 Click **Local Area Connection number**. The value of *number* varies from system to system. The Local Area Connection *number* Status window is displayed:



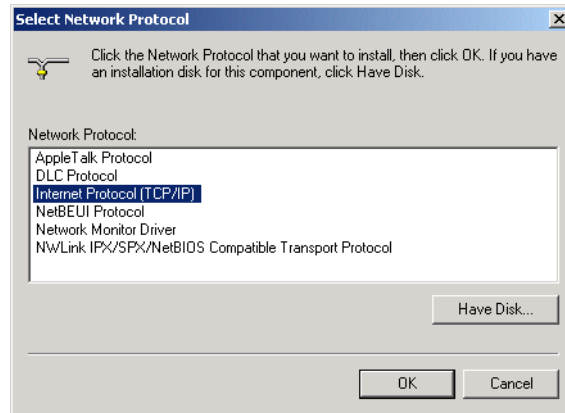
- 5 Click **Properties**. Information similar to the following window is displayed:



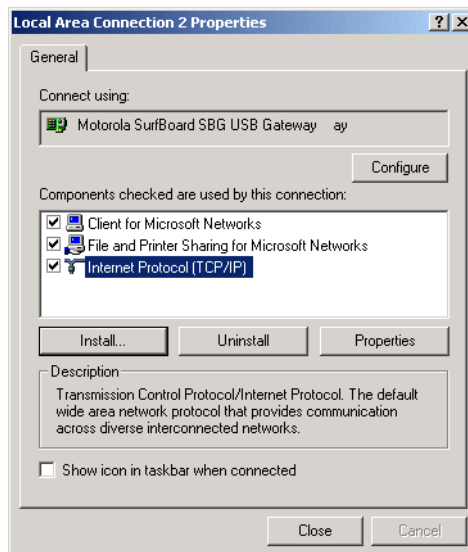
- 6 If Internet Protocol (TCP/IP) is in the list of components, TCP/IP is installed. You can skip to step 10.
If Internet Protocol (TCP/IP) is not in the list, click **Install**. The Select Network Component Type window is displayed:



- Click **Protocol** on the Select Network Component Type window and click **Add**. The Select Network Protocol window is displayed:

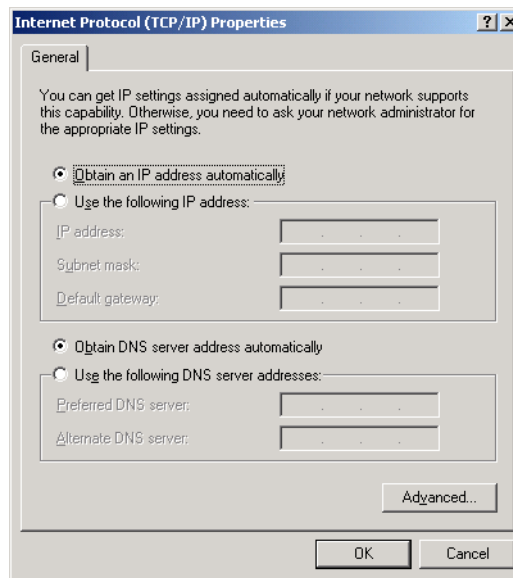


- Click **Internet Protocol (TCP/IP)**.
- Click **OK**. The Local Area Connection *number* Properties window is re-displayed.



- Be sure the box next to Internet Protocol (TCP/IP) is selected.

- 11 Click **Properties**. The Internet Protocol (TCP/IP) Properties window is displayed:

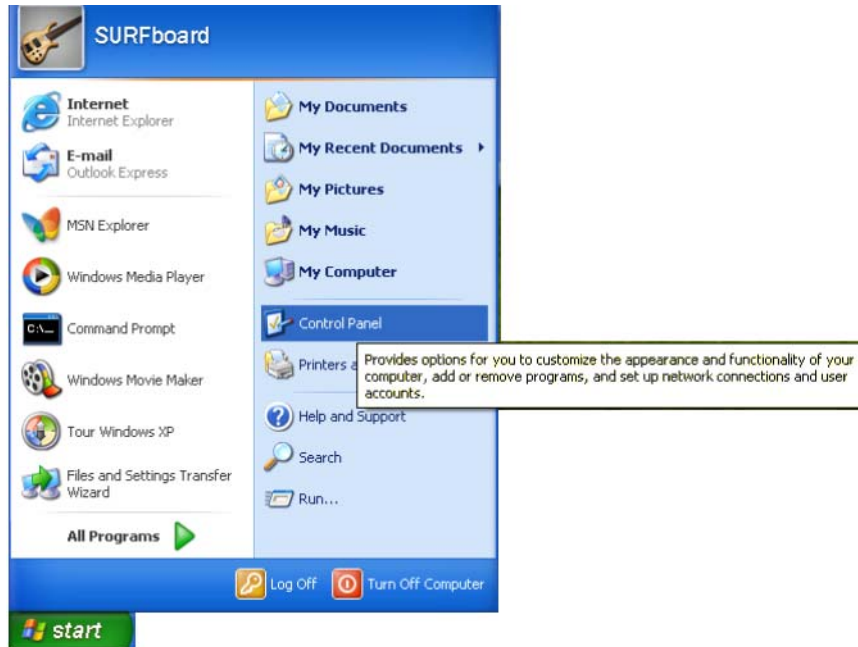


- 12 Be sure **Obtain IP address automatically** and **Obtain DNS server address automatically** are selected.
- 13 Click **OK** to accept the TCP/IP settings.
- 14 Click **Close** to close the Local Area Connection *number* Properties window.
- 15 Click **OK** when prompted to restart the computer and click **OK** again.

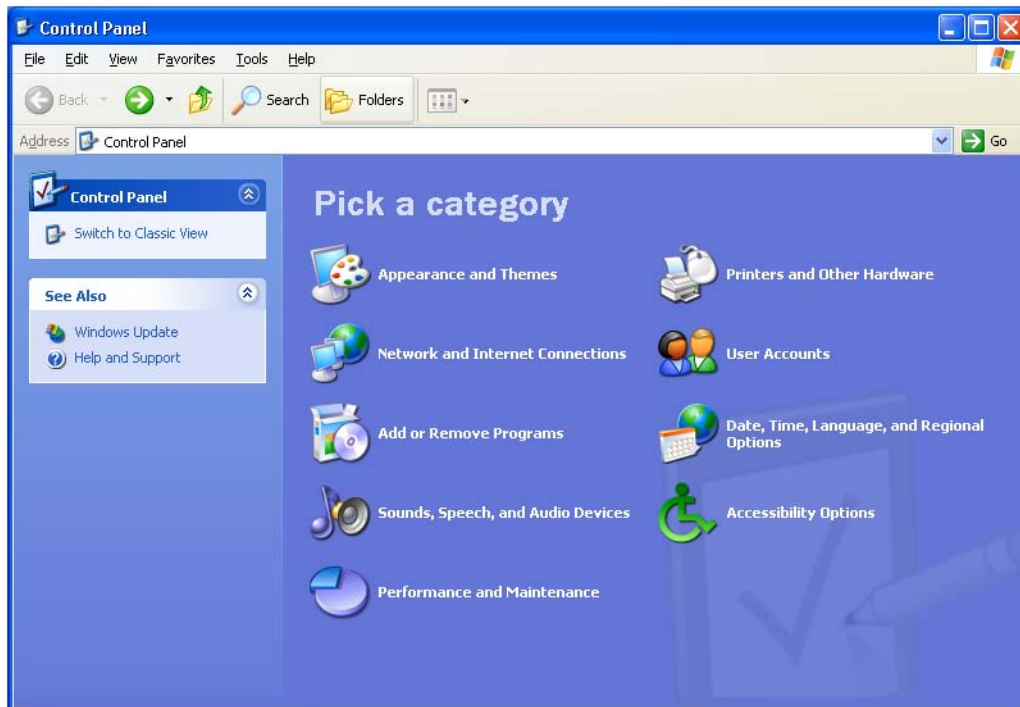
When you complete the TCP/IP configuration, go to [“Verifying the IP Address in Windows 2000 or Windows XP”](#).

Configuring TCP/IP in Windows XP

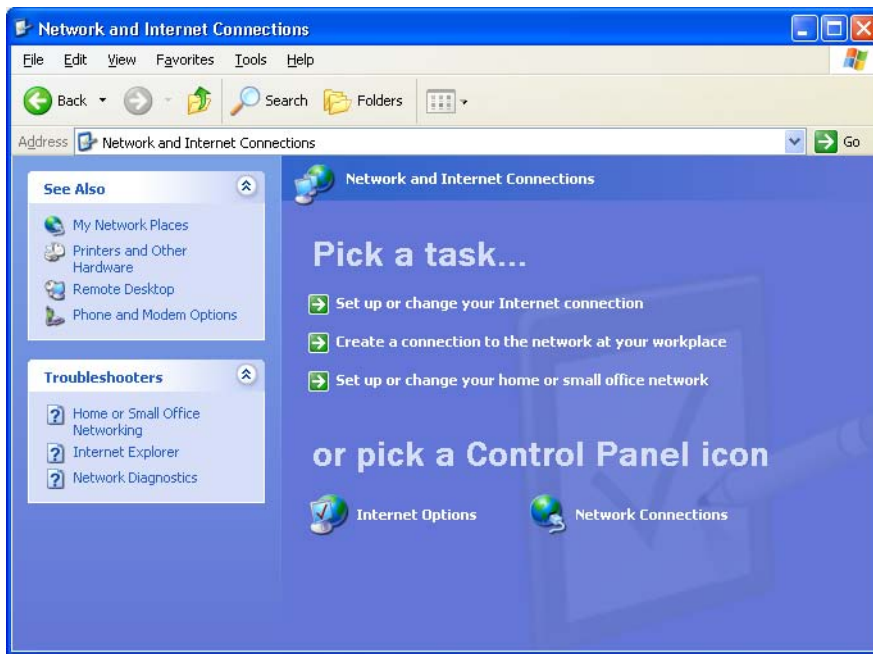
- 1 On the Windows desktop, click **Start** to display the Start window:



- 2 Click **Control Panel** to display the Control Panel window. The display varies, depending on the Windows XP view options. If the display is a Category view as shown below, continue with step 3. Otherwise, skip to step 5.



- Click **Network and Internet Connections** to display the Network and Internet Connections window:

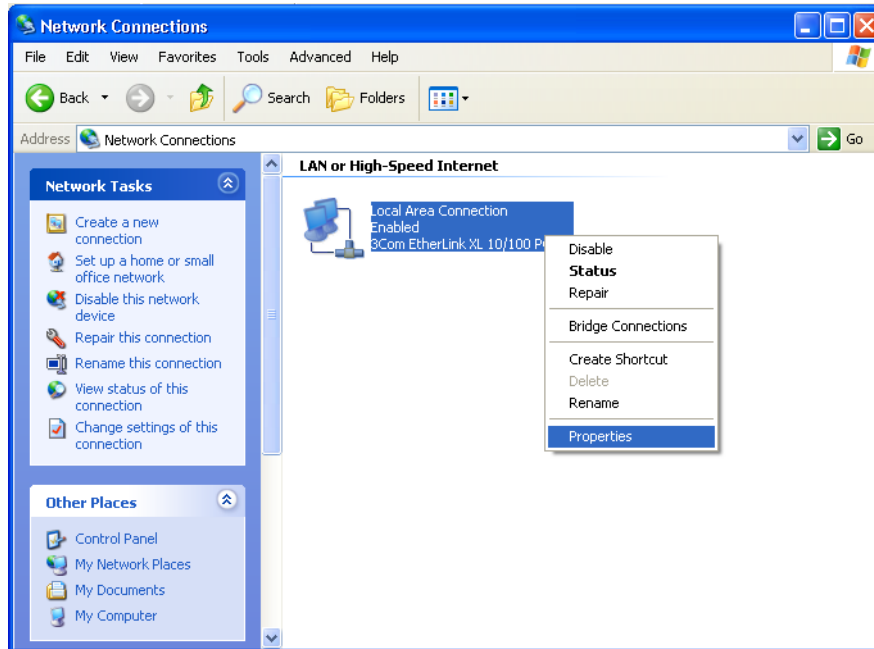


- Click **Network Connections** to display the LAN or High-speed Internet connections. Skip to step 7.
- If a classic view similar to below is displayed:

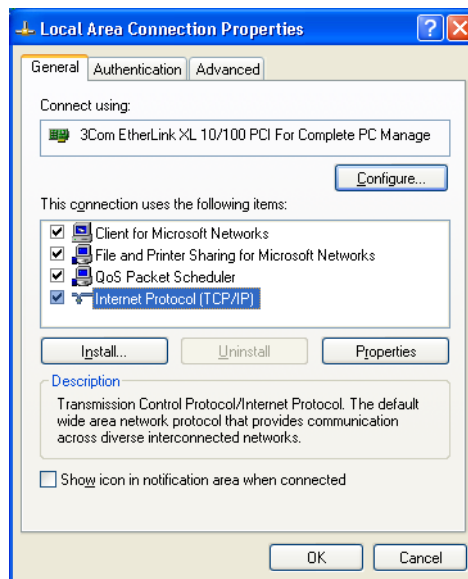


- Double-click **Network Connections** to display the LAN or High-speed Internet connections.

- 7 Right-click on the network connection. If more than one connection is displayed, be sure to select the one for your network interface:

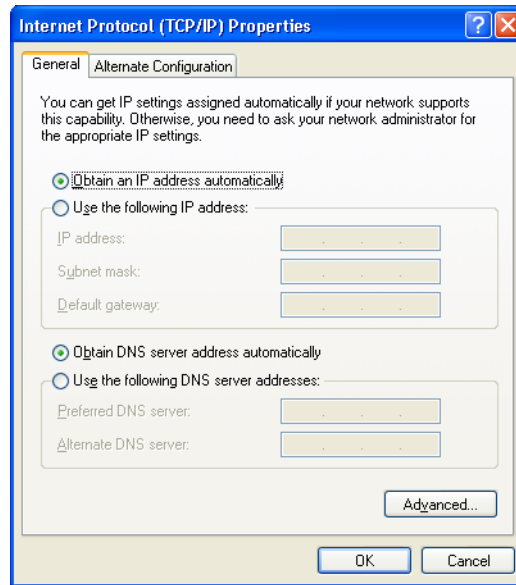


- 8 Select **Properties** from the pop-up menu to display the Local Area Connection Properties window:



- 9 On the Local Area Connection Properties window, select **Internet Protocol (TCP/IP)** if it is not selected.

- 10 Click **Properties** to display the Internet Protocol (TCP/IP) Properties window:



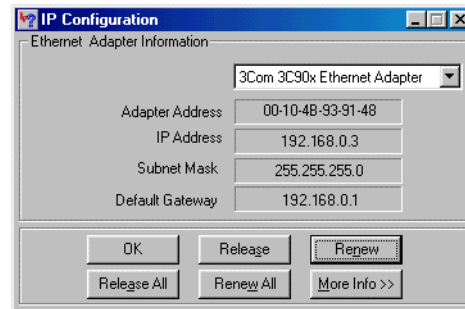
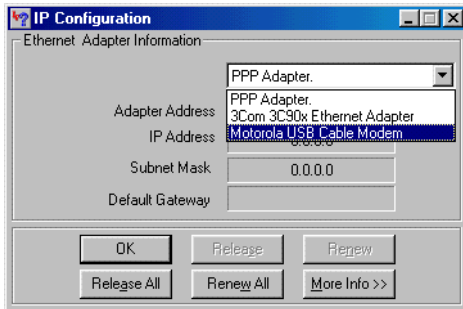
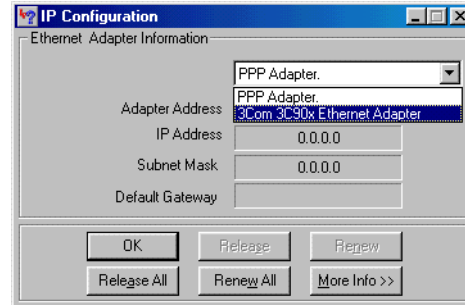
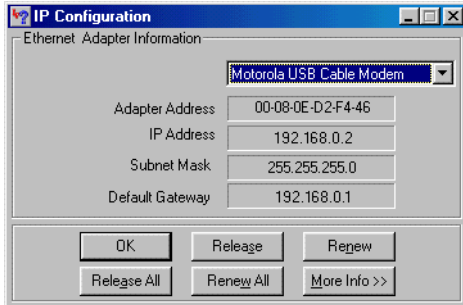
- 11 Verify that the settings are correct, as shown above.
- 12 Click **OK** to close the TCP/IP Properties window.
- 13 Click **OK** to close the Local Area Connection Properties window.

When you complete the TCP/IP configuration, go to [“Verifying the IP Address in Windows 2000 or Windows XP”](#).

Verifying the IP Address in Windows 95, Windows 98, or Windows Me

To check the IP address:

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Run**. The Run window is displayed.
- 3 Type **wiipcfg.exe** and click **OK**. The IP Configuration window is displayed. The Ethernet Adapter Information field will vary depending on the system, as shown in the following examples:



The values for Adapter Address, IP Address, Subnet Mask, and Default Gateway on the PC will be different than in the images.

In Windows 98, if “Autoconfiguration” is displayed before the IP Address as in the following image, call your service provider.

Adapter Address	00-80-C6-E7-59-E6
IP Autoconfiguration Address	169.254.191.251

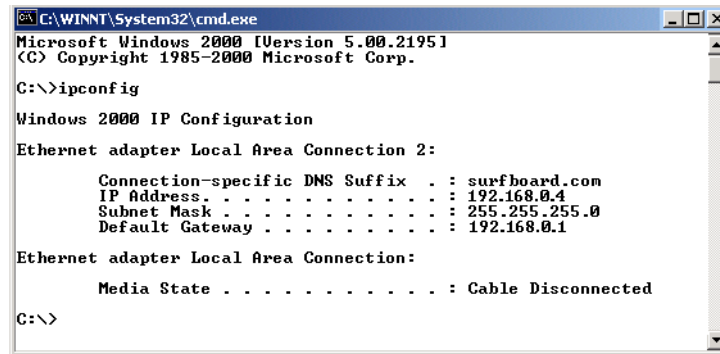
- 4 Select the adapter name — the Ethernet card or USB device.
- 5 Click **Renew**.
- 6 Click **OK** after the system displays an IP address.

If after performing this procedure the computer cannot access the Internet, call your cable provider for help.

Verifying the IP Address in Windows 2000 or Windows XP

To check the IP address:

- 1 On the Windows Desktop, click **Start**.
- 2 Select **Run**. The Run window is displayed.
- 3 Type **cmd** and click **OK** to display a command prompt window.
- 4 Type **ipconfig** and press **ENTER** to display the IP configuration. A display similar to the following indicates a normal configuration:



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

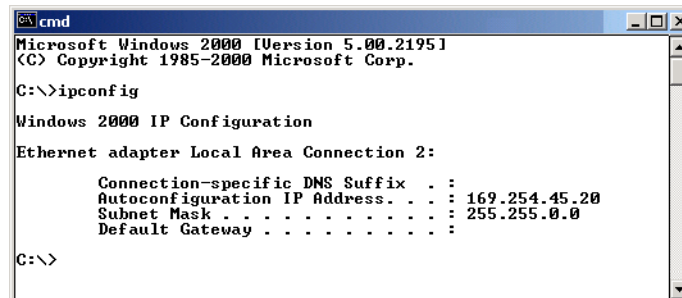
    Connection-specific DNS Suffix  . : surfboard.com
    IP Address. . . . .                : 192.168.0.4
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 192.168.0.1

Ethernet adapter Local Area Connection:

    Media State . . . . .              : Cable Disconnected

C:\>
```

If an Autoconfiguration IP Address is displayed as in the following window, there is an incorrect connection between the PC and the VT2500 or there are cable network problems. Check the cable connections and determine if you can view cable-TV channels on your television:



```
cmd
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

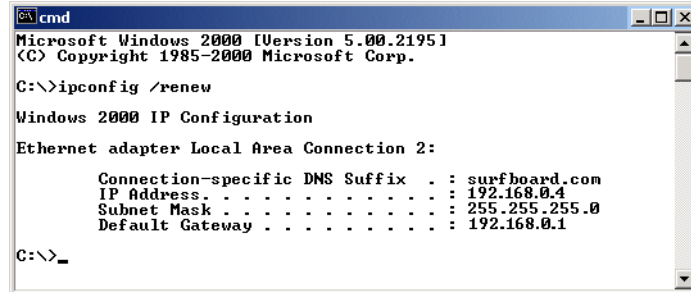
    Connection-specific DNS Suffix  . :
    Autoconfiguration IP Address. . . : 169.254.45.20
    Subnet Mask . . . . .              : 255.255.0.0
    Default Gateway . . . . .          :

C:\>
```

After verifying the cable connections and proper cable-TV operation, renew the IP address.

To renew the IP address:

- 1 Type **ipconfig /renew** and press **ENTER**. If a valid IP address is displayed as shown, Internet access should be available.



```
cmd
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig /renew

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : surfboard.com
    IP Address. . . . .                : 192.168.0.4
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 192.168.0.1

C:\>_
```

- 2 Type **exit** and press **ENTER** to return to Windows.

If after performing this procedure the computer cannot access the Internet, call your cable provider for help.

❖ Setting Up Your Wireless LAN (WLAN)

You can use the [VT2500](#) as an access point for a wireless LAN (WLAN) without changing its default settings.

Caution!



To prevent unauthorized eavesdropping or access to WLAN data, you must enable wireless security. The default [VT2500](#) settings provide no wireless security. After your WLAN is operational, be sure to enable wireless security.

To enable security for your WLAN, you can do the following on the [VT2500](#):

To	Perform	Use in Setup Program
Encrypt wireless transmissions and restrict WLAN access	Encrypting Wireless LAN Transmissions	Wireless > SECURITY — basic page
Further prevent unauthorized WLAN intrusions	Restricting Wireless LAN Access	Wireless > SECURITY — advanced page

Connect at least one computer to the [VT2500](#) Ethernet port to perform configuration. Do not attempt to configure the [VT2500](#) over a wireless connection.

You need to configure each wireless client (station) to access the [VT2500](#) LAN as described in “[Configuring the Wireless Clients](#)”.

Caution!



Never provide your ESSID, WPA or WEP passphrase, or WEP key to anyone who is not authorized to use your WLAN.

For descriptions of all wireless configuration fields, see “[Wireless Pages in the VT2500 Setup Program](#)”.

Another step to improve wireless security is to place wireless components away from windows. This decreases the signal strength outside the intended area.

Encrypting Wireless LAN Transmissions

To prevent unauthorized viewing of data transmitted over your WLAN, you must encrypt your wireless transmissions.

Use the [Wireless > SECURITY — basic](#) to encrypt your transmitted data. Choose one of:

Configure on the VT2500

If all of your wireless clients support Wi-Fi Protected Access (WPA), we recommend you follow [Configuring WPA on the VT2500](#)

Otherwise, perform [If you need to restore the wireless defaults, click Reset Security Defaults.](#)

Required On Each Wireless Client

If you use a local pre-shared key (WPA-PSK) passphrase, you must configure the identical passphrase to the [VT2500](#) on each wireless client. Home and small-office settings typically use a local passphrase.

Configuring a RADIUS server requires specialized knowledge that is beyond the scope of this guide. For more information, contact your network administrator.

You must configure each wireless client with the [VT2500's](#) WEP key (must be identical)

If all of your wireless clients support WPA encryption, we recommend using WPA instead of WEP because WPA:

- Provides much stronger encryption and is more secure
- Provides authentication to ensure that *only* authorized users can log on to your WLAN
- Is much easier to configure
- Uses a standard algorithm on all compliant products to generate a key from a textual passphrase
- Will be incorporated into the new IEEE 802.11i wireless networking standard

For new wireless LANs, we recommend purchasing client adapters that support WPA, such as the [Motorola Wireless Notebook Adapter WN825G](#), [Wireless PCI Adapter WPCI810G](#), and [Wireless USB Adapter WU830G](#).

For more information about the benefits of WPA, see the Wi-Fi Protected Access Web page:

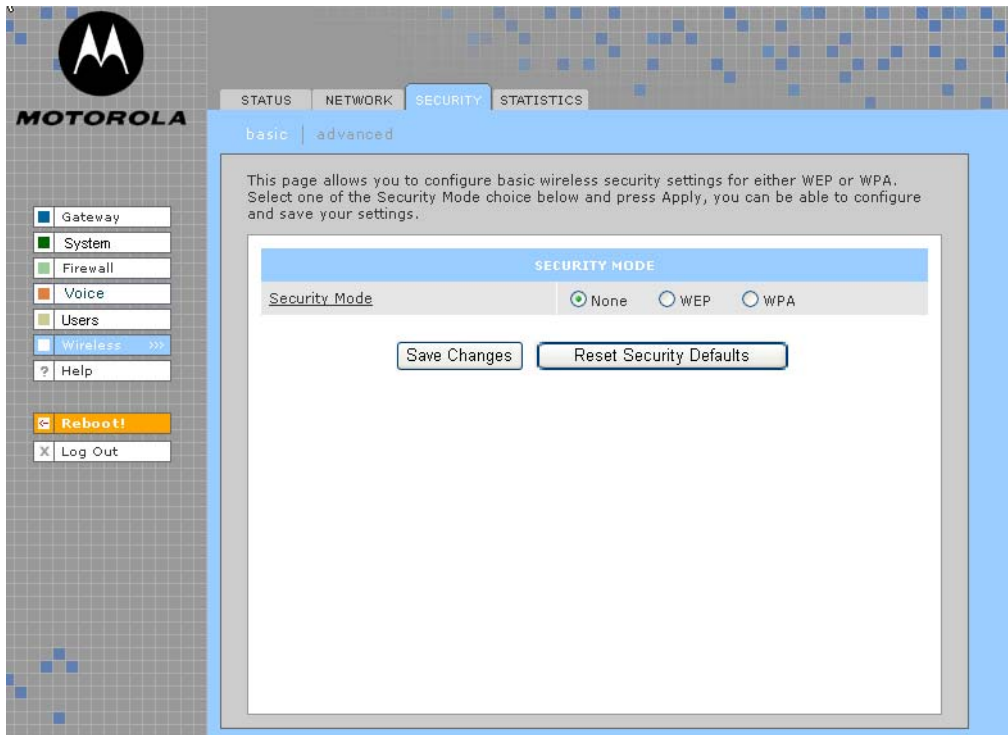
http://www.wifialliance.org/OpenSection/protected_access.asp.

Configuring WPA on the VT2500

After you enable and configure WPA on the VT2500, you must configure each WLAN client as described in the subsections under “[Configuring the Wireless Clients](#)”.

To enable WPA and set the key on the [VT2500](#):

- 1 On the [VT2500](#) Setup Program menu, click **Wireless**.
- 2 Click the **SECURITY** tab to display the [Wireless > SECURITY — basic](#) page:



- 3 In the **Security Mode** field, select **WPA** and click **Apply**.
- 4 Under WPA CONFIGURATION, choose *one* **WPA Encryption** type. *Because performance may be slow with TKIP, we recommend choosing AES if your clients support AES:*

TKIP Temporal Key Integrity Protocol provides data encryption including a per-packet key mixing function, message integrity check (MIC), initialization vector (IV), and re-keying mechanism.

AES The Advanced Encryption Standard algorithm implements symmetric key cryptography as a block cipher using 128-bit keys. We recommend this setting if all of your wireless clients support AES. The Motorola client adapters shown in “[Optional Accessories](#)” support AES.

Group Rekey Interval Set the WPA Group Rekey Interval in seconds. Set to zero to disable periodic rekeying. The value should be from 0 - (2³² - 1).

5 Choose the **WPA Authentication** type:

Remote (Radius) If a Remote Authentication Dial-In User Service (RADIUS) server is available, you can select this option and go to step 6. A RADIUS server is typically used in a large corporate location.

Local (WPA-PSK) If you choose Pre-Shared Key (PSK) local authentication, if the passphrase on any client supporting WPA matches the PSK Passphrase set on the [VT2500](#), the client can access the [VT2500](#) WLAN. To set the PSK Passphrase, go to step 7. A local key is typically used in a home or small office.

6 For **Remote (Radius)** authentication *only*, set:

Radius Port The port used for remote authentication through a RADIUS server. It can be from 0 to 65535.

Radius Key The key for remote authentication. It can be from 0 to 255 ASCII characters.

Radius Server Type Currently IPv4 *only*.

Radius Server The RADIUS server IP address in dotted-decimal format (example: 192.168.102.155).

7 For **Local (WPA-PSK)** authentication *only*, set:

PSK Passphrase The PSK password containing from 8 to 63 ASCII characters. You must set the identical passphrase on each WLAN client (see "[Configuring a Wireless Client for WPA](#)").

8 Click **Save Changes**.

If you need to restore the wireless defaults, click **Reset Security Defaults**.

Configuring WEP on the VT2500

After you enable and configure WEP on the VT2500, you must configure each WLAN client as described in the subsections under “[Configuring the Wireless Clients](#)”.

Use Wired Equivalent Privacy ([WEP](#)) only if you have wireless clients that do not support WPA.

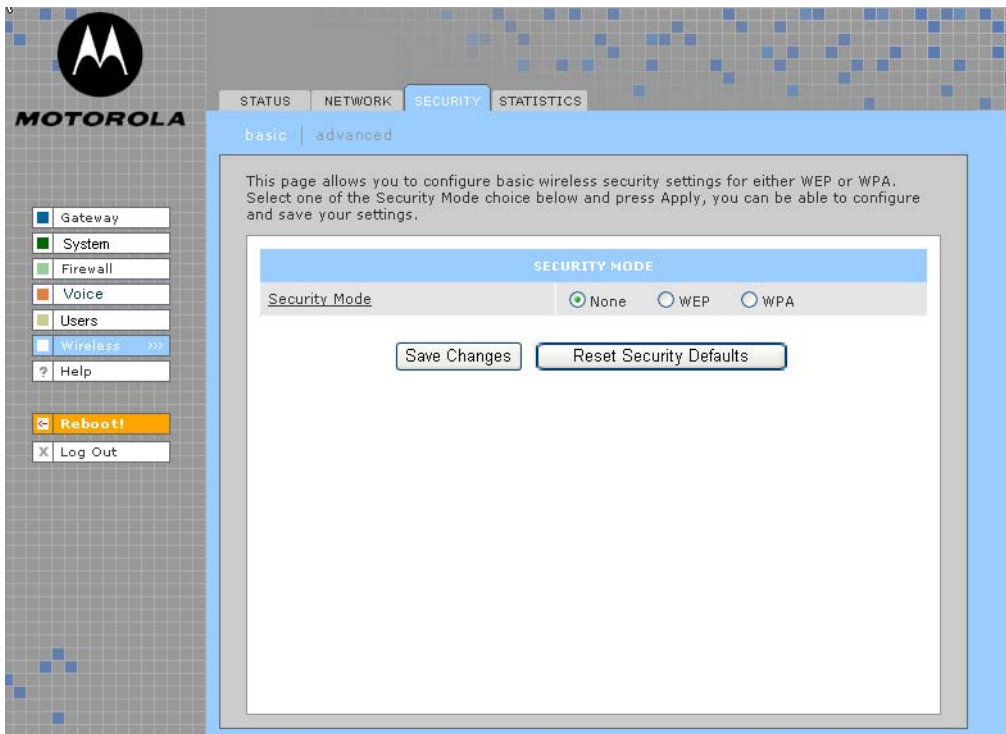
Caution!



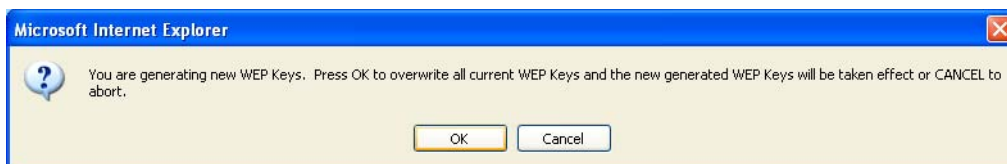
If you use WEP encryption, you must configure the same WEP key on the [VT2500 access point](#) and all wireless clients (stations). *Never provide your WEP key or passphrase to anyone who is not authorized to use your WLAN.*

To enable WEP and set the key on the [VT2500](#):

- 1 On the [VT2500](#) Setup Program menu, click **Wireless**.
- 2 Click the **SECURITY** tab to display the [Wireless > SECURITY — basic](#) page:



- 3 In the **Security Mode** field, select **WEP** and click **Apply**.
- 4 In the **WEP Passphrase** field, type a *passphrase* containing from 8 to 31 ASCII characters. For privacy, your passphrase displays as dots.
- 5 Click **Generate WEP Keys**. The following window is displayed:



6 Click **OK**. The WEP CONFIGURATION fields now appear something like this:

WEP CONFIGURATION		
WEP Passphrase	●●●●●●●●	<input type="button" value="Generate WEP Keys"/>
WEP Authentication	<input type="radio"/> Open	<input checked="" type="radio"/> Shared Key
Encryption	<input checked="" type="radio"/> Enable 64-Bit	<input type="radio"/> Enable 128-Bit
Key Type	Enter 10 HEX chars or 5 ASCII chars	Enter 26 HEX chars or 13 ASCII chars
<input checked="" type="radio"/> Key 1	<input type="text" value="e704d8bce7"/>	<input type="text" value="e704d8bce78be042718adca8b2"/>
<input type="radio"/> Key 2	<input type="text" value="718adca8b2"/>	<input type="text" value="8f4c696d44d10d6b8222d1f978"/>
<input type="radio"/> Key 3	<input type="text" value="8f4c696d44"/>	<input type="text" value="ffbd5918a1b024e93bd2475dc7"/>
<input type="radio"/> Key 4	<input type="text" value="8222d1f978"/>	<input type="text" value="cc1ad6dbfc137c898233206332"/>

Before performing step 7, consider the following:

- If all of your wireless adapters support 128-bit encryption, you can select **Enable 128 Bit**. Otherwise, you must select **Enable 64 Bit**.
- For a WLAN client equipped with a Motorola wireless adapter, you can enter the WEP Passphrase when you perform “[Configuring a Wireless Client for WEP](#)”. For all other wireless adapters, you will probably need to enter the generated WEP key that you designate in step 7.

7 Under WEP CONFIGURATION, set:

- WEP Authentication** Sets whether shared key authentication is enabled to provide data privacy on the WLAN:
- Open System — Any WLAN client can transmit data to any other client without authentication. It is the default, if the Security Mode is set to WEP.
 - Shared Key — The VT2500 authenticates and transfers data to and from all clients having shared key authentication enabled. *We recommend this setting.*
- Encryption** Use a WEP key length that is compatible with your wireless client adapters. Choose *one* of:
- Enable 64-Bit — Use only if you have wireless clients that do not support 128-bit encryption
 - Enable 128-Bit — We recommend this setting for stronger encryption; it is supported by the Motorola WN825G and WPCI810G wireless adapters and most current wireless adapters
- Key Type** (Key 1 to Key 4) Select the active key (1 to 4). Only *one* key can be active. You can generate WEP keys from a passphrase as described in steps 4 to 6 or type non-case-sensitive hexadecimal characters 0 to 9 and A to F to define up to:
- Four 10-character long key 64-bit WEP keys
 - Four 26-character long 128-bit WEP keys
- We recommend changing the WEP keys frequently. Never provide the WEP key to anyone who is not authorized to use your WLAN.*

8 Click **Save Changes** to save your changes.

If you need to restore the wireless defaults, click **Reset Security Defaults**.

Restricting Wireless LAN Access

The default [VT2500](#) wireless settings enable any computer having a compatible wireless adapter to access your WLAN. To protect your network from unauthorized intrusions, you can restrict access to your WLAN to a limited number of computers on the [Wireless > SECURITY — advanced](#) page.

You can configure one or both of:

Configure on the VT2500

Perform [Configuring the Wireless Network Name on the VT2500](#) to disable **Extended Service Set Identifier (ESSID) broadcasting** to enable closed network operation

Perform [Configuring a MAC Access Control List on the VT2500](#) to restrict access to wireless clients with known MAC addresses

Required On Each Wireless Client

You must configure each wireless client with the [VT2500](#)'s ESSID network name (must be identical).

No configuration is required on the client.

Configuring the Wireless Network Name on the VT2500

If you disable ESSID broadcasting on the [VT2500](#), it does not transmit the network name (ESSID). This provides additional protection because:

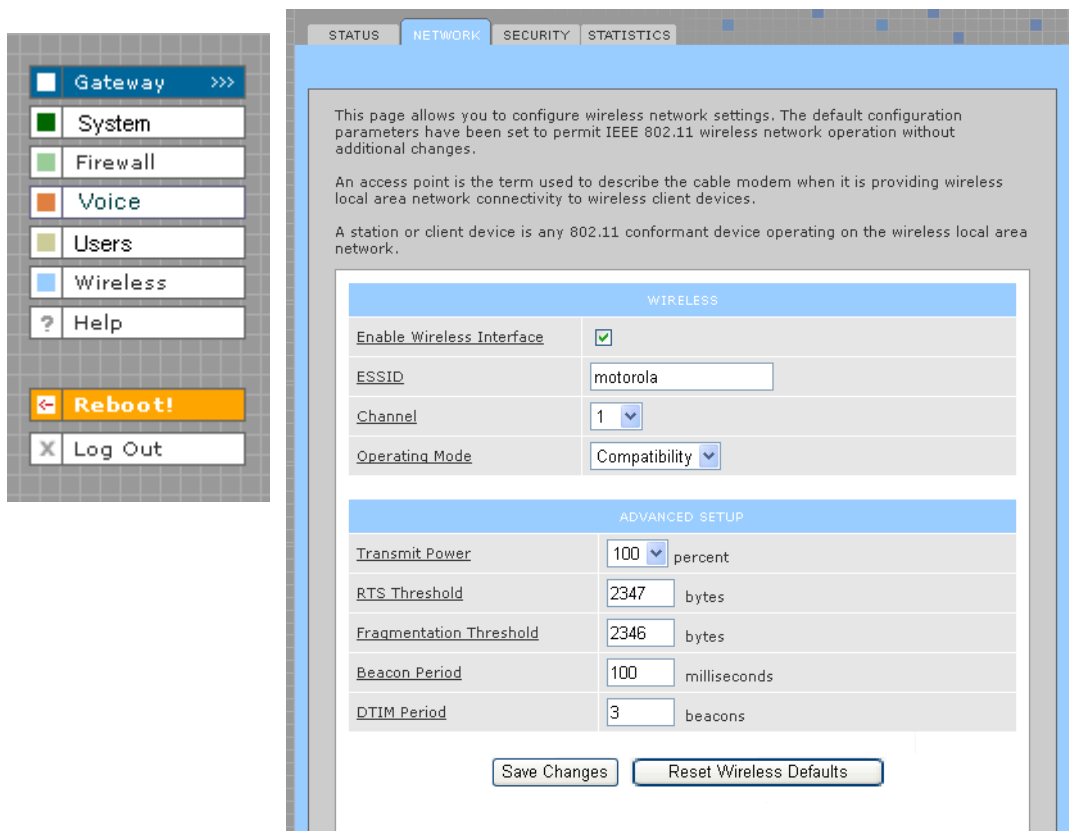
- Only wireless clients configured with your network name can communicate with the [VT2500](#)
- It is more difficult for unauthorized individuals who scan for unsecured WLANs to access your WLAN

Closed network operation is an enhancement of the IEEE 802.11b and IEEE 802.11g standards.

If you select Disable ESSID Broadcast, you must also perform [Configuring a Wireless Client with the Network Name \(ESSID\)](#) on all WLAN clients (stations). Never provide your ESSID to anyone who is not authorized to use your WLAN.

To configure the ESSID on the [VT2500](#):

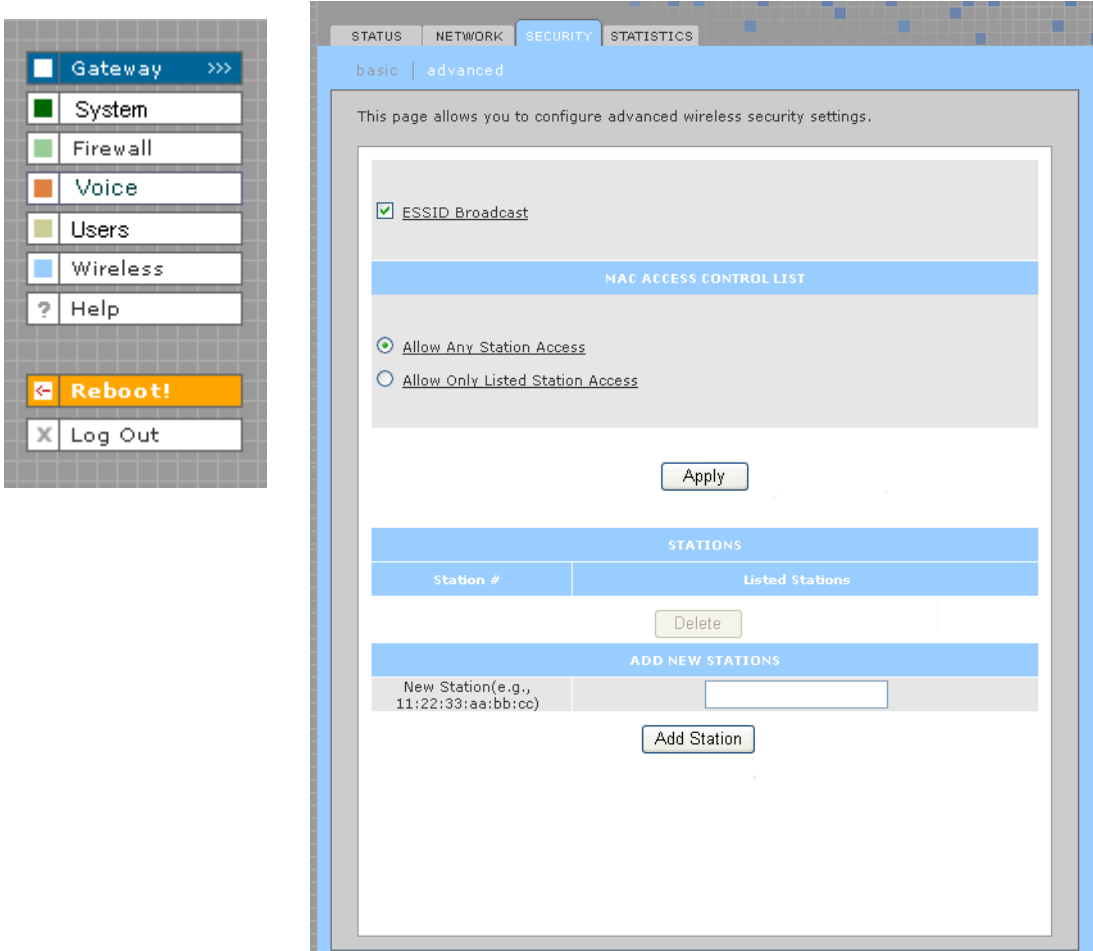
- 1 Start the [VT2500 Setup Program](#) as described in “[Starting the VT2400/VT2500 Voice Gateway Setup Program](#)”.
- 2 On the Setup Program menu, click **Wireless**.
- 3 Click the **NETWORK** tab to display the [Wireless > NETWORK](#) page:



- 4 In the **ESSID** field, type a unique **name**. It can be any alphanumeric, case-sensitive string up to 32 characters. The default is “Motorola.” *Do not use the default ESSID.*
- 5 Click **Save Changes** to save your changes.

6 To restrict WLAN access to clients configured with the same Network Name (ESSID) as the [VT2500](#), click the **SECURITY** tab.

7 Click **advanced** to display the [Wireless > SECURITY — advanced](#) page:



8 Select **ESSID Broadcast** to restrict WLAN access to clients configured with the same Network Name (ESSID) as the [VT2500](#).

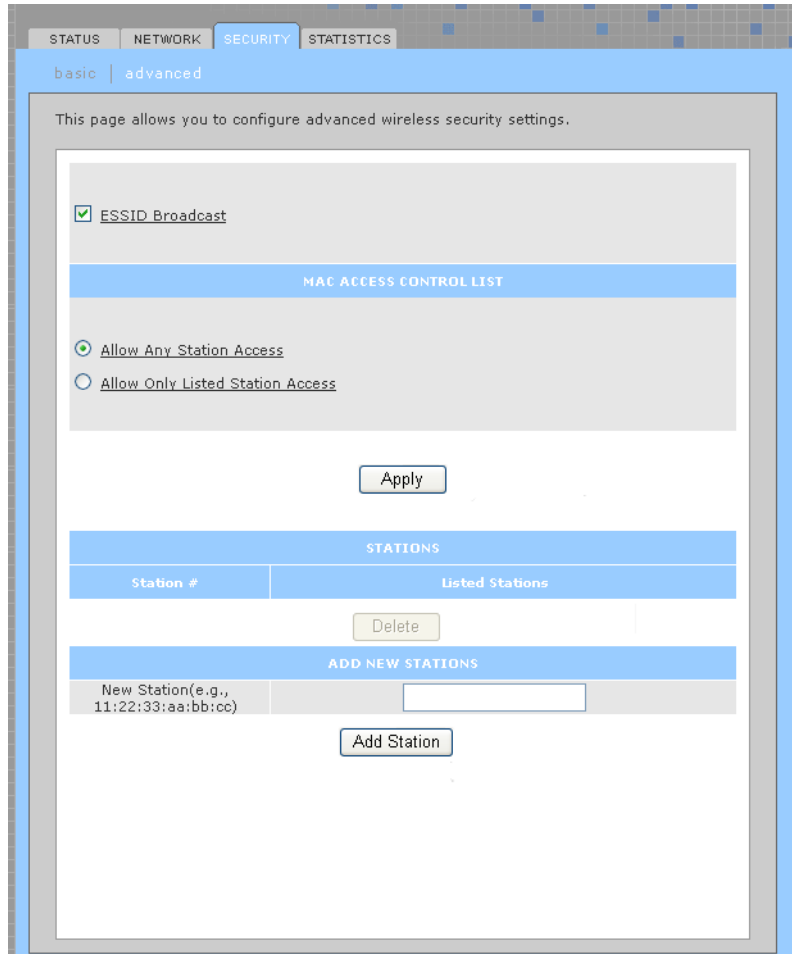
9 Click **Apply** to save your changes.

Configuring a MAC Access Control List on the VT2500

You can restrict wireless access to one to 32 wireless clients, based on the client MAC address.

To configure a MAC access control list:

- 1 On the [VT2500](#) Setup Program menu, click **Wireless**.
- 2 Click the **SECURITY** tab.
- 3 Click **advanced** to display the [Wireless > SECURITY — advanced](#) page:



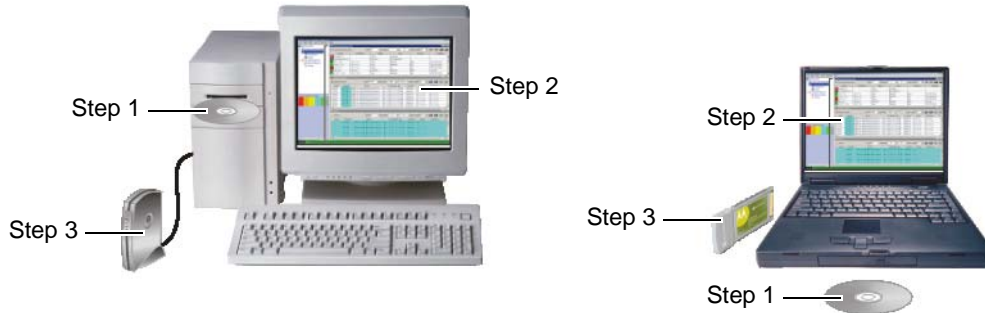
- 4 To restrict wireless access to systems in the MAC access control list, select **Allow Only Listed Stations Access** and click **Apply**.
- 5 To add a wireless client, type its MAC address in the format **xx:xx:xx:xx:xx:xx** in the **New Station** field and click **Add Station**.

You can add up to 32 wireless clients to the MAC access control list.

Configuring the Wireless Clients

For each wireless client computer (station), install the wireless adapter — such as a Motorola [WN825G](#), [WPCI810G](#), or [WU830G](#) — following the instructions supplied with the adapter. Be sure to:

- 1 Insert the CD-ROM for the adapter in the CD-ROM drive on the client.
- 2 Install the device software from the CD.
- 3 Insert the adapter in the PCMCIA or PCI slot or connect it to the USB port.



Configure the adapter to obtain an IP address automatically. The Motorola wireless adapters are supplied with a client configuration program called Wireless Client Manager, which is installed in the Windows Startup group.

On a PC with Wireless Client Manager installed, the  icon is displayed on the Windows task bar. Double-click the icon to launch the utility.

You may need to do the following to use a wireless client computer to surf the Internet:

If You Performed:

[Configuring WPA on the VT2500](#)

[If you need to restore the wireless defaults, click Reset Security Defaults.](#)

[Configuring the Wireless Network Name on the VT2500](#)

[Configuring a MAC Access Control List on the VT2500](#)

On Each Client, You Need to Review:

[“Configuring a Wireless Client for WPA”](#)

[“Configuring a Wireless Client for WEP”](#)

[“Configuring a Wireless Client with the Network Name \(ESSID\)”](#)

No configuration on client required

Configuring a Wireless Client for WPA

If you enabled WPA and set a PSK Passphrase by “[Configuring WPA on the VT2500](#)”, you must configure the same passphrase (key) on each wireless client. The VT2500 cannot authenticate a client if:

- WPA is enabled on the VT2500 but not on the client
- The client passphrase does not match the VT2500 PSK Passphrase

For information about the WPA support in Windows XP, visit:

WPA Wireless Security for Home Networks

<http://www.microsoft.com/WindowsXP/expertzone/columns/bowman/03july28.asp>

Overview of the WPA Wireless Security Update in Windows XP

<http://support.microsoft.com/?kbid=815485>

You can download the Microsoft Windows XP Support Patch for WPA from

<http://www.microsoft.com/downloads/details.aspx?FamilyId=009D8425-CE2B-47A4-ABEC-274845DC9E91&displaylang=en>.

Caution!



Never provide the PSK Passphrase to anyone who is not authorized to use your WLAN.

Configuring a Wireless Client for WEP

If you enabled WEP and set a key by [If you need to restore the wireless defaults, click Reset Security Defaults.](#), you must configure the same WEP key on each wireless client. The VT2500 cannot authenticate a client if:

- Shared Key Authentication is enabled on the VT2500 but not on the client
- The client WEP key does not match the VT2500 WEP key

On a WLAN client equipped with a Motorola wireless adapter, you can enter the WEP Passphrase you set when you configured the VT2500. For all other wireless adapters, you must enter the 64-bit or 128-bit WEP key generated by the VT2500.

Caution!



Never provide the WEP key to anyone who is not authorized to use your WLAN.

Configuring a Wireless Client with the Network Name (ESSID)

To distinguish it from other nearby WLANs, you should identify your WLAN with a unique network name (also known as a network identifier or ESSID). As you configure a wireless client, you will be prompted for the network identifier, network name, or ESSID; type the same **name** that appears in the ESSID field on the [Wireless > NETWORK](#) page in the VT2500 Setup Program (see [Wireless > NETWORK](#) for details). If the network name is not configured yet, see “[Configuring the Wireless Network Name on the VT2500](#)” to configure it.

After you specify the network name, many wireless cards or adapters automatically scan for an access point such as the VT2500 and the proper channel and data rate. If your card requires you to manually start scanning for an access point, do so following the instructions in the documentation supplied with the card.

Wireless Pages in the VT2500 Setup Program

Use the Wireless pages to control and monitor the wireless interface:

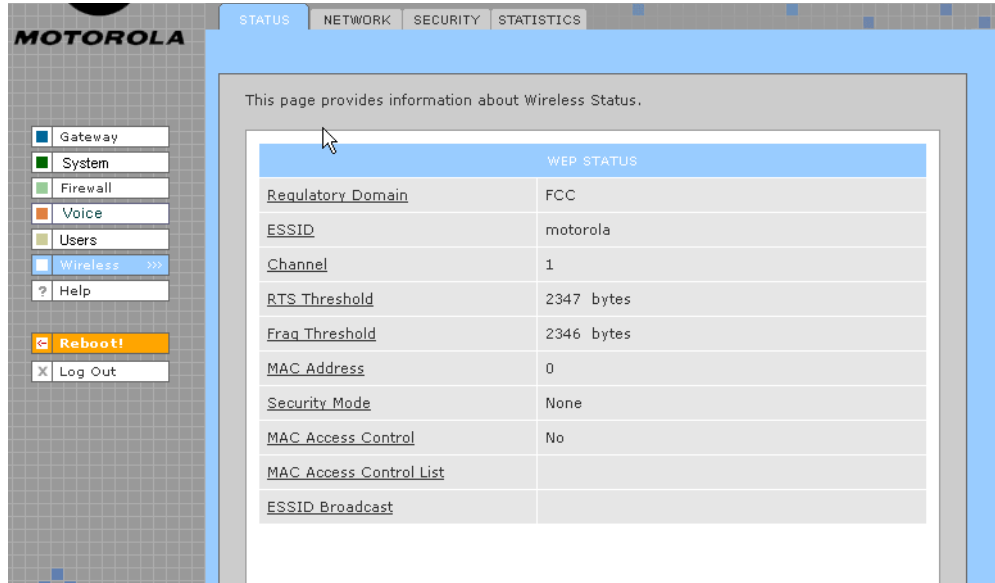
- [Wireless > STATUS](#) page
- [Wireless > NETWORK](#) page
- [Wireless > SECURITY — basic](#) page
- [Wireless > SECURITY — advanced](#) page
- [Wireless > STATISTICS](#) page

After you edit some fields and click Apply, you are required to reboot your voice gateway for your changes to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log in again.

Wireless > STATUS

You can use this read-only page to:

- View the wireless interface status
- Help perform [Troubleshooting](#) for wireless network problems



Wireless > STATUS Page Fields

- Regulatory Domain** Indicates the country for which the [VT2500](#) is manufactured. The list of channels depends on the country's standards for operation of wireless devices. Depending on the domain set at the factory, USA FCC, Europe, Spain, France, Japan, or some other country name is displayed. **The equipment version marketed in the United States is restricted to usage of channels 1 through 11 only.**
- ESSID** Displays the ESSID set on the [Wireless > NETWORK](#) page. For more information, see "[Configuring the Wireless Network Name on the VT2500](#)". *Never provide the ESSID to anyone who is not authorized to use your WLAN.*
- Channel** Displays the radio channel for the access point. If you encounter interference, you can set a different channel on the [Wireless > NETWORK](#) page.
- RTS Threshold** Displays the Request to Send Threshold set on the [Wireless > NETWORK](#) page.
- Frag Threshold** Displays the Fragmentation Threshold set on the [Wireless > NETWORK](#) page.
- MAC Address** Displays the [VT2500](#) MAC address.
- Security Mode** Displays the enabled wireless encryption type. For more information, see "[Configuring WPA on the VT2500](#)" or "[Configuring WEP on the VT2500](#)".
- MAC Access Control** Displays the MAC Access Control setting (see "[Configuring a MAC Access Control List on the VT2500](#)"):
 - Allow Listed — Only clients in the MAC access control list can access the WLAN.
 - Allow Any Station Access — Any wireless client can access the WLAN.



Wireless > STATUS Page Fields (continued)

MAC Access Control List Displays the MAC addresses of wireless clients having access (see “[Configuring a MAC Access Control List on the VT2500](#)”).

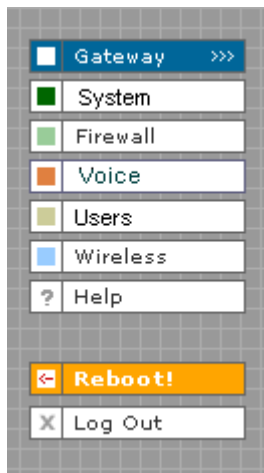
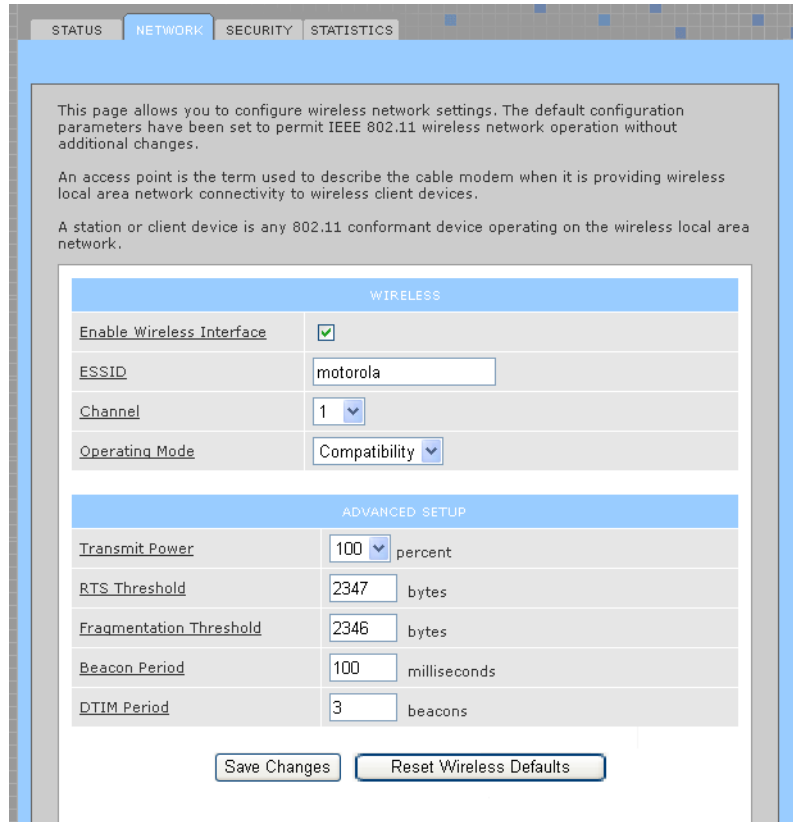
ESSID Broadcast If you disable ESSID broadcast, the network name (ESSID) will not be transmitted in the 802.11 beacon frame. This provides some additional protection for your network because only 802.11 stations that know your network name can be configured to associate with the SBG. Note: Disable ESSID broadcast operation is not part of the IEEE 802.11 standard.

Wireless > NETWORK

Use this page for:

- Enabling the wireless interface
- Configuring the wireless network name (also see [Configuring the Wireless Network Name on the VT2500](#))
- Configuring other WLAN settings

You can use the [VT2500](#) to operate a WLAN without changing its default settings.

The screenshot shows the 'Wireless' configuration page. It includes a 'WIRELESS' section with 'Enable Wireless Interface' checked, 'ESSID' set to 'motorola', 'Channel' set to '1', and 'Operating Mode' set to 'Compatibility'. Below this is an 'ADVANCED SETUP' section with fields for 'Transmit Power' (100 percent), 'RTS Threshold' (2347 bytes), 'Fragmentation Threshold' (2346 bytes), 'Beacon Period' (100 milliseconds), and 'DTIM Period' (3 beacons). At the bottom are 'Save Changes' and 'Reset Wireless Defaults' buttons.

Wireless > NETWORK page fields

Field	Description
WIRELESS	

Wireless > NETWORK page fields (continued)

Field	Description
Enable Wireless Interface	Select this box to enable the wireless interface.
ESSID	Sets a unique network name for the VT2500 WLAN to distinguish between multiple WLANs in the vicinity. <i>If you select Disable ESSID Broadcast on the Wireless > SECURITY — advanced page, all clients on the WLAN must have the same ESSID (network name) as the VT2500. It can be any alphanumeric, case-sensitive string up to 32 characters. The default is "Motorola." We strongly recommend not using the default. Never provide the ESSID to anyone who is not authorized to use your WLAN.</i>
Channel	Sets the wireless radio channel. You can change the channel if you encounter interference on the default channel. The default is 1 (one), except in countries where the first channel permitted for wireless operation is not one.
Operating Mode	Sets how the VT2500 communicates with wireless clients (stations): <ul style="list-style-type: none">• 11b/11g Standard — Enables all IEEE 802.11b and IEEE 802.11g clients to work with the VT2500. We recommend using this default setting in most cases because it is more flexible.• 11g Enhanced — Choose this option only if all IEEE 802.11g client adapters on the network support the performance-enhancing features of the IEEE 11g Enhanced mode. It is not supported by all IEEE 802.11g adapters.

ADVANCED SETUP

Transmit Power	Sets the VT2500 wireless transmission power — 3, 6, 12, 25, 50, 75, or 100%. The default is 100%. You can lower the Transmit Power to: <ul style="list-style-type: none">• Decrease "leakage" into outside areas, such as the street• Improve performance if you usually position your computer or laptop close to your VT2500 Transmission power control is an optional IEEE 802.11 feature.
RTS Threshold	The Request To Send Threshold sets the minimum packet size for which the VT2500 issues an RTS before sending a packet. A low RTS threshold can help when many clients are associated with the VT2500 , or the clients are far apart and can detect the VT2500 but not each other. It can be 0 to 2347 bytes. The default is 2347.
Fragmentation Threshold	Sets the size at which packets are fragmented (sent as several packets instead of as one packet). A low fragmentation threshold can help when communication is poor or there is a significant interference. It can be 256 to 2346 bytes. The default is 2346.
Beacon Period	Sets the time between beacon frames sent by the VT2500 for wireless network synchronization. It can be from 1 to 999 ms. The default is 100 ms.

SECOND PAGE ONLY

DTIM Period	The delivery traffic indication message (DTIM) period is the number of beacon periods that elapse before a wireless client operating in power save mode "listens" for buffered broadcast or multicast messages from the VT2500 . It can be from 1 to 99999. The default is 3.
--------------------	---

[Save Changes \(button\)](#)

[Reset Wireless Defaults \(button\)](#)

Wireless > SECURITY — basic

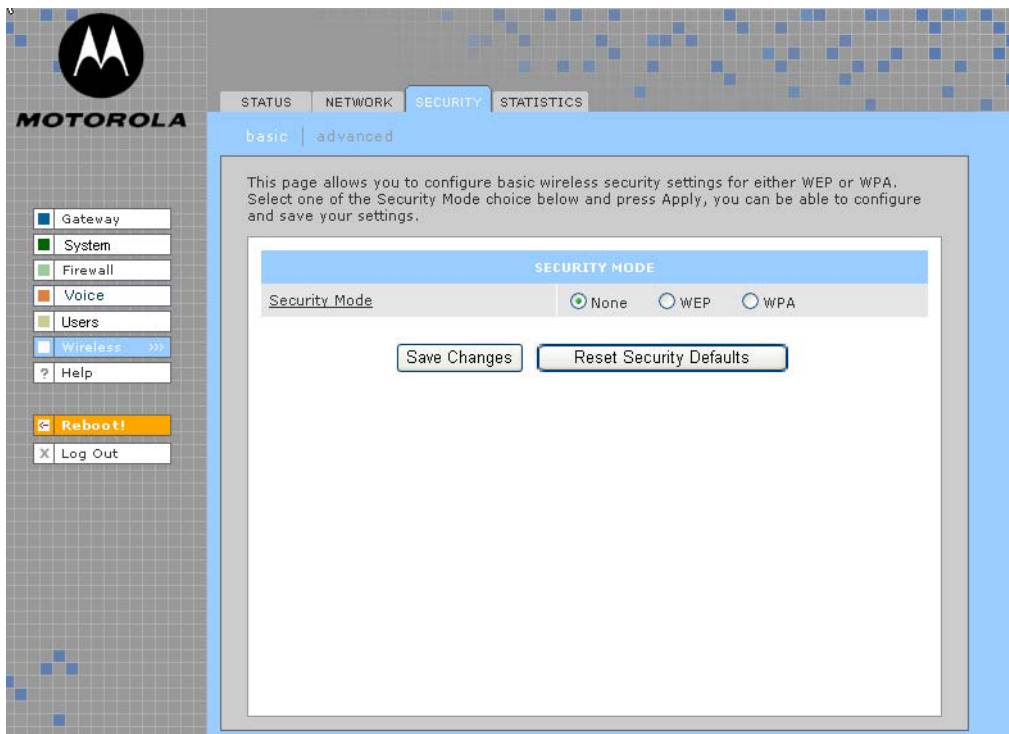
Use this page to configure how your VT2500 encrypts wireless transmissions. For information about using this page, review “[Encrypting Wireless LAN Transmissions](#)” in this section of the manual.

After you enable and configure WEP or WPA on the VT2500 by performing “[Configuring WPA on the VT2500](#)” or “[Configuring WEP on the VT2500](#)” (all options on the [Wireless > SECURITY — basic](#) page are described in these procedures), you must configure each WLAN client as described in the subsections under “[Configuring the Wireless Clients](#)”.

Caution!

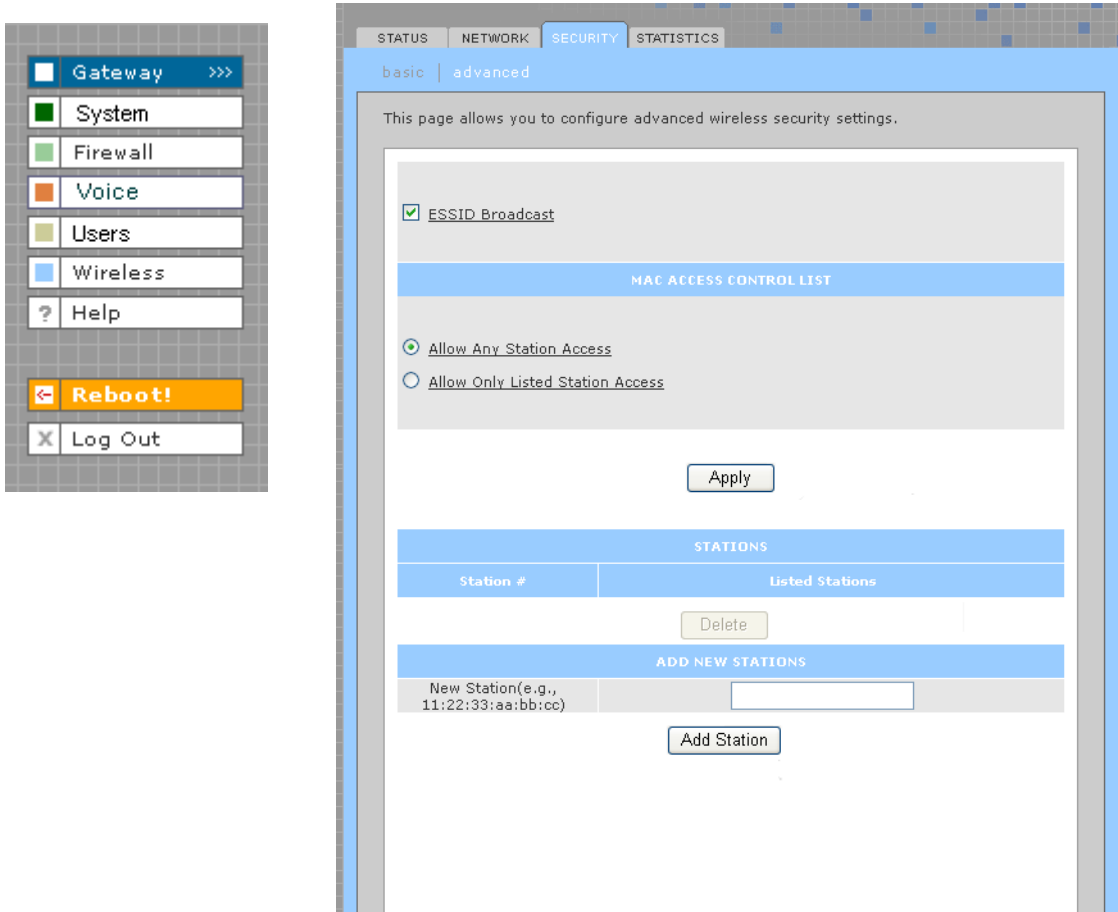


The default Security Mode setting None provides no security for transmitted data.



Wireless > SECURITY — advanced

Use this page to configure advanced wireless security settings.



Wireless > Security — ADVANCED page fields

Field or Button	Description
ESSID Broadcast	If selected, only wireless clients (stations) having the same Network Name (ESSID) as the VT2500 can communicate with the VT2500. Closed network operation is a VT2500 enhancement to IEEE 802.11b. The default is not selected (off).
MAC ACCESS CONTROL LIST	You can restrict wireless access to one to 32 wireless clients, based on the client MAC address.
Allow Any Station Access	If selected, any wireless client can access the VT2500 WLAN.
Allow Only Listed Stations Access	If selected, only wireless clients in the MAC access control list can access the VT2500 WLAN.
Apply (button)	Click to apply your change.
Station #	
Listed Stations	Lists the wireless clients in the MAC access control list having access if Allow Only Listed Stations Access is selected.

Wireless > Security — ADVANCED page fields (continued)

Field or Button	Description
Delete (button)	To delete a wireless client from the MAC access control list, select its Delete check box and click the Delete button.
ADD NEW STATIONS	
New Station (now Station #?)	Type the MAC address of the wireless client to add to the MAC access control list. Use the format xx:xx:xx:xx:xx:xx. The MAC access control list can contain one to 32 clients.
Add Station (button)	Click to add the New Station to the MAC access control list.

Wireless > STATISTICS

Use this page to display wireless statistics.

This page provides information about Wireless Stats.

WIRELESS STATISTICS	
Transmitted Fragment Count	1263
Multicast Transmitted Fragment Count	1262
Failed Count	1
Retry Count	0
Multiple Retry Count	0
Frame Duplicate Count	1
Request to Send Success Count	3341
Request to Send Failure Count	1996
Acknowledge Failed Count	0
Received Fragment Count	11
Multicast Received Fragment Count	11
Frame Check Sequence Error Count	10155
Transmitted Frame Count	1265
WEP Undecryptable Count	0

Refresh

Wireless > STATISTICS page fields

Field or Button	Description
-----------------	-------------

WIRELESS STATISTICS

Transmitted Fragment Count	The number of acknowledged MAC protocol data units (MPDUs) with an address in the address 1 field or an MPDU with a multicast address in the address 1 field of type data or management.
Multicast Transmitted Fragment Count	The number of transmitted fragments when the multicast bit is set in the destination MAC address of a successfully transmitted MAC service data unit (MSDU). When operating as a STA in an ESS, where these frames are directed to the AP, this implies having received an acknowledgment to all associated MPDUs.
Failed Count	The number of MSDUs not transmitted successfully because the number of transmit attempts exceeded the IEEE 802.11b short or long retry limit.
Retry Count	The number of successfully transmitted MSDUs after one or more retransmissions.

Wireless > STATISTICS page fields (continued)

Field or Button	Description
Multiple Retry Count	The number of successfully transmitted MSDUs after more than one retransmission.
Frame Duplicate Count	The number of frames received where the Sequence Control field indicated the frame was a duplicate.
Request To Send Success Count	The number of CTS messages received in response to RTS messages.
Request To Send Failure Count	The number of CTS messages not received in response to RTS messages.
Acknowledge Failed Count	The number of acknowledgment messages not received when expected from a data message transmission.
Received Fragment Count	The number of successfully received MPDUs of type Data or Management.
Multicast Received Fragment Count	The number of MSDUs received when the multicast bit was set in the destination MAC address.
Frame Check Sequence Error Count	The number of FCS errors detected in a received MPDU.
Transmitted Frame Count	The number of successfully transmitted MSDUs.
WEP Undecryptable Count	This number of frames received with the WEP subfield of the Frame Control field set to one and the WEP On key value mapped to the client MAC address. This indicates that the frame should not have been encrypted or was discarded due to the receiving client not having WEP enabled.
Refresh (button)??	Click to collect new data.

❖ Troubleshooting

If the solutions listed here do not solve your problem, contact your cable provider. Before calling your cable provider, try pressing the reset button on the rear panel. Resetting the VT2500 may take 5 to 30 minutes. Your service provider may ask for the status of the lights as described in [“Front-Panel Lights and Error Conditions”](#).

Problem	Possible Solutions
Green POWER light is off	<p>Check that the AC power adapter is properly plugged into the electrical outlet and the VT2400/VT2500.</p> <p>Check that the electrical outlet is working.</p>
Cannot send or receive data or phone calls or	<p>Be sure the telephone line cord is connected to the VT2400/VT2500.</p> <p>Check all other cabling between the modem, the VT2400/VT2500, and the computer. Be sure you used the cables provided with the VT2400/VT2500. All Ethernet cables must be straight-through cables.</p>
No dial tone	<p>Check the lights on the modem front panel. For information, see your broadband modem user guide.</p> <p>Check the POWER light (see “Front Panel” on page 5).</p>
A wireless client(s) cannot send or receive data (VT2500 only)	<ul style="list-style-type: none">• Be sure that your wireless adapter (PCI card, Notebook or Ethernet adapter) on the PC is installed correctly and is active.• Be sure that your wireless adapter's radio signal is enabled. Review your adapter's documentation for further instructions.• Be sure that your wireless adapter for your PC and the wireless router security settings are the same so that it will allow your computer to access the wireless network. Also, verify that the list of <i>Restricted Wireless MAC Addresses</i> (on the WIRELESS Page of the Web-based Configuration Utility is not configured to block your PC. For details on adjusting your security settings, please refer to the descriptions of the WIRELESS and SECURITY Pages in Section 3: Configuration.• Be sure that your wireless adapter is within range of the voice gateway and is not behind an obstruction. For example, metal structures will interfere with the signal, as will 2.4 GHz cordless phones and microwaves.• Be sure that the PC's wireless adapter antenna is properly connected.
A wired client cannot send or receive data (VT2400/VT2500)	<ul style="list-style-type: none">• If you have cable TV, check that the TV is working and the picture is clear. If you cannot receive regular TV channels, the data service will not function.• Check the coaxial cable at the SBG900 and wall outlet. Hand-tighten if necessary.• Check the IP address. Follow the steps for verifying the IP address for your system. See “Configuring TCP/IP”. Call your cable provider if you need an IP address.• Check that the Ethernet cable is properly connected to the SBG900 and the computer.
Slow wireless transmission speed with SPA enabled	<ul style="list-style-type: none">• On the Wireless > SECURITY — basic page, check whether the WPA Encryption type is TKIP. If all of your wireless clients support AES, change the WPA Encryption to AES as described in step 4 in “Configuring WPA on the VT2500” on page 96.”

Front-Panel Lights: Status and Error Conditions

Light	Color	Description
Power	Green	Indicates if the product has power.
Status	Green	Indicates the state the product is in: One blink (every two seconds) - performing initial boot sequence Two blinks - obtaining network IP address Three blinks - Downloading its configuration profile from your VoIP provider
WLAN	Green	Indicates activity on the wireless interface
WAN	Green and Amber	Indicates activity on the WAN and link speed Green = 100baseT, Amber = 10baseT
LAN1	Green or Amber	Indicates activity on the LAN port and link speed Green = 100baseT, Amber = 10baseT
LAN2	Green or Amber	Indicates activity on the LAN port and link speed Green = 100baseT, Amber = 10baseT
LAN3	Green or Amber	Indicates activity on the LAN port and link speed Green = 100baseT, Amber = 10baseT
LAN4	Green or Amber	Indicates activity on the LAN port and link speed Green = 100baseT, Amber = 10baseT
Line 1 and Line 2	Green	Indicates status of line 1: Off - service is not present on the line One blink - The line is off the hook Continuous blink - Attempting to reregister with your VoIP provider after an interruption in service (see PSTN failover in " Rear Panel " on page 7) Solid - Successfully registered with your VoIP provider



Contact Us

If you need assistance while working with the [VT2400/VT2500](#), contact your cable provider. For more information about customer service, technical support, or warranty claims, see the *Regulatory, Safety, Software License, and Warranty Information* card provided with the [VT2400/VT2500](#).

For answers to typical questions, see “[Frequently Asked Questions](#)” on page 119.

For more information about Motorola consumer cable products, education, and support, visit <http://broadband.motorola.com/consumers>.

❖ Frequently Asked Questions

If you do not understand a term or acronym, check the [Glossary](#).

Q What does the Motorola voice terminal do?

A The [VT2400/VT2500 Voice Gateway](#) is part stand-alone media terminal adapter (S-MTA) and part home broadband router:

- As an S-MTA, it converts analog voice signals to and from a standard telephone to digital data that can be transmitted through a broadband connection across the Internet. It provides an alternate means to make voice calls.
- It provides basic routing to enable simultaneous voice and data communication.

Q Will the [VT2400/VT2500 Voice Gateway](#) work with a cable modem or DSL modem?

A Yes. The [VT2400/VT2500 Voice Gateway](#) supports [DHCP](#), which is specified for [DOCSIS](#) cable modems, and [PPPoE](#), which is used by most DSL providers.

Q Can end users operate a virtual private network (VPN) application behind the [VT2400/VT2500](#)?

A Yes. The [VT2400/VT2500 Voice Gateway](#) supports [IPSEC](#) and [PPTP](#), the most common VPN protocols.

Q Can the end user play online games through their [VT2400/VT2500](#)?

A By default, the [VT2400/VT2500 Voice Gateway](#) blocks all unsolicited messages to the computer or end-user network as a standard security measure. However, for online games that require some unsolicited messages to be transmitted through the [VT2400/VT2500](#), the end user can specify ports and IP addresses on which to allow unsolicited messages. The [VT2400/VT2500 Voice Gateway](#) enables the end user to set up virtual servers or a [DMZ](#).

Q How does the end user configure the [VT2400/VT2500](#)?

A *Most end users who perform the appropriate installation procedure in “[Connecting the VT2400/VT2500 to a Network](#)” can send and receive calls immediately!* Configuring your home or office network is done through a GUI where configuration options are selected using a connected PC configured to use DHCP to obtain its network IP address (see “[Gateway > WAN — DHCP Client](#)” on page 34). Or, the user can configure the computer statically to 192.169.102.xxx (xxx is from 2 to 254), subnet 255.255.255.0, and default gateway 192.168.102.1 (see “[Gateway > WAN — Static](#)” on page 36). Or, the user can configure a DSL connection by using the PPPoE Client configuration method (see “[Gateway > WAN — PPPoE Client](#)” on page 35).

Q What is included with the built-in Ethernet router and wireless access point?

A The [VT2400/VT2500 Voice Gateway](#) supports a firewall, RIP, parental control, port triggers, advanced ALGs such as RSVP, POP3, **SNMP**, and streaming media. No separate routers or wireless access points are needed.

Q Is any Quality of Service (QoS) implemented on the [VT2400/VT2500 Voice Gateway](#)?

A Although VoIP service is typically best-effort, the [VT2400/VT2500](#) provides upstream voice prioritization to ensure that upstream voice data has priority over other Web data. This ensures good voice quality even during heavy upstream data transfers, such as e-mail synchronization or file sharing.



Q What voice protocols and CODECs does the [VT2400/VT2500 Voice Gateway](#) support?

A Refer to “[Supported VoIP Protocols, Codecs, and Calling Features](#)” on page 1.

❖ Specifications

General

WAN and PC interfaces	1 WAN 10/100BASE-T 4 PC/LAN 10/100BASE-T
Data protocol	TCP/IP
Dimensions	1.6" inch (H) x 5.5" inch (W) x 6.5" (L)
Input power	12 VDC

Telephony

Phone lines	Two RJ-11 ports for one or two analog telephones
Fax support	T.38 fax and g.711 fax send-and-receive Adaptive jitter buffer Optional PSTN failover
Services	Call waiting, caller ID, call blocking, 3-way conference calling, call forwarding, etc.
Codecs supported	g.711 (A-law and X-law), g.726, g.726 (reverse nibble), g.729ab, g.729e, g.723.1, g.728
Maximum line length (one-way)	1000 ft. (maximum)

Wireless (VT2500)

CPE wireless interface	802.11b/g; WiFi certified
Quality of service	802.11e WMM/WME for wireless QOS

Routing

CPE network interface	Ethernet 10/100Base-T NAPT, DMZ, port forwarding, VPN pass-through
Security	Firewall with stateful packet inspection, Dynamic port triggers, parental controls
Session initiation protocol	SIP RFC 2543/3261 compatibility; extensive support for SIP methods and extensions STUN, TURN, and outbound proxy support for NAT traversal
IP addressing	DHCP, static IP, or PPPoE

Electrical

Input voltage range	100 – 240 VAC, 50 – 60 Hz
Power consumption	9 watts (nominal)

Environmental

Operating temperature	32° to 113° F (0° to 40° C)
Storage temperature	–40° to 149° F (–40° to 65° C)
Operating humidity	5% to 95% R.H. (non-condensing) 32° to 95° F (0° to 35° C)



Storage humidity 95% R.H.

Antennas

LED Indicators

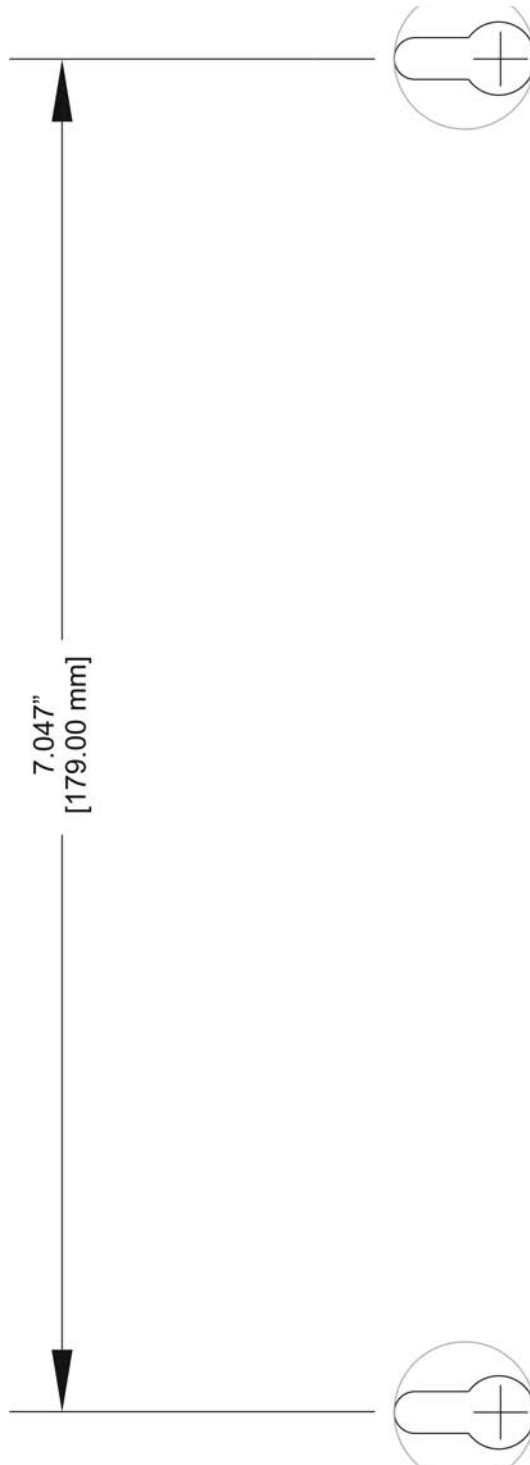
Physical Dimensions

width

height

Wall Mounting Template

Print out the template below to perform the wall mounting procedure in section 2.




Glossary

This glossary defines terms and lists acronyms used with the [VT2400/VT2500 Voice Gateway](#).


To return to your previous page, click the Acrobat Go to Previous View  button.

A


access point	A device that provides WLAN connectivity to wireless clients (stations). The VT2500 acts as a wireless access point.
adapter	A device or card that connects a computer, printer, or other peripheral device to the network or to some other device. A <i>wireless adapter</i> connects a computer to the WLAN.
address translation	See <i>NAT</i> .
ALG	Application level gateway triggers are required by some file transfer (for example, FTP), game, and video conferencing applications to open one or more ports to enable the application to operate properly.
American Wire Gauge (AWG)	A standard system used to designate the size of electrical conductors; gauge numbers are inverse to size.
ANSI	The American National Standards Institute is a non-profit, independent organization supported by trade organizations, industry, and professional societies for standards development in the United States. This organization defined ASCII and represents the United States to the International Organization for Standardization.
ANX	Automotive Network Exchange
ARP	Address Resolution Protocol broadcasts a datagram to obtain a response containing a MAC address corresponding to the host IP address. When it is first connected to the network, a client sends an ARP message. The VT2500 responds with a message containing its MAC address. Subsequently, data sent by the computer uses the VT2500 MAC address as its destination.
ASCII	The American Standard Code for Information Interchange refers to alphanumeric data for processing and communication compatibility among various devices; normally used for asynchronous transmission.
asynchronous timing	The VT2500 uses synchronous timing for upstream data transmissions. The CMTS broadcasts messages that bandwidth is available. The VT2500 reserves data bytes requiring x-number of mini-slots. The CMTS replies that it can receive data at a specified time (synchronized). At the specified time, the VT2500 transmits the x-number of data bytes.
attenuation	The difference between transmitted and received power resulting from loss through equipment, transmission lines, or other devices; usually expressed in decibels.
authentication	A process where the CMTS verifies that access is authorized, using a password, trusted IP address, or serial number.
authorization	Part of the process between a CMTS and the cable modem or gateway to enable Baseline Privacy.
auto-MDIX	Automatic medium-dependent interface crossover detects and corrects cabling errors by automatically reversing the send and receive pins on any port. It enables the use of straight-through wiring between the VT2500 Ethernet port and any computer, printer, or hub.

B To return to your previous page, click the Acrobat Go to Previous View  button.

bandwidth	The transmission capacity of a medium in terms of a range of frequencies. Greater bandwidth indicates the ability to transmit more data over a given period of time.
Baseline Privacy	An optional feature that encrypts data between the CMTS and the cable modem or gateway. Protection of service is provided by ensuring that a cable modem or gateway, uniquely identified by its MAC address, can only obtain keys for services it is authorized to access.
baud	The analog signaling rate. For complex modulation modes, the digital bit rate is encoded in multiple bits per baud; for example, 64 QAM encodes 6 bits per baud and 16 QAM encodes 4 bits per baud.
BCP	Binary Communication Protocol
BER	The bit error rate is the ratio of the number of erroneous bits or characters received from some fixed number of bits transmitted.
binary	A numbering system that uses two digits, 0 and 1.
bit rate	The number of bits (digital 0s and 1s) transmitted per second in a communications channel. It is usually measured in bits per second bps.
BPKM	Baseline Protocol Key Management encrypts data flows between a cable modem or gateway and the CMTS. The encryption occurs after the cable modem or gateway registers to ensure data privacy across the RF network.
bps	bits per second
bridge	An OSI layer 2 networking device that connects two LANs using similar protocols. It filters frames based on the MAC address to reduce the amount of traffic. A bridge can be placed between two groups of hosts that communicate a lot together, but not so much with the hosts in the other group. The bridge examines the destination of each packet to determine whether to transmit it to the other side. See also <i>switch</i> .
broadband	High bandwidth network technology that multiplexes multiple, independent carriers to carry voice, video, data, and other interactive services over a single cable. A communications medium that can transmit a relatively large amount of data in a given time period. A frequently used synonym for cable TV that can describe any technology capable of delivering multiple channels and services.
broadband Internet provider	A company that provides high-speed cable data or DSL service.
BTI	Broadband telephony interface. See MTA and S-MTA .
broadcast	Simultaneous transmission to multiple network devices; a protocol mechanism supporting group and universal addressing. See also <i>multicast</i> and <i>unicast</i> .


C To return to your previous page, click the Acrobat Go to Previous View  button.

CableHome	A project of CableLabs and technology suppliers to develop interface specifications for extending high-quality cable-based services to home network devices. It addresses issues such as device interoperability, QoS, and network management. CableHome will enable cable service providers to offer more services over HFC. It will improve consumer convenience by providing cable-delivered services throughout the home.
CableLabs	A research consortium that defines the interface requirements for cable modems and acknowledges that tested equipment complies with DOCSIS.
cable modem	A device installed at a subscriber location to provide data communications over an HFC network. Unless otherwise specified, all references to “cable modem” in this documentation refers to DOCSIS or Euro-DOCSIS cable modems <i>only</i> .
cable modem configuration file	File containing operational parameters that a cable modem or gateway downloads from the cable provider’s TFTP server during registration.
circuit-switched	Network-connection scheme used in the traditional PSTN telephone network where each connection requires a dedicated path for its duration. An alternative is packet-switched.
CLASS	Customer Local Area Signaling Service. One of an identified group of network-provided enhanced services. A CLASS group for a given network usually includes several enhanced service offerings, such as incoming-call identification, call trace, call blocking, automatic return of the most recent incoming call, call redial, and selective forwarding and programming to permit distinctive ringing for incoming calls.
Class C network	An IP network containing up to 253 hosts. Class C IP addresses are in the form “network.network.network.host.”
client	In a client/server architecture, a client is a computer that requests files or services such as file transfer, remote login, or printing from the server. Also called a CPE. On a WLAN, a client is any host that can communicate with the access point. A wireless client is also called a “station.”
CMTS	A cable modem termination system is a device in the cable system headend that interfaces the HFC network to local or remote IP networks to connecting IP hosts, cable modems or gateways, and subscribers. It manages all cable modem bandwidth. It is sometimes called an edge router.
CNR	carrier to noise ratio
coaxial cable (coax)	A type of cable consisting of a center wire surrounded by insulation and a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference. Coaxial cable has high bandwidth and can support transmission over long distances.
CODEC	COmpression/DECompression. A software-only or a hardware-assisted scheme that is used to process digital video or audio files. The amount of data required to represent moving pictures with sound is reduced by a CODEC, which normally discards redundant data on compression.
CoS	Class of service traffic management or scheduling functions are performed when transferring data upstream or downstream on HFC.
CPE	Customer premise equipment, typically computers, printers, etc., are connected to the cable modem or gateway at the subscriber location. CPE can be provided by the subscriber or the cable provider. Also called a client.
crosstalk	Undesired signal interfering with the desired signal.
CSMA/CD	carrier sense multiple access with collision detection

D To return to your previous page, click the Acrobat Go to Previous View  button.

datagram	In RFC 1594, a datagram is defined as “a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.” For the most part, it has been replaced by the term packet.
default route	The route by which packets are forwarded when other routes in the routing table do not apply.
dB	decibel
dBc	Signal level expressed in dB relative to the unmodulated carrier level desired.
DBm	A unit of measurement referenced to one milliwatt across specified impedance. 0dBm = 1 milliwatt across 75 ohms.
dBmV	Signal level expressed in dB as the ratio of the signal power in a 75-ohm system to a reference power when 1 mV is across 75 ohms.
demodulation	An operation to restore a previously modulated wave and separate the multiple signals that were combined and modulated on a subcarrier.
DHCP	<p>A Dynamic Host Configuration Protocol server dynamically assigns IP addresses to client hosts on an IP network. DHCP eliminates the need to manually assign static IP addresses by “leasing” an IP address and subnet mask to each client. It enables the automatic reuse of unused IP addresses.</p> <p><i>The VT2500 is simultaneously a DHCP client and a DHCP server.</i></p> <ul style="list-style-type: none">• A DHCP server at the cable system headend assigns a public IP address to the VT2500 and optionally to clients on the VT2500 LAN.• The VT2500 contains a built-in DHCP server that assigns private IP addresses to clients.
distortion	An undesired change in signal waveform within a transmission medium. A nonlinear reproduction of the input waveform.
DMZ	A “de-militarized zone” is one or more hosts logically located between a private LAN and the Internet. A DMZ prevents direct access by outside users to private data. (The term comes from the geographic buffers located between some conflicting countries, such as North and South Korea.) In a typical small DMZ configuration, the DMZ host receives requests from private LAN users to access external web sites and initiates sessions for these requests. The DMZ host cannot initiate a session back to the private LAN. Internet users outside the private LAN can access only the DMZ host. You can use a DMZ to set up a web server or for gaming without exposing confidential data.
DNS	The Domain Name System is the Internet system for converting domain names to IP addresses. A DNS server contains a table matching domain names such as Internetname.com to IP addresses such as 192.169.9.1. When you access the world-wide web, a DNS server translates the URL displayed on the browser to the destination website IP address. The DNS lookup table is a distributed Internet database; no one DNS server lists all domain name to IP address matches.
DOCSIS	The CableLabs Data-Over-Cable Service Interface Specification defines interface standards for cable modems, gateways, and supporting equipment to deliver data between an HFC network and computer systems or television sets. To emphasize its use as a cable modem standard, DOCSIS is now called CableLabs Certified Cable Modems. Euro-DOCSIS is DOCSIS adapted for use in Europe.
domain name	A unique name, such as motorola.com, that maps to an IP address. Domain names are typically much easier to remember than are IP addresses.
dotted-decimal format	<p>Method of representing an IP address or subnet mask using four decimal numbers called octets. Each octet represents eight bits.</p> <p>In a class C IP address, the octets are “network.network.network.host.” The first three octets together represent the network address and the final octet is the host address. In the VT2500 LAN default configuration, 192.168.100 represents the network address. In the final octet, the host address can be from 2 to 254.</p>


download	To copy a file from one computer to another. You can use the Internet to download files from a server to a computer. A DOCSIS or Euro-DOCSIS cable modem or gateway downloads its configuration file from a TFTP server during start-up.
downstream	In a cable data network, the direction of data received by the computer from the Internet.
driver	Software that enables a computer to interact with a network or other device. For example, there are drivers for printers, monitors, graphics adapters, modems, Ethernet, USB, HPNA, and many others.
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum is an IEEE 802.11b RF modulation protocol.
dynamic IP address	An IP address that is temporarily leased to a host by a DHCP server. The opposite of <i>static IP address</i> .

E To return to your previous page, click the Acrobat Go to Previous View  button.


encapsulate	To include data into some other data unit to hide the format of the included data.
encode	To alter an electronic signal so that only an authorized user can unscramble it to view the information.
encrypt	To encode data.
endpoint	A VPN endpoint terminates the VPN at the router so that computers on the VT2500 LAN do not need VPN client software to tunnel through the Internet to the VPN server.
ESSID	The Extended Service Set Identifier or network name is a unique identifier that wireless clients use to associate with an access point to distinguish between multiple WLANs in the same area. All clients on a WLAN must have the same ESSID as the access point. On the VT2500, you can set the ESSID on the Wireless > NETWORK page.
Ethernet	The most widely used LAN type, also known as IEEE 802.3. The most common Ethernet networks are 10Base-T, which provide transmission speeds up to 10 Mbps, usually over unshielded, twisted-pair wire terminated with RJ-45 connectors. Fast Ethernet (100Base-T) provides speeds up to 100 Mbps. "Base" means "baseband technology" and "T" means "twisted pair cable." Each Ethernet port has a physical address called the MAC address.
Euro-DOCSIS	A tComLabs standard that is DOCSIS adapted for use in Europe
event	A message generated by a device to inform an operator or the network management system that something has occurred.
expansion slot	A connection point in a computer where a circuit board can be inserted to add new capabilities.
EAP	Extensible Authentication Protocol

F To return to your previous page, click the Acrobat Go to Previous View  button.


FCS	frame check sequence
F-type connector	A type of connector used to connect coaxial cable to equipment such as the VT2500.
firewall	A security software system on the VT2500 that enforces an access control policy between the Internet and the VT2500 LAN.
flash	To press the flash button on the telephone, which allows you to retrieve or go between two calls.
flow	A data path moving in one direction.
FEC	Forward error correction is a technique to correct transmission errors without requiring the transmitter to resend any data.
FDMA	Frequency Division Multiple Access is a method to allow multiple users to share a specific radio spectrum. Each active user is assigned an individual RF channel (or carrier) with the carrier frequency of each channel offset from its adjacent channels by an amount equal to the channel spacing, which allows the required bandwidth per channel.
FQDN (Fully Qualified Domain Name)	A fully qualified domain name consists of a host and domain name, including top-level domain. For example, www.motorola.com is a fully qualified domain name. www is the host, motorola is the second-level domain, and .com is the top level domain.
frame	A unit of data transmitted between network nodes that contains addressing and protocol control data. Some control frames contain no data.
frequency	Number of times an electromagnetic signal repeats an identical cycle in a unit of time, usually one second, measured in Hz, kHz, MHz, or GHz.
FTP	File Transfer Protocol is a standard Internet protocol for exchanging files between computers. FTP is commonly used to download programs and other files to a computer from web pages on Internet servers.
full-duplex	The ability to simultaneously transmit and receive data. See also <i>half-duplex</i> .

G To return to your previous page, click the Acrobat Go to Previous View  button.

gain	The extent to which a signal is boosted. A high gain antenna increases the wireless signal level to increase the distance the signal can travel and remain usable.
gateway	A device that enables communication between networks using different protocols. See also <i>router</i> . The VT2500 enables up to 253 computers supporting IEEE 802.11b, Ethernet, or USB to share a single broadband Internet connection.
gateway IP address	The address of the default gateway router on the Internet. Also known as the “giaddr.”
GHz	Gigahertz — one billion cycles per second.
GUI	graphical user interface

H To return to your previous page, click the Acrobat Go to Previous View  button.

H.323	A suite of protocols created by the ITU for interactive video-conferencing, data sharing, and audio applications such as VoIP.
half-duplex	Network where only one device at a time can transmit data. See also <i>full-duplex</i> .
headend	A location that receives TV programming, radio programming, data, and telephone calls that it modulates onto the HFC network. It also sends return data and telephone transmissions. Headend equipment includes transmitters, preamplifiers, frequency terminals, demodulators, modulators, and other devices that amplify, filter, and convert incoming broadcast TV signals to wireless and cable channels.
header	The data at the beginning of a packet that identifies what is in the packet.
hexadecimal	A base-sixteen numbering system that uses sixteen sequential numbers (0 to 9 and the letters A to F) as base units before adding a new position. On computers, hexadecimal is a convenient way to express binary numbers.
HFC	A hybrid fiber/coaxial cable network uses fiber-optic cable as the trunk and coaxial cable to the subscriber premises.
hop	The interval between two routers on an IP network. The number of hops a packet traverses toward its destination (called the hop count) is saved in the packet header. For example, a hop count of six means the packet has traversed six routers. The packet hop count increases as the time-to-live (TTL) value decreases.
host	In IP, a host is any computer supporting end-user applications or services with full two-way network access. Each host has a unique host number that combined with the network number forms its IP address. Host also can mean: <ul style="list-style-type: none">• A computer running a web server that serves pages for one or more web sites belonging to organization(s) or individuals• A company that provides this service• In IBM environments, a mainframe computer
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol. The client-server TCP/IP used for exchanging HTML documents on the World Wide Web.
hub	On a LAN, a hub is a device that connects multiple hosts to the LAN. A hub performs no data filtering. See also <i>bridge</i> and <i>router</i> . An IP hub is typically a unit on a rack or desktop. On an HFC network, a hub is a scaled-down headend that performs some or all headend functions for part of the system.
Hz	Hertz — one cycle per second. The unit to measure the frequency that an alternating electromagnetic signal cycles through its highest and lowest states. Used to define the bands of the electromagnetic spectrum used in voice and data communications, or to define the bandwidth of a transmission medium.

I To return to your previous page, click the Acrobat Go to Previous View  button.

IANA	The Internet Numbering Address Authority (IANA) is an organization under the Internet Architecture Board (IAB) of the Internet Society that oversees IP address allocation. It is under a contract from the U.S. government.
ICMP	Internet Control Message Protocol is a protocol used for error, problem, and informational messages sent between IP hosts and gateways. ICMP messages are processed by the IP software and are not usually apparent to the end-user.


ICSA	The International Computer Security Association is the security industry's main source of research, intelligence, and product certification.
IEEE	The Institute of Electrical and Electronics Engineers, Inc. (http://www.ieee.org) is an organization that produces standards, technical papers, and symposiums for the electrical and electronic industries and is accredited by ANSI.
IEEE 802.11b IEEE 802.11g	IEEE wireless network standards.
IEEE 802.3	See <i>Ethernet</i> .
IETF	The Internet Engineering Task Force (http://www.ietf.org) is an open international community of network designers, operators, vendors, and researchers to develop and maintain Internet architecture. Technical working groups issue working documents called Internet-Drafts. The IETF publishes review versions of the drafts called requests for comments (RFCs).
IGMP	Internet Group Membership Protocol — the Internet multicasting standard. IGMP establishes and maintains a database of group multicast addresses and interfaces to which a multicast router forwards multicast packets. IGMP runs between multicast hosts and their immediately-neighboring multicast routers.
IGMP spoofing	A process where a router acts as an IGMP querier for multicast hosts and an IGMP host to a multicast router.
impedance	The total opposition to AC electron current flow within a device. Impedance is typically 75 ohms for coax cable and other CATV components.
impulse noise	Noise of very short duration, typically of the order of 10 microseconds. It is caused by electrical transients such as voltage spikes, electric motors turning on, and lightning or switching equipment that bleed over to the cable.
ingress noise	Noise typically caused by discrete frequencies picked up by the cable plant from radio broadcasts or an improperly grounded or shielded home appliance such as a hair dryer. Ingress is the major source of cable system noise.
Internet	A worldwide collection of interconnected networks using TCP/IP.
Internetwork	A collection of interconnected networks allowing communication between all devices connected to any network in the collection.
IP	Internet Protocol is a set of standards that enable different types of computers to communicate with one another and exchange data through the Internet. IP provides the appearance of a single, seamless communication system and makes the Internet a virtual network.

To return to your previous page, click the Acrobat Go to Previous View  button.


IP address	<p>A unique 32-bit value that identifies each host on a TCP/IP network. TCP/IP networks route messages based on the destination IP address. An IP address has two parts:</p> <ul style="list-style-type: none">• The network address is assigned by IANA.• The VT2500 network administrator assigns a host address to each host connected to the VT2500, automatically using its DHCP server as a static IP address. <p>For a Class C network, the first 24 bits are the network address and the final 8 bits are the host address; in dotted-decimal format, it appears "network.network.network.host."</p> <p>If you enable the VT2500 DHCP client on the WAN page, the cable provider automatically assigns the network address, subnet mask, domain name, and DNS server to provide a continuous Internet connection.</p>
IPSec	The Internet Protocol Security protocols are IETF authentication and encryption standards for secure packet exchange over the Internet. IPSec works at OSI layer 3 and secures everything on the network.




IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	The International Organization for Standardization (http://www.iso.ch) is a worldwide federation of national standards bodies from approximately 140 countries. ISO is a non-governmental organization established in 1947 to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity.
ISP	Internet Service Provider
ITSP	Internet Telephony Service Provider. A company that provides VoIP telephone service. It may be the same as or different from the end-user broadband Internet provider. Also referred to as a "VoIP provider" or "voice provider."
ITU	International Telecommunications Union

KTo return to your previous page, click the Acrobat Go to Previous View  button.


kHz kilohertz — one thousand cycles per second

L To return to your previous page, click the Acrobat Go to Previous View  button.

L2F	Layer 2 Forwarding is an OSI layer 2 protocol that establishes a secure tunnel across the Internet to create a virtual PPP connection between the user and the enterprise network. L2F is the most established and stable layer 2 tunneling protocol.
L2TP	Layer 2 Tunnel Protocol is a PPP extension that enables ISPs to operate VPNs. L2TP merges the best features of the PPTP and L2F. L2TP is the emerging IETF standard.
LAC	An L2TP access concentrator is a device to which the client directly connects through which PPP frames are tunneled to the LNS. The LAC need only implement the media over which L2TP operates to transmit traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F NAS.
LAN	A local area network provides a full-time, high-bandwidth connection over a limited area, such as a building or campus. Ethernet is the most widely used LAN standard.
layer	In networks, layers are software protocol levels. Each layer performs functions for the layers above it. OSI is a reference model having seven functional layers.
LCP	Link Control Protocol establishes, configures, and tests data link connections used by PPP.
latency	The time required for a signal to pass through a device. It is often expressed in a quantity of symbols.
LED	light-emitting diode
LNS	An L2TP network server is a termination point for L2TP tunnels where PPP frames are processed and passed to higher layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single media over which L2TP tunnels arrive. The LNS can have a single LAN or WAN interface but can terminate calls arriving at any of the LACs full range of PPP interfaces (asynchronous, synchronous, ISDN, V.120, etc.). The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.
loopback	A test that loops the transmit signal to the receive signal. Usually the loopback test is initiated on a network device. The test is used to verify a path or to measure the quality of a signal on that path.


M To return to your previous page, click the Acrobat Go to Previous View  button.

MAC address	The Media Access Control address is a unique, 48-bit value permanently saved in ROM at the factory to identify each Ethernet network device. It is expressed as a sequence of 12 hexadecimal digits printed on the bottom of the VT2400 or VT2500. You need to provide the HFC MAC address to the cable provider. Also called an Ethernet address, physical address, hardware address, or NIC address.
MB	One megabyte; equals 1,024 x 1,024 bytes, 1,024 kilobytes, or about 8 million bits.
Mbps	Million bits per second (megabits per second). A rate of data transfer.
media	The various physical environments through which signals pass; for example, coaxial, unshielded twisted-pair (UTP), or fiber-optic cable.
MIB	A management information base is a unique hierarchical structure of software objects used by the SNMP manager and agent to configure, monitor, or test a device.
MHz	Megahertz — one million cycles per second. A measure of radio frequency.
MPDU	MAC protocol data unit (PDU)
MSDU	MAC service data unit
MSO	Multiple Systems Operator. A company that owns and operates more than one cable system. Also called a group operator.
MTA	Multimedia Terminal Adapter. See S-MTA .
MTU	The Maximum Transmission Unit is the largest amount of data that can be transmitted in one discrete message on a given physical network. The MTU places an upper bound on the size of a message that can be transferred by the network in a single frame. Messages exceeding the MTU must be fragmented before transmission, and reassembled at the destination.
multicast	A data transmission sent from one sender to multiple receivers. See also <i>broadcast</i> and <i>unicast</i> .
mW	milliwatts


N To return to your previous page, click the Acrobat Go to Previous View  button.

NAS	network access server
NAT	Network Address Translation is an Internet standard for a LAN to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. NAT provides some security because the IP addresses of VT2500 LAN computers are invisible on the Internet. If NAT is enabled on the Gateway page, there is a one-to-one mapping between each public IP address and client IP address.
NAPT	Network Address Port Translation is the most common form of address translation between public and private IP addresses. NAPT is a mapping of one public IP address to many private IP addresses. If NAPT is enabled on the Gateway page, one public IP address is mapped to an individual private IP address for up to 245 LAN clients.
NEC	National Electrical Code (in the United States) are the regulations for construction and installation of electrical wiring and apparatus, suitable for mandatory application by a wide range of state and local authorities.
network	Two or more computers connected to communicate with each other. Networks have traditionally been connected using some kind of wiring.
network driver	Software packaged with a NIC that enables the computer to communicate with the NIC.

network layer	Layer 3 in the OSI architecture that provides services to establish a path between open systems. The network layer knows the address of the neighboring nodes, packages output with the correct network address data, selects routes, and recognizes and forwards to the transport layer incoming messages for local host domains.
NIC	A network interface card converts computer data to serial data in a packet format that it sends over the LAN. A NIC is installed in an expansion slot or can be built-in. Every Ethernet NIC has a MAC address permanently saved in its ROM.
node	On a LAN, a generic term for any network device. On an HFC network, the interface between the fiber-optic trunk and coaxial cable feeders to subscriber locations. A node is typically located in the subscriber neighborhood.
noise	Random spurts of electrical energy or interface. May produce a salt-and-pepper pattern on a television picture.


O To return to your previous page, click the Acrobat Go to Previous View  button.

ohm	A unit of electrical resistance.
OOB DTMF	Out-of-band dual tone multi-frequency signals are generated when you press the keys of an ordinary telephone. In the United States, it is referred to as a "touch-tone" phone (formerly a registered trademark of AT&T).
OSI	The Open Systems Interconnection reference model is an illustrative model describing how data moves from an application on the source host through a network to an application on the destination host. It is a conceptual framework developed by ISO that is now the primary model for intercomputer communications. OSI is a model <i>only</i> ; it does not define a specific networking interface.


P To return to your previous page, click the Acrobat Go to Previous View  button.

packet	The unit of data that is routed between the sender and destination on the Internet or other packet-switched network. When data such as an e-mail message or other file is sent over the Internet, IP on the sender divides the data into uniquely-numbered packets. The packet header contains the source and destination IP addresses. The individual packets may travel different routes. When all packets arrive at the destination, IP at that end reassembles the packets. The header and the data can vary in length. Packet and datagram are similar in meaning.
packet-switched	A scheme to handle transmissions on a connectionless network such as the Internet. An alternative is circuit-switched.
PacketCable	A CableLabs-led project to define a common platform to deliver advanced real-time multimedia services over two-way HFC cable plant. Built on DOCSIS 1.1, PacketCable networks use IP technology as the basis for a highly-capable multimedia architecture.
pass-through	A pass-through client on the VT2500 LAN obtains its public IP address from the cable provider DHCP server.
PAT	Port Address Translation
PCI	
PCMCIA	The Personal Computer Memory Card International Association sets international standards for connecting peripherals to portable computers. Laptop computers typically have a PCMCIA slot that can hold one or two PC Cards to provide features such as Ethernet connectivity.
PDA	personal desktop assistant
PDU	A protocol data unit is a message containing operational instructions used for SNMP. The basic SNMP V2 PDU types are get-request, get-next-request, get-bulk-request, response, set-request, inform-request, and trap.
Peer-to-peer network	A network in which each computer is independent and can serve the others or act as a workstation. Peripherals connected to any computer networked in this fashion are available to any of the other peer computers connected.
periodic ranging	Ranging that is performed on an on-going basis after initial ranging has taken place.
physical layer	Layer 1 in the OSI architecture. It provides services to transmit bits or groups of bits over a transmission link between open systems. It entails the electrical, mechanical, and handshaking procedures.
piggybacking	A process that occurs when a cable modem simultaneously transmits data and requests additional bandwidth.
PING	A network utility that tests host reachability by sending a small packet to the host and waiting for a reply. If you PING a computer IP address and receive a reply, you know the computer is reachable over the network. It also stands for "Packet InterNet Groper."
PMD	The physical media-dependent sublayer of the physical layer which transmits bits or groups of bits over particular types of transmission links between open systems. It entails the electrical, mechanical, and handshaking procedures.
point-to-point	Physical connection made from one point to another.
POTS	The "plain old telephone service" offered through the PSTN; basic analog telephone service. POTS uses the lowest 4 kHz of bandwidth on twisted pair wiring.
port	On a computer or other electronic device, a port is a socket or plug used to physically connect it to the network or to other devices. in TCP/IP, a port is a number from 0 to 65536 used logically by a client program to specify a server program. Ports 0 to 1024 are reserved.

port mirroring	A feature that enables one port (source) on the VT2500 to be copied to another port (destination) to be studied. The destination mirrors the transmitted (from) or received (to) data on the source port to enable the person managing the network to monitor activity.
port triggering	A mechanism that allows incoming communication with specified applications. Primarily used for gaming applications.
PPP	Point-to-Point Protocol is used to transport other protocols, typically for simple links over serial lines. It is most commonly used to access the Internet with a dial-up modem.
PPPoE	Point-to-Point Protocol over Ethernet. A specification for connecting to the Internet with DSL modems.
PPTP	Point-to-Point Tunneling Protocol encapsulates other protocols. It is a new technology to create VPNs developed jointly by several vendors.
private IP address	An IP address assigned to a computer on the VT2500 LAN by the DHCP server on the VT2500 for a specified lease time. Private IP addresses are used by the VT2500 LAN only; they are invisible to devices on the Internet. See also <i>public IP address</i> .
protocol	A formal set of rules and conventions for exchanging data. Different computer types (for example PC, UNIX, or mainframe) can communicate if they support common protocols.
provisioning	The process of autodiscovery or manually configuring a cable modem on the CMTS.
PSTN	The public switched telephone network is the traditional circuit-switched, voice-oriented telephone network. See also <i>POTS</i> .
public IP address	The IP address assigned to the VT2500 by the cable provider. A public IP address is visible to devices on the Internet. See also <i>private IP address</i> .

Q To return to your previous page, click the Acrobat Go to Previous View  button.

QAM	Quadrature Amplitude Modulation uses amplitude and phase modulation to encode multiple bits of data in one signaling element. QAM achieves faster data transfer than amplitude or phase modulation alone, but the signal is more prone to errors caused by noise. QAM requires a transmission circuit with a higher CNR than alternate modulation formats such as QPSK. Two types of QAM are: <ul style="list-style-type: none">• 16 QAM encodes four bits per symbol as one of 16 possible amplitude and phase combinations.• 64 QAM encodes six bits per symbol as one of 64 possible amplitude and phase combinations.
QPSK	Quadrature Phase Shift Key (QPSK) modulation sends two bits of information per symbol period with one symbol 90 degrees out of phase with other symbols. The four constellation points represented by the coordinates (0,0 - 0,1 - 1,0 - 1,1) represent the four possible combinations.
QoS	Quality of service describes the priority, delay, throughput, and bandwidth of a connection.

R To return to your previous page, click the Acrobat Go to Previous View  button.


RADIUS	Remote Authentication Dial-In User Service server typically used in large corporate settings.
RAS	Remote Access Server
registration	How a cable modem makes itself known to the CMTS. The cable modem configuration file and authorization are verified and the CoS is negotiated.
return loss	A measurement of the quality of the match of the device to the cable system. Return loss is the ratio of the amount of power reflected by the device. A return loss of 20 dB or greater is preferred.
RF	Radio Frequency — signals used by the CMTS transmitter and receiver to send data over HFC. The carrier is modulated to encode the digital data stream for transmission across the cable network.
RFC	Request for Comments published on the IETF or other websites. Many RFCs become international standards.
RJ-11	The most common type of connector for household or office phones.
RJ-45	An 8-pin modular connector; the most common connector type for 10Base-T or 100Base-T Ethernet networks.
ROM	read-only memory
router	<p>On IP networks, a device connecting at least two networks, which may or may not be similar. A router is typically located at a <i>gateway</i> between networks. A router operates on OSI network layer 3. It filters packets based on the IP address, examining the source and destination IP addresses to determine the best route on which to forward them.</p> <p>A router is often included as part of a network switch. A router can also be implemented as software on a computer.</p>
routing table	A table listing available routes that is used by a router to determine the best route for a packet.
RTP	A protocol that enables real-time data, such as voice traffic, to be carried in packets over the Internet.
RTCP	A protocol for monitoring RTP performance.
RTS	request to send

S To return to your previous page, click the Acrobat Go to Previous View  button.


server	In a client/server architecture, a dedicated computer that supplies files or services such as file transfer, remote login, or printing to clients.
scope	The set of IP addresses that a DHCP server can lease to clients.
service provider	A company providing cable data services to subscribers.
SDP	A protocol that describes multimedia sessions for the purpose of session announcement, session invitation, and other forms of multimedia initiation.
SDU	service data unit
SID	A service ID is a unique 14-bit identifier the CMTS assigns to a cable modem or gateway that identifies the traffic type it carries (for example, data or voice). The SID provides the basis for the CMTS to allocate bandwidth to the cable modem and implement CoS.
SIP	Session Initiation Protocol. SIP is a text-based protocol, similar to HTTP and SMTP, for initiating interactive communication sessions between users. Such sessions include voice, video, chat, interactive games, and virtual reality.
SME	small and medium enterprise
S-MTA	Stand-Alone Multiservice Terminal Adapter. A device that converts analog voice signals to and from a standard telephone to digital data that can be transmitted through a broadband connection over the Internet. An SMTA is typically connected through Ethernet.
SMTP	Simple Mail Transfer Protocol is a standard Internet protocol for transferring e-mail.
SNMP	Simple Network Management Protocol is a standard to monitor and manage networks and network devices. Data is exchanged using PDU messages.
SOHO	small office home office
spectrum	A specified range of frequencies used for transmission of electromagnetic signals.
spectrum allocation	An allocation of portions of the available electromagnetic spectrum for specific services, such as AM, FM, or personal communications.
splitter	A device that divides the signal from an input cable between two or more cables.
stateful inspection	<p>A type of firewall that tracks each connection traversing all firewall interfaces to ensure validity. In addition to examining the source and destination in the packet header based on static rules, a stateful inspection firewall:</p> <ul style="list-style-type: none">• Examines packet headers on context established by previous packets that traversed the firewall• Monitors the connection state and saves it in a table• Closes ports until a connection to a specific port is requested• May examine the packet contents up through the application layer to determine more than just the source and destination <p>A stateful-inspection firewall is more advanced than a static filter firewall.</p>
static filter	A type of firewall that examines the source and destination in the packet header based on administrator-defined rules <i>only</i> .
static IP address	An IP address that is permanently assigned to a host. Normally, a static IP address must be assigned manually. The opposite of dynamic IP address.
static route	A manually-defined route.
station	IEEE 802.11b term for wireless client.
STUN	Simple Traversal of UDP through NAT - an intrusion detection system which inspects all inbound and outbound network activity.



subscriber	A home or office user who accesses television, data, or other services from a cable provider.
subnet mask	A bit mask that is logically ANDed with the destination IP address of a packet to determine the network address. A router routes packets using the network address.
subnetwork	A part of a network; commonly abbreviated "subnet." When subnetting is used, the host portion of the IP address is divided into a subnet and host number. Hosts and routers use the subnet mask to identify the bits used for the network and subnet number.
switch	On an Ethernet network, a switch filters frames based on the MAC address, in a manner similar to a bridge. A switch is more advanced because it can connect more than two segments.
symbol rate	Also known as baud rate, is a measure of the number of times per second a signal in a communications channel varies, or makes a transition between states (states being frequencies, voltage levels or phase angles). Usually measured in symbols per second (sps).
SYSLOG	A de-facto UNIX standard for logging system events.

T To return to your previous page, click the Acrobat Go to Previous View  button.

TBCP	Tagged Binary Communication Protocol
TCP	Transmission Control Protocol on OSI transport layer four, provides reliable transport over the network for data transmitted using IP (network layer three). It is an end-to-end protocol defining rules and procedures for data exchange between hosts on top of connectionless IP. TCP uses a timer to track outstanding packets, checks error in incoming packets, and retransmits packets if requested.
TCP/IP	The Transmission Control Protocol/Internet Protocol suite provides standards and rules for data communication between networks on the Internet. It is the worldwide internetworking standard and the basic communications protocol of the Internet.
Telnet	The Internet standard protocol for remote terminal connection service. Telnet allows a user at one site to interact with a system at another site as if the user's terminal were directly connected to the host computer.
TFTP	Trivial File Transfer Protocol is a very simple protocol used to transfer files.
THDD	Telephony Hardware Device Driver.
TKIP	Temporal Key Integrity Protocol
transparent bridging	A method to enable all hosts on the wired Ethernet LAN, WLAN, and USB connection to communicate as if they were all connected to the same physical network.
transport layer	Layer of the OSI concerned with protocols for error recognition and recovery. This layer also regulates information flow.
trunk	Electronic path over which data is transmitted.
TTL	The time to live is the number of routers (or hops) a packet can traverse before being discarded. When a router processes a packet, it decreases the TTL by 1. When the TTL reaches zero, the packet is discarded.
tunnel	To place packets inside other packets to send over a network. The protocol of the enclosing packet is understood by each endpoint, or tunnel interface, where the packet enters and exits the network. VPNs rely on tunneling to create a secure network. Tunneling requires the following protocol types: <ul style="list-style-type: none">• A carrier protocol, such as TCP, used by the network over which the data travels• An encapsulating protocol, such as IPSec, L2F, L2TP, or PPTP, that is wrapped around the original data• A passenger protocol, such as IP, for the original data
two-way	A cable system that can transmit signals in both directions to and from the headend and the subscriber.

U-Z To return to your previous page, click the Acrobat Go to Previous View  button.

UDP	User Datagram Protocol
unicast	A point-to-point data transmission sent from one sender to one receiver. This the normal way you access websites. See also <i>broadcast</i> and <i>multicast</i> .
upstream	In a cable data network, upstream describes the direction of data sent from the subscriber computer through the cable modem to the CMTS and the Internet.
USB	Universal Serial Bus is a computer interface for add-on devices such as printers, scanners, mice, modems, or keyboards. USB supports data transfer rates of 12 Mbps and plug-and-play installation. You can connect up to 127 devices to a single USB port.
UTP	unshielded twisted pair (wire)
VCM	In a telecommunications connection, the segment of the bandwidth allocated to transmitting voice messages.
VLAN	A virtual local area network is group of devices on different LAN segments that are logically configured to communicate as if they are connected to the same wire.
VoIP	Voice over Internet Protocol is a method to exchange voice, fax, and other information over the Internet. Voice and fax have traditionally been carried over traditional telephone lines of the PSTN using a dedicated circuit for each line. VoIP enables calls to travel as discrete data packets on shared lines. VoIP is an important part of the convergence of computers, telephones, and television into a single integrated information network.
VoIP Provider	A company that provides voice-over internet protocol telephone service.
VPN	A virtual private network is a private network that uses “virtual” connections (tunnels) routed over a public network (usually the Internet) to provide a secure and fast connection; usually to users working remotely at home or in small branch offices. A VPN connection provides security and performance similar to a dedicated link (for example, a leased line), but at much lower cost.
WAN	A wide-area network provides a connection over a large geographic area, such as a country or the whole world. The bandwidth depends on need and cost, but is usually much lower than for a LAN.
WAP	Wireless access point or Wireless Access Protocol. See also <i>access point</i> .
WECA	The Wireless Ethernet Compatibility Alliance is a trade organization that works to ensure that all wireless devices — computer cards, laptops, air routers, PDAs, etc — can communicate with each other.
WEP	Wired Equivalent Privacy encryption protects the privacy of data transmitted over a WLAN. WEP uses keys to encrypt and decrypt transmitted data. The access point must authenticate a client before it can transfer data to another client. WEP is part of IEEE 802.11b. <i>Because WEP can be difficult to use and does not provide very strong encryption, we recommend using WPA if possible.</i>
WiFi	Wireless fidelity (pronounced y-phi) brand name applied to products supporting IEEE 802.11b.
Wireless Access Point (WAP)	A device that provides network connectivity to one or more client computers using radio signals over a wireless connection.
Wireless Cable Modem Gateway	A single device, such as the SBG9000, that combines a cable modem, router, Ethernet switch, wireless access point, and DHCP server for SOHO or SME use.
Wireless Voice Gateway	A single device, such as the VT2500, that rovides two telephone lines for voice-over-data, a built-in wireless access point and router, and connection to a modem.
WLAN	wireless LAN



world wide web An interface to the Internet that you use to navigate and hyperlink to information.

WPA Wi-Fi Protected Access (WPA) encryption, as described on the Wi-Fi Alliance [Wi-Fi Protected Access](http://www.wifialliance.org/OpenSection/protected_access.asp) web page http://www.wifialliance.org/OpenSection/protected_access.asp). It is a far more robust form of encryption than WEP. *We recommend using WPA if all of your client hardware supports WPA.*

❖ Software License

SOFTWARE LICENSE

Motorola, Inc., [Connected Home Solutions](#) ("Motorola") 101 Tournament Drive, Horsham, PA 19044

IMPORTANT: PLEASE READ THIS SOFTWARE LICENSE ("LICENSE") CAREFULLY BEFORE YOU INSTALL, DOWNLOAD OR USE ANY APPLICATION SOFTWARE, USB DRIVER SOFTWARE, FIRMWARE AND RELATED DOCUMENTATION ("SOFTWARE") PROVIDED WITH MOTOROLA'S VOICE GATEWAY PRODUCT (THE "VOICE GATEWAY PRODUCT"). BY USING THE VOICE GATEWAY PRODUCT AND/OR INSTALLING, DOWNLOADING OR USING ANY OF THE SOFTWARE, YOU INDICATE YOUR ACCEPTANCE OF EACH OF THE TERMS OF THIS LICENSE. UPON ACCEPTANCE, THIS LICENSE WILL BE A LEGALLY BINDING AGREEMENT BETWEEN YOU AND MOTOROLA. THE TERMS OF THIS LICENSE APPLY TO YOU AND TO ANY SUBSEQUENT USER OF THIS SOFTWARE.

IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE (I) DO NOT INSTALL OR USE THE SOFTWARE AND (II) RETURN THE VOICE GATEWAY PRODUCT AND THE SOFTWARE (COLLECTIVELY, "PRODUCT"), INCLUDING ALL COMPONENTS, DOCUMENTATION AND ANY OTHER MATERIALS PROVIDED WITH THE PRODUCT, TO YOUR POINT OF PURCHASE OR SERVICE PROVIDER, AS THE CASE MAY BE, FOR A FULL REFUND.

The Software includes associated media, any printed materials, and any "online" or electronic documentation, as well as any updates, revisions, bug fixes, or drivers obtained by you from Motorola or your service provider. Software provided by 3rd parties may be subject to separate end-user license agreements from the manufacturers of such Software.

The Software is never sold. Motorola licenses the Software to the original customer and to any subsequent licensee for personal use only on the terms of this License. Motorola and its 3rd party licensors retain the ownership of the Software.

You may:

USE the Software only in connection with the operation of the Product.

TRANSFER the Software (including all component parts and printed materials) permanently to another person, but only if the person agrees to accept all of the terms of this License. If you transfer the Software, you must at the same time transfer the Product and all copies of the Software (if applicable) to the same person or destroy any copies not transferred.

TERMINATE this License by destroying the original and all copies of the Software (if applicable) in whatever form.

You may not:

(1) Loan, distribute, rent, lease, give, sublicense or otherwise transfer the Software, in whole or in part, to any other person, except as permitted under the TRANSFER paragraph above. (2) Copy or translate the User Guide included with the Software, other than for personal use. (3) Copy, alter, translate, decompile, disassemble or reverse engineer the Software, including but not limited to, modifying the Software to make it operate on non-compatible hardware. (4) Remove, alter or cause not to be displayed, any copyright notices or startup message contained in the Software programs or documentation. (5) Export the Software or the Product components in violation of any United States export laws.

The Product is not designed or intended for use in on-line control of aircraft, air traffic, aircraft navigation or aircraft communications; or in design, construction, operation or maintenance of any nuclear facility. MOTOROLA AND ITS 3rd PARTY LICENSORS DISCLAIM ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCH USES. YOU REPRESENT AND WARRANT THAT YOU SHALL NOT USE THE PRODUCT FOR SUCH PURPOSES.

Title to this Software, including the ownership of all copyrights, mask work rights, patents, trademarks and all other intellectual property rights subsisting in the foregoing, and all adaptations to and modifications of the foregoing shall at all times remain with Motorola and its 3rd party licensors. Motorola retains all rights not expressly licensed under this License. The Software, including any images, graphics, photographs, animation, video, audio, music and text incorporated therein is owned by Motorola or its 3rd party licensors and is protected by United States copyright laws and international treaty provisions. Except as otherwise expressly provided in this License, the copying, reproduction, distribution or preparation of derivative works of the Software, any portion of the Product or the documentation is strictly prohibited by such laws and treaty provisions. Nothing in this License constitutes a waiver of Motorola's rights under United States copyright law.



This License and your rights regarding any matter it addresses are governed by the laws of the Commonwealth of Pennsylvania, without reference to conflict of laws principles. THIS LICENSE SHALL TERMINATE AUTOMATICALLY if you fail to comply with the terms of this License.

Motorola is not responsible for any 3rd party software provided as a bundled application, or otherwise, with the Software.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Product and documentation is provided with RESTRICTED RIGHTS. The use, duplication or disclosure by the Government is subject to restrictions as set forth in subdivision (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at 52.227-7013. The contractor/manufacturer is Motorola, Inc., [Connected Home Solutions](#), 101 Tournament Drive, Horsham, PA 19044.

Visit our website at:
www.motorola.com



521569-001
7/05
MGBI