



WR100

802.11g Wireless Router

User Guide



Copyright © ViewSonic Corporation, 2004. All rights are reserved.

ViewSonic and the three birds logo are registered trademarks of ViewSonic Corporation.

UPnP™ is a trademark of UPnP™ Implementers Corporation (UIC).

The 'Wi-Fi CERTIFIED' logo is a certification mark of the Wi-Fi Alliance.

Broadcom and the pulse logo are trademarks of Broadcom Corporation and/or its affiliates in the United States and certain other countries.

Microsoft, Windows, the Microsoft Internet Explorer logo graphic, and the Windows logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Corporate names and trademarks are the property of their respective companies.

Disclaimer: ViewSonic Corporation shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from furnishing this material, or the performance or use of this product.

In the interest of continuing product improvement, ViewSonic Corporation reserves the right to change product specifications without notice. Information in this document may change without notice.

No part of this document may be copied, reproduced, or transmitted by any means, for any purpose without prior written permission from ViewSonic Corporation.

Product Registration

To meet your future needs and to receive additional product information as it becomes available, register your ViewSonic® product at: www.viewsonic.com.

For Your Records

Model Name:	WR100
Model Number:	VS10276
Document Number:	A-WR100-1_CD 07-21-04
Serial Number:	_____
Purchase Date:	_____

Table of Contents

Product Registration.....	i
For Your Records.....	i
Overview	1
Finally, networking made easy.....	1
Chapter 1: Getting Started	
Freedom of a wireless network.....	2
Package Contents	3
Safety Notice	4
Front of router.....	6
Chapter 2: Product Description	
Back of router	7
Chapter 3: Setting up the wireless router	
Configuring the wireless router using Web-based utility screens	14
Wireless.....	19
Security.....	21
System.....	24
DHCP Server.....	30
Status.....	33
Advanced Wireless	34
Access Filters	38
Virtual Server.....	44
Routing Table	47
Operating Mode	47

Dynamic Routing (RIP) 47

Static Routing, Destination IP Address, Subnet Mask, Gateway, and Interface 48

Appendix

Specifications..... 51

Wireless Security & Glossary 52

Troubleshooting..... 73

Compliances..... 77

Cleaning & Maintenance..... 80

Customer Support..... 81

Limited Warranty..... 82

Chapter 1: Getting Started

This chapter provides an Overview of the ViewSonic WR100 Wireless Router, Package Contents, and Safety Notice.

Overview

Congratulations on purchasing the ViewSonic Wireless Router!

Finally, networking made easy.

Networking your home or small business is easy with ViewSonic's WR100 Wireless Router. The WR100 functions as the CENTRAL GATEWAY IN YOUR HOME OR OFFICE NETWORK, allowing you to share your broadband, files and printers with any PC in your office or home. The WR100 boasts a stylish, compact design that offers high performance wireless 802.11g, 802.11b and wired Ethernet connectivity. HIGH-LEVEL SECURITY FEATURES include Virtual Private Network (VPN) support, parental controls, firewall, and strong wireless security. The WR100 Wireless Network Router is the cost-effective, and security-conscious networking solution for your home or office.

Freedom of a wireless network.

- **Create a wireless network for your home or office**
Create a local area network (LAN) with the WR100 Wireless Router and share a single high-speed broadband connection, files, printers and other peripherals among all your computers.
- **Robust security keeps your data secure**
Network Address Translation (NAT) and Stateful Packet Inspection (SPI) firewall ensures your networked data is safe from Internet intruders. Wireless security includes 64-bit/128-bit Wired Equivalency Privacy (WEP), 256-bit Wi-Fi Protected Access™ (WPA) and Medium Access Controller (MAC) address filtering.
- **Superior performance and speed Zero waiting time.**
Transfer data at up to 10 times the speed of standard 802.11b wireless networks. Share your files, videos, music and pictures almost instantly with the 125* high speed mode within your network.

* When operating at highest speeds, this WiFi device achieves an actual throughput of up to 34 Mbps, which is the equivalent throughput of a system following 802.11g protocol and operating at a signaling rate of 125 Mbps. This mode requires the same technology from the client devices.
- **Easy set up**
User-friendly set up wizard on the Network Companion CD makes installation a snap.

Using the router with a ViewSonic Wireless Network Adapters enables you to connect notebooks and/or desktop PCs to your high-speed network in your home or office. Enjoy the flexibility and freedom of a wireless network in your home or small business with a ViewSonic Wireless Router.

Package Contents

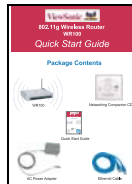
Check to make sure all of the items shown below are included in the package.



Wireless WR100 Router



Network Companion CD



Quick Start Guide



AC Power Adapter



Ethernet LAN Cable
(6 feet)

For information on optional accessories and products, go to www.viewsonic.com.

Safety Notice

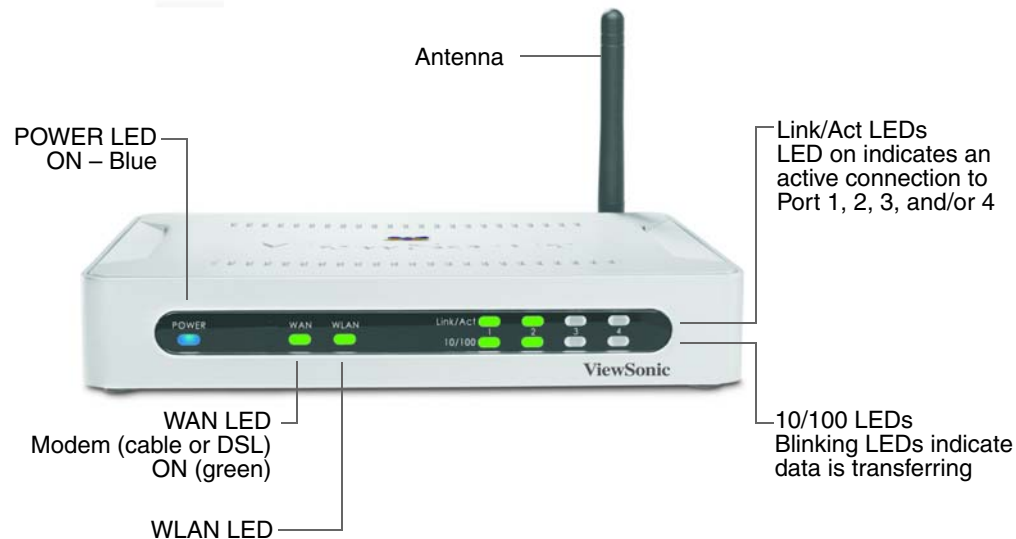
To ensure safe operation, following these simply rules:

- Place device in a safe, secure location.
- Read the user guide thoroughly before installing the device.
- The device should only be repaired by authorized and qualified personnel. Do not try to open or repair the device yourself as this voids the warranty.
- Do not place the device in a damp, wet, or humid location like a bathroom.
- Do not expose the device to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.

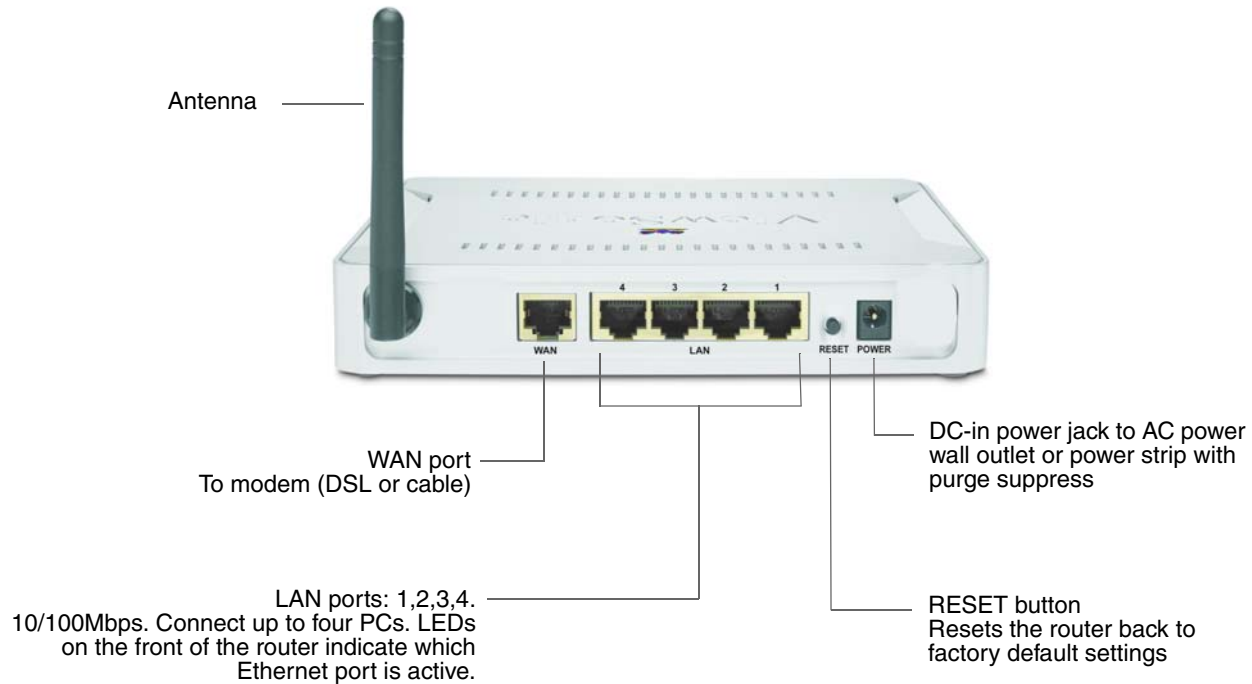
Chapter 2: Product Description

This chapter describes the parts of the router on the **Front** and **Back** panels.

Front of router



Back of router



Chapter 3: Setting up the wireless router

This chapter shows how to set up the ViewSonic wireless router to work with multiple devices in three steps: 1. Connect the wireless router.. 2. Configure your PC (by CD or manually). 3. Configure the wireless router. A typical setup may look like the following:

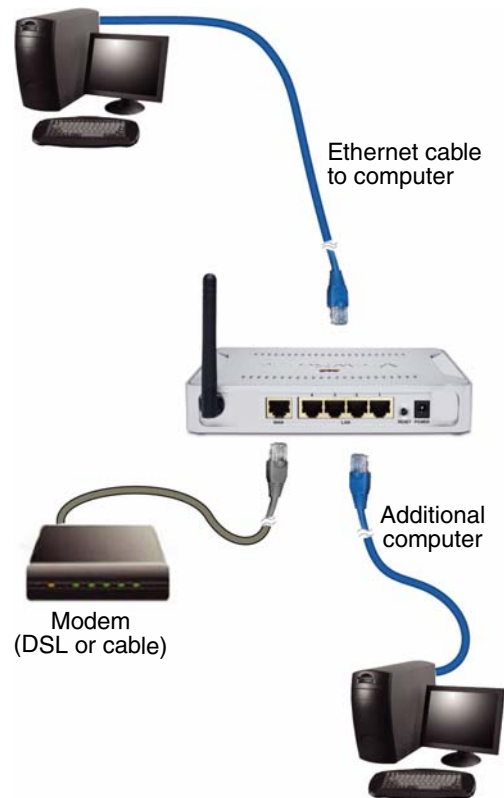


Step 1. Connect the wireless router.

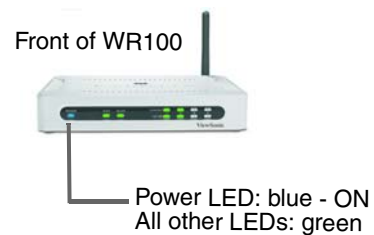
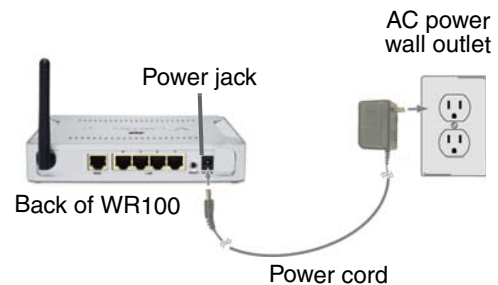
- 1 Make sure you have all the setup information from your Internet Service Provider (ISP) and/or Network IT Administrator.
- 2 Make sure that all network hardware is turned off, including the router, computer(s), and modem (cable or DSL).
- 3 Connect one end of an Ethernet cable to one of the LAN ports (labeled 1, 2, 3, or 4 on the back of the router). Plug the other end of the cable to the Ethernet port on your computer. To connect more computers or network devices to the router, repeat this step.

Optional: Connect another Ethernet cable from your modem (cable or DSL) to the WAN port on the back of the router.

- 4 Connect your modem to the WAN port of the router. Make sure the modem (cable or DSL) power is on.



- 5 Connect the power adapter from the power jack on the back of the router to an AC wall outlet as shown or to a power strip with surge protection. The Power LED on the front of the router turns blue.

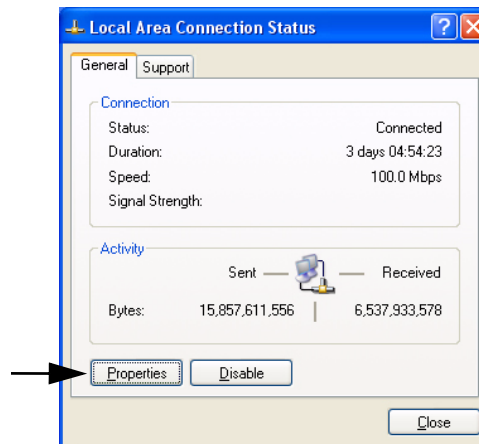


Step 2 Configure your PC

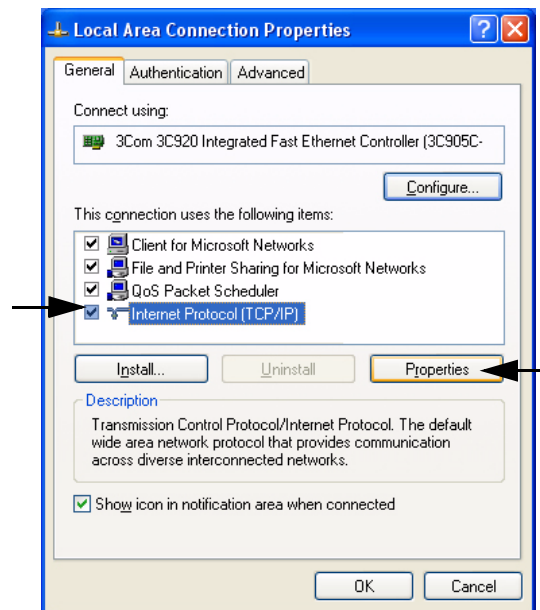
Make sure that your computer is set to DHCP (Dynamic Host Configuration Protocol) to obtain an IP address automatically. By default, your computer should already be set to Obtain an IP Address Automatically. But, if you've changed these settings and want to obtain an IP Address automatically now, do the following:

For Windows 2000 or XP

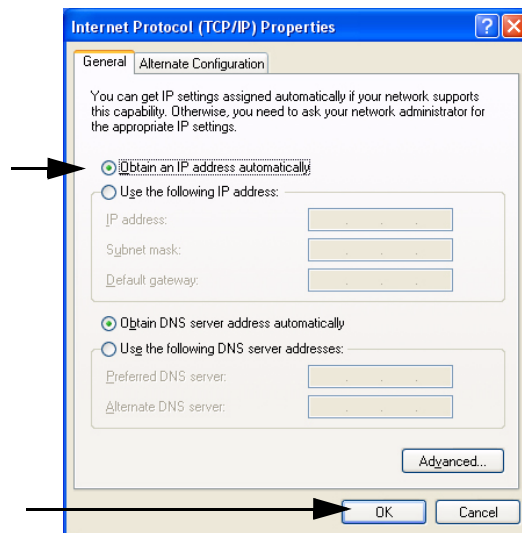
- 1 Click the Windows **Start** button > **Control Panel** > **Network and Internet Connections** > **Local Area Connection**. The **Local Area Connection** screen appears as shown on the right.
- 2 Click **Properties**. The **Local Area Connection Properties** screen appears on the next page.



- 3 Check the box next to **Internet Protocol (TCP/IP)** if it isn't already checked by default. Highlight **Internet Protocol (TCP/IP)** if it isn't already highlighted automatically. Click **Properties**. The **Internet Protocol (TCP/IP) Properties** screen appears.



- 4 Select **Obtain an IP address automatically**. Click **OK > OK > Close** to complete the PC configuration.
- 5 Restart your computer if prompted to do so.



Configuring the wireless router using Web-based utility screens

You only need to configure the router once on any computer that you already have set up. Default settings in the table on the right may be helpful during the configuration process.

- 1 Open your web browser. In the address field, enter **http://192.168.1.1** and press **Enter**. A log on window appears like the one shown on the next page.

Basic Settings	Default
Internet Configuration Type	Automatic Configuration-DHCP
Router* IP Address	192.168.1.1
Router Subnet Mask	255.255.255.0
Router Password	admin (lowercase)
DHCP Settings	
DHCP Server	Enable
DHCP Starting IP Address	192.168.1.100
Number of DHCP Client Users	50
2.4GHz Wireless Setting	
SSID	viewsonic
Channel	6
WEP (Encryption)	Disable

*Wireless Router

Leave the **User name** field empty. In the **Password** field, enter the default password “admin” in all lower case letters. (Later on, for added security, change the password to your own using the password tab with the Password tab of the web-based utility.) Click **OK**. The Primary Setup screen appears as shown on the next page.



Connect to 192.168.1.1

802.11G Wireless Broadband Router

User name:

Password:

☐ Remember my password

OK Cancel

- 2 If requested by your ISP (usually cable ISPs), complete the **Host Name** and **Domain Name** fields. Otherwise, leave them blank. Click the **down arrow** next to the **Connection Type** field. A drop-down menu appears with several connection types as described below. Select a **Connection Type**. The **Primary Setup** screen offers different features depending on the connection type you select. Click **Apply**.

Connection Type:

Automatic Configuration - DHCP. If you are connecting through DHCP or a dynamic IP address from your ISP, keep this default setting.

Static IP. If your ISP assigns you a static IP address, select Static IP from the drop-down menu. Complete the Internet IP Address, Subnet Mask, Default Gateway, and DNS fields. Enter at least one DNS address.

PPPoE. If you are connecting through PPPoE, select PPPoE from the dropdown menu. Complete the User Name and Password fields.

PPTP. PPTP is a service used in Europe only. If you are using a PPTP connection, check with your ISP for the necessary setup information.



The image shows the 'Primary Setup' screen of a ViewSonic Wireless Router. The top navigation bar includes 'Primary Setup', 'Security', 'System', 'DHCP Server', 'Status', and 'Advanced Setting'. The 'Primary Setup' section contains a 'Time Zone' dropdown set to '(GMT-08:00) Pacific Time (USA & Canada)' and a checked checkbox for 'Automatically adjust clock for daylight saving changes.' Below this are three sections: 'Internet', 'LAN', and 'Wireless'. The 'Internet' section shows a MAC Address of '00:0C:10:21:32:03', empty fields for 'Host Name' and 'Domain Name', and a 'Connection Type' dropdown set to 'Dynamic IP Setting'. The 'LAN' section shows a MAC Address of '00:0C:10:21:32:05', an IP Address of '192.168.1.1', and a Subnet Mask of '255.255.255.0'. The 'Wireless' section shows a MAC Address of '00:0C:10:21:32:04', a 'Mode' dropdown set to '11g Only', a 'Domain' of 'FCC', a 'Channel' dropdown set to '3', an empty 'SSID' field, an 'SSID Broadcast' dropdown set to 'Enable', and 'Security' options 'Enable' and 'Disable' with a 'Configure Security' button. At the bottom are 'Apply' and 'Cancel' buttons.

ViewSonic Primary Setup Security System DHCP Server Status Advanced Setting

Primary Setup

This section contains the primary configuration for the Access Point. You should be able to customize easily the Ethernet and Wireless interface in this section. **Remember to press Apply for finalizing your configuration.**

Time Zone: (GMT-08:00) Pacific Time (USA & Canada) ☒ Automatically adjust clock for daylight saving changes.

Internet MAC Address: 00:0C:10:21:32:03

Host Name: Host and Domain settings may be required by your ISP.

Domain Name:

Connection Type: Dynamic IP Setting Select the type of connection you have to the Internet.

LAN MAC Address: 00:0C:10:21:32:05

IP Address: 192.168.1.1 This is the IP address and Subnet Mask of

Subnet Mask: 255.255.255.0 Access Point as it is seen by your local network

Wireless: MAC Address: 00:0C:10:21:32:04

Mode: 11g Only

Domain: FCC

Channel: 3

SSID: SSID Broadcast: Enable

Security: ☐ Enable ☒ Disable

- 3 To configure the router for your wireless network, select one of the following network modes:

2.4GHz Wireless Mode

Mixed: If you have Wireless-G and 802.11b devices in your network, then keep the default setting, Mixed.

G-Only: If you have only Wireless-G devices, select G-Only.

Disable: To disable wireless networking for 54g and 802.11b, select Disable.

- 4 Customize the SSID and Channel settings as needed. For added security, change the default SSID (**viewsonic**) to a unique name and enable **WEP encryption** (recommended). To enable **WEP encryption**, click the **Security tab** from the **Primary Setup** screen. The **Security** screen appears.

- 5 Click **Enable** next to WEP. Click **Edit WEP Settings**. A screen like the one on the right appears. Customize the WEP encryption settings as needed. To save your settings, click **Apply**.
- 6 On the Setup screen, click **Apply** to save your settings. Close the web browser.
- 7 Restart your computer(s) to get the router's new settings if prompted.
- 8 Test the setup by opening your web browser from any computer and entering <http://www.viewsonic.com>. The ViewSonic web site should appear.

For more detailed information, see the Troubleshooting section in this guide. If needed, contact ViewSonic for additional assistance. For contact information, see the Appendix – Customer Support.

G Wireless Router : Wep Key Setting - Microsoft Internet Explo

Security

The Access Point supports 3 differer are: WPA Pre-Shared Key, WPA R2 help tab for more details on the differ

Security Mode: WEP

Default Transmit Key: ☒ 1 ☐ 2 ☐ 3 ☐ 4

WEP Encryption: 64 bits/10 hex digits

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

Wireless

This section provides the Wireless Network settings for your WLAN.

SSID: The service set identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. You shall have selected the same SSID for all the wireless routers that will be communicating with mobile wireless stations.

Domain: The displaying information is related with each domain regulation.

Channel: Select the appropriate channel from the list provided to correspond with your network settings. You shall assign a different channel for each wireless router to avoid signal interference.

Security: There are 3 types of security to be selected. To secure your Wireless Networks, it's strongly recommended that you enable this feature.

WEP: Make sure that all wireless devices on your network are using the same encryption level and key. WEP keys must consist of the letters "A" through "F" and the numbers "0" through "9."

The screenshot shows the 'Primary Setup' page of a ViewSonic wireless router. The 'Wireless' section is expanded, showing fields for MAC Address, Mode (11g Only), Domain (FCC), Channel (3), SSID, and SSID Broadcast (Enable). The 'Security' option is set to 'Enable' and is circled in red. A red arrow points to this option from the left. The page also includes tabs for Primary Setup, Security, System, DHCP Server, Status, and Advanced Setting.

TBD. Writer to fix a screen showing Security **ENABLED** add "viewsonic", change channel number to a shadow,

Important Notice: In order to make the correct use of the WPA, make sure that your current wireless router's driver, and Wireless Utility can support the WPA. The WPA needs 802.1x authentication (when RADIUS mode is chosen), though the Operating System must also support 802.1x protocol. For Microsoft's OS family, only Windows XP has incorporated this by default. Other operating systems must install a third-party client software such as Funk ODySSey.

WPA-Preshared key: There are two encryption options for WPA Pre-Shared Key; **TKIP** and **AES**.

- **TKIP** stands for Temporal Key Integrity Protocol. TKIP uses a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.
- **AES** stands for Advanced Encryption System, which uses a symmetric 128-Bit block data encryption.

To use WPA Pre-Shared Key, enter a password in the WPA Shared Key field between 8 and 63 characters long. You may also enter a Group Key Renewal Interval time between 0 and 99,999 seconds.

WPA RADIUS: WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS Port (default is 1812) and the shared secret from the RADIUS server.

Click Apply to save your settings.

Security Mode: WPA RADIUS
WPA Algorithms: TKIP
RADIUS Server Address: 0 . 0 . 0 . 0
RADIUS Server Port: 1812
Radius Shared Secret:
Group Key Renewal: 300 seconds
Apply Cancel Help

WPA Algorithms
Choose your algorithm method: TKIP or AES.
Radius Server Address
Input your RADIUS Server IP address.
RADIUS Server Port
Input the Authentication port of your RADIUS server; the default port being used is 1812
RADIUS Shared Key
The RADIUS server accepts the authentication if both Shared Keys match.
Group Key Renewal
Input the period of renewal time; the default selection is 300 seconds

Security

Wireless router Password: Change the password for the Wireless router by typing the password in the **Enter New Password** field. Then, type it again into the **Re-enter** field to confirm. Click the **Apply** button to save the setting.

Use the default password (“admin”) when you first open the configuration pages. After you have configured these settings, set a new password for the Wireless router (using the Security screen). This increases security by protecting the Wireless router from unauthorized changes.

VPN Pass-Through: Virtual Private Networking (VPN) is typically used for work-related networking. For VPN tunnels, the Wireless router supports IPsec Pass-Through, L2TP Pass-Through, and PPTP Pass-Through.

- **IPSec** - Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Wireless router, IPSec Pass-Through is enabled by default. To disable IPSec Pass-Through, uncheck the box next to IPSec.
- **L2TP** - Layer 2 Tunneling Protocol is a protocol used to tunnel Point-to-Point Protocol (PPP) over the Internet. To allow L2TP tunnels to pass through the Wireless router, L2TP Pass-Through is enabled by default. To disable L2TP Pass-Through, uncheck the box next to L2TP.

The screenshot shows the 'Security' configuration page of a wireless router. At the top, a note mentions three security types: WPA Pre-Shared Key, WPA RADIUS, and WEP. The 'Security Mode' is currently set to 'WEP'. Under 'Default Transmit Key', there are four radio buttons numbered 1 through 4, with the first one selected. The 'WEP Encryption' is set to '64 bits/10 hex digits'. A 'Passphrase' field is present with a 'Generate' button next to it. Below the passphrase field are four input fields for 'Key 1', 'Key 2', 'Key 3', and 'Key 4'. At the bottom of the page are 'Apply', 'Cancel', and 'Help' buttons. A black arrow points from the right side of the image towards the 'Generate' button.

- **PPTP** - Point-to-Point Tunneling Protocol is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP tunnels to pass through the Wireless router, PPTP Pass-Through is enabled by default. To disable PPTP Pass-Through, uncheck the box next to PPTP.

Web Filters: Using the Web Filters feature, you may enable up to four different filters.

- **Proxy** - Use of WAN proxy servers may compromise network security. Denying Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click the box next to Proxy.
- **Java** - Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. To enable Java filtering, click the box next to Java.
- **ActiveX** - ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click the box next to ActiveX.
- **Cookies** - A cookie is data stored on your PC and used by Internet sites when you interact with them. To enable cookie filtering, click the box next to Cookies.

DMZ: The DMZ hosting feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Forwarding feature is more secure because it only opens the ports you want to have

opened, while DMZ hosting opens all the ports of one computer, exposing the computer so the Internet can see it.

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

1 To expose one PC, select Enable.

2 Enter the computer's IP address in the DMZ Host IP Address field.

3 Click the Apply button.

Block WAN ICMP Request: By enabling the Block WAN Request feature, you can prevent your network from being "pinged," or detected, by other Internet users. The Block WAN Request feature also reinforces your network security by hiding your network ports. Both functions of the Block WAN Request feature make it more difficult for outside users to work their way into your network. This feature is enabled by default. Select **Disable** to disable this feature.

* Check all the settings and click **Apply** to save them.

System

Restore Factory Default: Click the **Yes** button to reset all configuration settings to factory default values.

IMPORTANT: Any settings you have saved will be lost when the default settings are restored. Click the **No** button to disable the Restore Factory Defaults feature.

Click the **Apply** button to save the setting.

Firmware Upgrade: Click the **Upgrade** button to load new firmware onto the Wireless router. If the wireless router is not experiencing difficulties, then there is no need to download a more recent firmware version, unless that version has a new feature that you want to use.

Note: When you upgrade the wireless router's firmware, you may lose its configuration settings, so make sure you write down the wireless router's settings before you upgrade its firmware.

The screenshot shows the 'System' configuration page of a ViewSonic wireless router. The page has a blue header with the ViewSonic logo and a navigation menu with links: Home, Security, System, DHCP, WAN, Status, Help, and Advanced Settings. The 'System' section is active. Below the header, there is a text box stating: 'This section contains some general feature of the Router such as Restore Default, Firmware Upgrade or Remote Management. For further detail of each function, please consult on the User Guide.' The 'Restore Factory Defaults' section has two radio buttons: 'Yes' (selected) and 'No'. Below this is a caution message: 'CAUTION: Any setting you have saved will be lost when the default settings are Yes.' The 'Firmware Upgrade' section has a 'Current Version' field and a 'Firmware Upgrade' button. The 'Multicast Pass-Through' section has a 'Disable' button. The 'MAC Cloning' section has a 'Disable' button and a 'MAC Address' field with four input boxes. The 'Remote Management' section has a 'Disable' button and a 'Port Number' field with the value '8080'. The 'MTU' section has an 'Auto' button and a 'Size' field with the value '1400'. The 'Traffic Log' section has a 'Disable' button. At the bottom of the page are three buttons: 'Apply', 'Cancel', and 'Help'. A large 'TBD' watermark is overlaid on the right side of the form.

To upgrade the Wireless router's firmware:

- 1 Download the firmware upgrade file from the internet.**
- 2 Extract the firmware upgrade file.**
- 3 Click the Upgrade button.**
- 4 On the Firmware Upgrade screen, click the Browse button to locate the firmware upgrade file.**
- 5 Double-click the firmware upgrade file.**
- 6 Click the Upgrade button, and follow the on-screen instructions.**

IMPORTANT! Do not power off the wireless router or press the Reset button while the firmware is being upgraded.



MAC Cloning: The Wireless router's MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs require that you register the MAC address of your network card/adaptor, which was connected to your cable or DSL modem during installation. If your ISP requires MAC address registration, find your wireless router's MAC address by following the instructions for your PC's operating system.

For Windows 98 and Millennium:

- 1 Click the Start button on your PC and select Run.**
- 2 Type "winipcfg" in the field provided and press the OK key.**
- 3 Select the Ethernet Adapter you are using.**
- 4 Click More Info.**
- 5 Write down your Ethernet MAC address.**

For Windows 2000 and XP:

- 1 Click the Start button and select Run.**
- 2 Type cmd in the field provided, and press the OK key.**
- 3 At the command prompt, run ipconfig /all, and look at your wireless router's physical address.**
- 4 Write down your wireless router's MAC address.**

To clone your network wireless router's MAC address onto the wireless router and avoid calling your ISP to change the registered MAC address, follow these instructions.

- 1 Select Enable.**
- 2 Enter your wireless router's MAC address in the MAC Address field.**
- 3 Click the Apply button.**

To disable MAC address cloning, keep the default setting, Disable.

Remote Management: This feature allows you to manage your wireless router from a remote location.

Internet. To disable this feature, keep the default setting, Disable.

To enable this feature, select Enable, and use the specified port (default is 8080) on your PC to remotely manage the wireless router. Also, change the wireless router's default password to one of your own, if you haven't already. A unique password increases security.

To remotely manage the wireless router, enter <http://xxx.xxx.xxx.xxx:8080> (the x's represent the wireless router's Internet IP address, and 8080 represents the specified port) in your web browser's address field. You will be asked for the wireless router's password. After successfully entering the password, you will be able to access the wireless router's web-based utility.

IMPORTANT: If the Remote Management feature is enabled, anyone who knows the wireless router's Internet IP address and password will be able to alter the wireless router's settings.

MTU: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Keep the default setting, Auto, to have the wireless router select the best MTU for your Internet connection, To specify a MTU size, select Manual, and enter the value desired (default is 1400). You should leave this value in the 1200 to 1500 range.

Traffic Log: The wireless router can keep logs of all incoming or outgoing traffic for your Internet connection. This feature is disabled by default. To keep activity logs, select Enable.

To keep a permanent record of activity logs as a file on your PC's hard drive, Log viewer software must be used. In the Send Log to field, enter the fixed IP address of the PC running the Log viewer software. The wireless router will send updated logs to that PC.

To see a temporary log of the wireless router's most recent incoming traffic, click the Incoming Access Log button. To see a temporary log of the wireless router's most recent outgoing traffic,

click the Outgoing Access Log button. Click the Apply button to save the setting.

DHCP Server

The DHCP Server screen allows you to configure the settings for the wireless router's Dynamic Host Configuration Protocol (DHCP) server function. The wireless router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the wireless router's DHCP server option, you must configure your entire network PCs to connect to a DHCP server, the wireless router.

If you disable the wireless router's DHCP server function, you must configure the IP Address, Subnet Mask, and DNS for each network computer (note that each IP Address must be unique).

DHCP Server: Select the Enable option to enable the wireless router's DHCP server option.

If you already have a DHCP server on your network or you do not want a DHCP server, then select Disable from the options.

The screenshot shows the ViewSonic DHCP Server configuration page. At the top, there is a navigation bar with tabs: Primary Setup, Security, System, DHCP Server, Status, and Advanced Setting. The DHCP Server tab is selected. Below the navigation bar, there is a section titled 'DHCP Server' with a description: 'You can customize and make use of the Router to accomplish the DHCP Server Role in your Network. A DHCP Server automatically distribute and assign one unique IP to each workstation in your Network, if you have already have a DHCP Server, please disable this feature to avoid any conflict.' Below this, there is a 'DHCP Server' dropdown menu with 'Enable' selected, which is circled in red. Below the dropdown, there are several input fields: 'Starting IP Address' (192.168.1.100), 'Maximum Number of DHCP Users' (50), 'Client Lease Time' (0 Minutes), 'Static DNS 1', 'Static DNS 2', 'Static DNS 3', and 'WINS'. At the bottom, there is a 'Currently Assigned' section with a 'DHCP Clients Table' button. The 'Apply' button is circled in red.

Starting IP Address: Enter a numerical value for the DHCP server to start with when issuing IP addresses. Because the wireless router's default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.5.253. The default Starting IP Address is 192.168.1.100.

Maximum Number of DHCP Users: Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The absolute maximum is 253 - possible if 192.168.1.1 is your starting IP address. The default is 50.

Client Lease Time: The Client Lease Time is the amount of time a network user will be allowed connection to the wireless router with their current dynamic IP address.

Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. The default is 0 minutes, which means one day.

Static DNS 1-3: The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to utilize another, enter that IP Address in one of these fields. You can enter up to three DNS Server IP Addresses here. The wireless router will utilize these for quicker access to functioning DNS servers.

WINS: The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

Currently Assigned: Click the DHCP Clients Table button to see a list of PCs assigned IP addresses by the wireless router. For each PC, the list shows the client hostname, MAC address, IP address, and the amount of DHCP client lease time left. Click the **Refresh** button to display the most current information.

* Click **Apply** to save your settings.

Status

This screen displays the wireless router's current status and settings. This information is read-only.

This page will auto re-flash every five seconds to keep most update information.

Host Name: The **Host Name** is the name of the wireless router. This entry is necessary for some ISPs.

Domain Name: The **Domain Name** is the name of the wireless router's domain. This entry is necessary for some ISPs.

WAN IP Release: Click the **WAN IP Release** button to delete the wireless router's current Internet IP address.

WAN IP Renew: Click the **WAN IP Renew** button to get a new Internet IP address for the wireless router.

*Click the **Refresh** button to refresh the wireless router's status and settings.

ViewSonic Primary Setup Security System DHCP Server **Status** Advanced Setting

Status This section contains a summary of the system. Please note that the information will be updated and displayed automatically every 10 seconds.

Firmware Version: v1.03 (ViewSonic for test), May 19, 2004
Current Time: Thu Jan 1 00:03:58 1970
Host Name:
Domain Name:

LAN **MAC Address:** 00:0C:10:21:32:05
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP server: Enable

Wireless **MAC Address:** 00:0C:10:21:32:04
Mode: 11g Only
Channel: 3
SSID: ViewSonic
Encryption Function: Disabled

WAN **MAC Address:** 00:0C:10:21:32:06
Configuration Type: Automatic Configuration - DHCP
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0
DNS: 0.0.0.0
WAN IP Release **WAN IP Renew**
Refresh

Advanced Wireless

Wireless MAC Filters: This function allows the administrator to have access control by entering the MAC address of client stations.

- 1 When you select **Enable**, two new options appear under Wireless MAC Filters: **Prevent** or **Permit**.
- 2 Select **Prevent** or **Permit**.
- 3 Click on **Edit MAC Filter List** to add the client stations. The MAC list shown on the next page.

ViewSonic Advanced Wireless Access Filter Virtual Server Routing Table Primary Setup

Advanced Wireless The Advanced Wireless settings should be left at their default values. Improper configuration may result in poor network performance.

Wireless MAC Filter: ☒ **Enable**

☐ Prevent PCs listed from accessing the wireless network.

☒ Permit PCs listed to access the wireless network.

[Edit MAC Filter List](#)

Authentication Type: Auto (Default: Auto)

Transmit Rate: Auto (Default: Auto)

Beacon Interval: 100 (Default: 100, Milliseconds, Range: 1 - 65535)

DTIM Interval: 1 (Default: 3, Range: 1 - 255)

RTS Threshold: 2347 (Default: 2346, Range: 0 - 2346)

Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 2346)

Operating Mode: ☒ Access Point (Default Selection)

☐ Wireless Bridge

Please input the MAC Address of the remote Wireless Bridge:

Note: When the unit is operating as "Wireless Bridge", it will interact only with other remote Wireless Bridge on the MAC Address list.

Apply Cancel

The list could store up to 40 different MAC addresses. When entering an address, use the format shown under the title of the screen.

MAC Address Filter List

Enter MAC Address in (xx:xx:xx:xx:xx:xx) format

MAC Addresses 1~20

MAC 01 :	00:00:00:00:00:00	MAC 11 :	00:00:00:00:00:00
MAC 02 :	00:00:00:00:00:00	MAC 12 :	00:00:00:00:00:00
MAC 03 :	00:00:00:00:00:00	MAC 13 :	00:00:00:00:00:00
MAC 04 :	00:00:00:00:00:00	MAC 14 :	00:00:00:00:00:00
MAC 05 :	00:00:00:00:00:00	MAC 15 :	00:00:00:00:00:00
MAC 06 :	00:00:00:00:00:00	MAC 16 :	00:00:00:00:00:00
MAC 07 :	00:00:00:00:00:00	MAC 17 :	00:00:00:00:00:00
MAC 08 :	00:00:00:00:00:00	MAC 18 :	00:00:00:00:00:00
MAC 09 :	00:00:00:00:00:00	MAC 19 :	00:00:00:00:00:00
MAC 10 :	00:00:00:00:00:00	MAC 20 :	00:00:00:00:00:00

ApplyCancelClose

Authentication Type:

Auto: Auto is the default authentication algorithm. It will change its authentication type automatically to fulfill client's requirement.

Open System: Open System authentication is not required to be successful while a client may decline to authenticate with any particular other client.

Shared Key: Shared Key is only available if the WEP option is implemented. Shared Key authentication supports authentication of clients as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in clear. Requiring the use of the WEP privacy mechanism.

Transmission Rate: The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select AUTO to have the wireless router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the wireless router and a wireless client. The default setting is AUTO.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends

the next DTIM with a DTIM Interval value. Access Point Clients hear the beacons and awaken to receive the broadcast and multicast messages.

Beacon Interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the wireless router to synchronize the wireless network. The default value is 100.

RTS Threshold: This value should remain at its default setting of 2346. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The wireless router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

Fragmentation Threshold: This value specifies the maximum size for a packet before data is fragmented into multiple packets. It should remain at its default setting of 2346. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

AP Mode or Wireless Bridge Mode: wireless router can operate in two modes. When the AP Mode is selected, the device operates

as a normal Access Point. Providing every wireless client station a join network point. The Wireless Bridge Mode will be able to join different wireless router wirelessly by input the destination MAC Address.

* Click Apply to save your settings.

Access Filters

The Access Filter screen allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific PCs and set up filters by using network port numbers.

ViewSonic

Advanced Wireless Access Filter Virtual Server Routing Table Primary Setup

Access Filter

In this section you can easily create policy to prevent and allow any traffic from Internet connection to your Network.

Internet Access Policy: 1 (-) Delete Summary

Enter Policy Name:

Policy Type: Outgoing Traffic

☒ Deny ☐ Allow

PCs: Edit List

Days: ☒ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Time: ☒ 24 Hours ☐ From: 1:00 AM To: 1:00 AM

Blocking Services: Disable 0 Add Service

Add service to list

ViewSonic Advanced Wireless Access Filter Virtual Server Routing Table Primary Setup

Access Filter In this section you can easily create policy to prevent and allow any traffic from Internet connection to your Network.

Internet Access Policy: 1 (←) Delete Summary

Enter Policy Name:
Policy Type: Outgoing Traffic
☒ Deny ☐ Allow Internet access for listed PCs during selected days and hours.
PCs:
Days: ☒ Everyday
☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
Time: ☒ 24 Hours
☐ From: 1:00 AM To: 1:00 AM
Blocking Services: Disable 0 ~ 0

Service Name
Protocol ICMP
Port Range ~

DNS [53~53]
Ping [0~0]
HTTP [80~80]
HTTPS [443~443]
FTP [21~21]
POP3 [110~110]
IMAP [143~143]
SMTP [25~25]
NNTP [119~119]
Telnet [23~23]
SNMP [161~161]
TFTP [69~69]

INTERNET ACCESS POLICY

This feature allows you to customize up to ten (10) different Internet Access Policies for particular PCs, which are identified by their IP or MAC addresses. For each policy's designated PCs, the wireless router can do one or more of the following:

- Block or allow Internet access or inbound traffic during the days and time periods specified
- Block designated services
- Block websites with specific URL addresses
- Block websites that use specific keywords in their URL addresses.

To create or edit a policy, do the following:

- 1** Select the policy's number (1-10) in the drop-down menu.
- 2** Enter a name in the **Enter Policy Name** field.
- 3** Select Internet Access or **Inbound Traffic** from the Policy Type drop-down box, depending on the kind of access you want to control. Select **Internet Access** to control your network PCs' access to the Internet. Select **Inbound Traffic** to control Internet PCs' access to your local area network.

IMPORTANT! The screen's settings will vary depending on which Policy Type you select.

- 4 Select Deny or Allow, depending on how you want to control access for specific PCs.
 - 5 Click the Edit List button next to PCs or Internet PCs.
 - A. On the List of PCs or List of Internet PCs screen, specify PCs by IP address or MAC address. Enter the appropriate IP addresses into the IP fields. If you have a range of IP addresses to filter, complete the appropriate IP Range fields. Enter the appropriate MAC addresses into the MAC fields.
 - B. Click the **Apply** button to save your changes. Click the **Cancel** button to cancel your unsaved changes. Click the **Close** button to return to the Internet Filter screen.
 - 6 Set the days when access will be filtered. Keep the default setting, Everyday, or select the appropriate days of the week.
 - 7 Set the time when access will be filtered. Keep the default setting, 24 Hours, or check the box next to From and use the drop-down boxes to designate a specific time period.
- IMPORTANT!** Access for the listed PCs is controlled during the selected days and times. Any blocked services or websites are blocked at all times.
- 8 In the Blocking Services drop-down boxes, select the services you want to block (the default setting is None). In the Blocking Services fields, the range of ports for this service will appear. If

The top screenshot shows the 'Access Filter' configuration page. The 'Policy Type' is set to 'Outgoing Traffic'. The 'PCs' section has the 'Edit List' button circled in red. The 'Days' section shows 'Everyday' selected. The 'Time' section shows '24 Hours' selected. The 'Create' button is at the bottom right.

The bottom screenshot shows the 'Blocking Services' configuration page. The 'Blocking Services' list includes DNS, Ping, HTTP, HTTPS, FTP, POP3, SMTP, NNTP, Telnet, SNMP, and TFTP. The 'Website Blocking by URL' and 'Website Blocking by Keyword' sections are visible. The 'Apply' button is circled in red at the bottom right.

you want to change the range of **ports**, enter the new numbers in the Blocking Services fields, or edit the service's settings.

To add a service or edit a service's settings

- A. Click the **Add Service** button.
 - B. To create a new service, enter the name of the service in the **Service Name** field. To edit a service's settings, select the service from the box on the right of the screen.
 - C. From the **Protocol** drop-down menu, select the protocol type for this service: **ICMP**, **UDP**, **TCP**, or **UDP & TCP**.
 - D. In the **Port Range** fields, enter the range of ports for this service.
 - E. To add a service, click the **Add** button. To edit the settings for a service, click the **Modify** button.
 - F. To delete a service, select the service from the box on the right of the screen. Click the **Delete** button.
 - G. Click the **Apply** button to save your changes. Click the **Cancel** button to undo your changes. Click the **Close** button to close the **Add Service** window.
- 9** If you want to block websites with specific URL addresses, enter each URL address in a Website Blocking by URL Address field. You can enter up to four URL addresses. (This feature is not available if you chose Inbound Traffic for the Policy Type.)
- 10** If you want to block websites that use specific keywords as part of their URL addresses, enter each keyword in a Website

Service Name

Protocol: ICMP

Port Range: ~

Add Modify Delete

Apply Cancel Close

- DNS [53~53]
- Ping [0~0]
- HTTP [80~80]
- HTTPS [443~443]
- FTP [21~21]
- POP3 [110~110]
- IMAP [143~143]
- SMTP [25~25]
- NNTP [119~119]
- Telnet [23~23]
- SNMP [161~161]
- TFTP [69~69]

Blocking by Keyword field. You can enter up to six keywords.
(This feature is not available if you chose Inbound Traffic for the Policy Type.)

11 Click the **Apply** button to save your settings for an Internet Access Policy. Click the **Cancel** button to cancel your unsaved changes.

12 To create or edit additional policies, repeat steps 1-11.

Delete

To delete an Internet Access Policy, select the policy's number, and click the **Delete** button.

Summary

To see a summary of all the policies, click the **Summary** button. The **Internet Policy Summary** screen will show each policy's number, Name, Type, Days, and Time of Day. To delete a policy, click its box, and then click the **Delete** button. Click the **Close** button to return to the **Internet Filter** screen.

Virtual Server

The **Virtual Server** screen sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

When users send this type of request to your network via the Internet, the wireless router will forward those requests to the appropriate PC. Any PC whose port is being forwarded must have its **DHCP client** function disabled and must have a new static IP address assigned to it because its IP address may change when using the DHCP function.



The screenshot shows the 'Virtual Server' configuration page of a ViewSonic wireless router. At the top, there are navigation tabs: 'Advanced Wireless', 'Access Filter', 'Virtual Server' (selected), 'Routing Table', and 'Primary Setup'. Below the tabs, a description states: 'This feature allows you to send incoming traffic on certain ports to a defined PC. This can let you setup a web server, mail server, FTP server, DNS, etc on your LAN so it can be accessed from the Internet.' The main section is titled 'Customized Applications' and contains a table with columns: 'External Port', 'Protocol TCP', 'Protocol UDP', 'IP Address', and 'Enable'. There are 10 rows in the table, each with input fields for the external port, protocol checkboxes, and IP address, followed by an 'Enable' checkbox. Below the table, there is a 'Port Triggering' button and 'Apply' and 'Cancel' buttons.

External Port	Protocol TCP	Protocol UDP	IP Address	Enable
0 to 0	☐	☐	192.168.1.0	☐
0 to 0	☐	☐	192.168.1.0	☐
0 to 0	☐	☐	192.168.1.0	☐
0 to 0	☐	☐	192.168.1.0	☐
0 to 0	☐	☐	192.168.1.0	☐
0 to 0	☐	☐	192.168.1.0	☐
0 to 0	☐	☐	192.168.1.0	☐
0 to 0	☐	☐	192.168.1.0	☐
0 to 0	☐	☐	192.168.1.0	☐
0 to 0	☐	☐	192.168.1.0	☐

Port Triggering

Apply Cancel

Customized Applications
Enter the name of the public service or other Internet application in the field provided.
External Port
Enter the numbers of the External Ports (the port numbers seen by users on the Internet).
TCP Protocol
Click this checkbox if the application requires TCP.
UDP Protocol
Click this checkbox if the application requires UDP.
IP Address
Enter the IP Address of the PC running the application.
Enable
Click the Enable checkbox to enable port forwarding for the application.
Port Triggering

Port Triggering is used for special Internet applications whose outgoing ports differ from the incoming ports. For this feature, the wireless router will watch outgoing data for specific port numbers. The wireless router will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the wireless router, the data is pulled back to the proper computer by way of IP address and port mapping rules. Click the Port Triggering button to set up triggered ports, and follow these instructions:

1 Enter the Application Name of the trigger.

2 Enter the Outgoing Port Range used by the application. Check with the Internet application for the port number(s) needed.

3 Enter the Incoming Port Range used by the application. Check with the Internet application for the port number(s) needed.

4 Click the Apply button to save your changes. Click the Cancel button to cancel your unsaved changes. Click the Close button to return to the Port Forwarding screen.

Check all the settings and click **Apply** to save them.

Routing Table

On the Routing Table screen, you can set the routing mode and settings of the wireless router. Gateway mode is recommended for most users.

Operating Mode

The default setting is **Gateway**. Choose the correct working mode. Keep the default setting, Gateway, if the wireless router is hosting your network's connection to the Internet (Gateway mode is recommended for most users). Select wireless router if the wireless router exists on a network with other routers.

Dynamic Routing (RIP)

IMPORTANT! This feature is not available in **Gateway** mode. The default setting is **Disable**.

Dynamic Routing enables the wireless router to automatically adjust to physical changes in the network's layout and exchange routing tables with other wireless routers. The wireless router determines the network packets' route based on the fewest number of hops between the source and destination.

To enable the Dynamic Routing feature, select **Enable**. To disable the Dynamic Routing feature for all data transmissions, keep the default setting, **Disable**.

The screenshot shows the 'Routing Table' configuration page of a ViewSonic wireless router. The page has a blue header with the ViewSonic logo and navigation tabs: 'Advanced Wireless', 'Access Filter', 'Virtual Server', 'Routing Table' (selected), and 'Primary Setup'. Below the header, the 'Routing Table' section is titled. A note states: 'If there is more than one router on a network, this Routing table must be configured because the router needs to know what packet goes to which router. A routing table entry is required for each LAN segment on the network.' The configuration area includes a 'Static Routing' section with a dropdown menu set to '1 -- (Select Route Entry)' and a 'Delete This Entry' button. Below this are input fields for 'Enter Route Name:', 'Destination IP Address:' (0 . 0 . 0 . 0), 'Subnet Mask:' (0 . 0 . 0 . 0), 'Gateway:' (0 . 0 . 0 . 0), and 'Interface:' (LAN & Wireless). There is a 'Show Routing Table' button. At the bottom are 'Apply' and 'Cancel' buttons.

Static Routing, Destination IP Address, Subnet Mask, Gateway, and Interface

- 1 To set up a static route between the wireless router and another network, select a number from the Static Routing drop-down list. (A static route is a pre-determined pathway that network information must travel to reach a specific host or network.)
- 2 Enter the following data:
 - **Destination IP Address** - The **Destination IP Address** is the address of the network or host that you want to assign a static route.
 - **Subnet Mask** - The **Subnet Mask** determines which portion of an IP address is the network portion, and which portion is the host portion.
 - **Gateway** - This is the IP address of the gateway device that allows for contact between the wireless router and the network or host.
- 3 Depending on where the Destination IP Address is located, select **LAN & Wireless** or **Internet (WAN)** from the Interface drop-down menu.
- 4 To save your changes, click the **Apply** button. To cancel your unsaved changes, click the **Cancel** button.
- 5 For additional static routes, repeat steps 1-4.

To delete a static route entry:

- 1** From the **Static Routing** drop-down list, select the **Entry Number** of the static route.
- 2** Click **Delete This Entry**.
- 3** To save a deletion, click **Apply** button. To cancel a deletion, click the **Cancel** button.

Click the **Show Routing Table** button to view all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry. Click the **Refresh** button to refresh the data displayed.

- **Destination LAN IP** - The Destination IP Address is the address of the network or host to which the static route is assigned.
- **Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- **Gateway** - This is the IP address of the gateway device that allows for contact between the wireless router and the network or host.
- **Interface** - This interface tells you whether the Destination IP Address is on the LAN & Wireless (internal wired and wireless networks), the WAN (Internet), or Loopback (a dummy network in which one PC acts like a network—necessary for certain software programs).

* Click **Apply** to save your settings.

Appendix

The Appendix has the following sections:

- Specification
- Wireless Security & Glossary
- Troubleshooting
- Compliances
- Cleaning & Maintenance
- Customer Support
- Limited Warranty

Specifications

WLAN standards	IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps IEEE 802.11b: 11, 5.5, 2, 1 Mbps
Ports	WAN: 1 LAN: 4
Main Board Memory	Flash: 4MB SDRAM: 8MB
Antenna	Single external antennas
LED Status	LEDs: Power, Standby, Ethernet & Wireless Link/Activity
Networking Interface	Ethernet: IEEE 802.3 10-base T, IEEE 802.3u 100-base T Wireless: IEEE 802.11g (2.4Ghz-DSSS)
Channels	1-11 United States, Canada
Output Power	Max 100 mW (after antenna)
Coverage Area	Up to 100 meters indoors Up to 400 meters outdoors
Wireless Security	64/128 bit WEP Encryption, WPA (Windows XP SP1 and Windows 2000 SP4 only)
Integrated VPN	Router supports VPN (L2TP and IPSec) traffic. Router also supports reverse VPN functionality.
Physical Dimensions	180 mm x 30 mm x 148 mm 7.08" x 1.18" x 5.83"
Weight	Net: TBD lb. (TBD kg) Gross: TBD lb. (TBD kg)

Wireless Security & Glossary

10BaseT. An IEEE standard (802.3) for operating 10 Mbps Ethernet networks (LANs) with twisted pair cabling and a wiring hub.

802.11 standard. 802.11 or IEEE 802.11 is a type of radio technology used for wireless local area networks (WLANs). It is a standard that has been developed by the IEEE (Institute of Electrical and Electronic Engineers), <http://standards.ieee.org>. The IEEE is an international organization that develops standards for hundreds of electronic and electrical technologies. The organization uses a series of numbers, like the Dewey Decimal system in libraries, to differentiate between the various technology families.

The 802 subgroup (of the IEEE) develops standards for local and wide area networks with the 802.11 section reviewing and creating standards for wireless local area networks.

Wi-Fi, 802.11 is composed of several standards operating in different radio frequencies: 802.11b is a standard for wireless LANs operating in the 2.4 GHz spectrum with a bandwidth of 11 Mbps; 802.11a is a different standard for wireless LANs, and pertains to systems operating in the 5 GHz frequency range with a bandwidth of 54 Mbps. Another standard, 802.11g, is for WLANs operating in the 2.4 GHz frequency but with a bandwidth of 54 Mbps.

802.11a. An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.725 GHz to 5.850 GHz) with a maximum 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz frequency, because the 802.11a specification offers more radio channels than the 802.11b. These additional channels can help avoid radio and microwave interference.

802.11b. International standard for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835 GHz) and provides a throughput of up to 11 Mbps. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz frequency band.

802.11g. Similar to 802.11b, but this standard provides a throughput of up to 54 Mbps. It also operates in the 2.4 GHz frequency band but uses a different radio technology in order to boost overall bandwidth.

Access point. A wireless LAN transceiver or “base station” that can connect a wired LAN to one or many wireless devices. Access points can also bridge to each other. There are various types of access points and base stations used in both wireless and wired networks. These include bridges, hubs, switches, routers and gateways. The differences between them are not always precise, because certain capabilities associated with one can also be added to another. For example, a router can do bridging, and a hub may

also be a switch. But they are all involved in making sure data is transferred from one location to another.

A bridge connects devices that all use the same kind of protocol. A router can connect networks that use differing protocols. It also reads the addresses included in the packets and routes them to the appropriate computer station, working with any other routers in the network to choose the best path to send the packets on. A wireless hub or access point adds a few capabilities such as roaming and provides a network connection to a variety of clients, but it does not allocate bandwidth. A switch is a hub that has extra intelligence: It can read the address of a packet and send it to the appropriate computer station. A wireless gateway is an access point that provides additional capabilities such as NAT routing, DHCP, firewalls, security, etc.

Ad-Hoc mode. A client setting that provides independent peer-to-peer connectivity in a wireless LAN. An alternative set-up is one where PCs communicate with each other through an AP.

Applet. An application or utility program that is designed to do a very specific and limited task.

Backbone. The central part of a large network that links two or more subnetworks and is the primary path for data transmission for a large business or corporation. A network can have a wired backbone or a wireless backbone.

Bandwidth. The amount of transmission capacity that is available on a network at any point in time. Available bandwidth depends on several variables such as the rate of data transmission speed between networked devices, network overhead, number of users, and the type of device used to connect PCs to a network. It is similar to a pipeline in that capacity is determined by size: the wider the pipe, the more water can flow through it; the more bandwidth a network provides, the more data can flow through it. Standard 802.11b provides a bandwidth of 11 Mbps; 802.11a and 802.11g provide a bandwidth of 54 Mbps.

Bits per second (bps). A measure of data transmission speed over communication lines based on the number of bits that can be sent or received per second. Bits per second—bps—is often confused with bytes per second—Bps. While "bits" is a measure of transmission speed, "bytes" is a measure of storage capability. 8 bits make a byte, so if a wireless network is operating at a bandwidth of 11 megabits per second (11 Mbps or 11 Mbits/sec), it is sending data at 1.375 megabytes per second (1.375 MBps).

Bluetooth wireless technology. A technology specification for linking portable computers, personal digital assistants (PDAs) and mobile phones for short-range transmission of voice and data across a global radio frequency band without the need for cables or wires. Bluetooth is a frequency-hopping technology in the 2.4 GHz frequency spectrum, with a range of 30 feet.

Bridge. A product that connects a local area network (LAN) to another local area network that uses the same protocol (for

example, wireless, Ethernet or token ring). Wireless bridges are commonly used to link buildings in campuses.

Broadband. A comparatively fast Internet connection. Services such as ISDN, cable modem, DSL and satellite are all considered broadband as compared to dial-up Internet access. There is no official speed definition of broadband but services of 100Kbps and above are commonly thought of as broadband.

Bus adapter. A special adapter card that installs in a PC's PCI or ISA slot and enables the use of PC Card radios in desktop computers. Some companies offer one-piece PCI or ISA Card radios that install directly into an open PC or ISA slot.

Cable modem. A kind of converter used to connect a computer to a cable TV service that provides Internet access. Most cable modems have an Ethernet out-cable that then attaches to the user's Wi-Fi gateway.

Client. Any computer connected to a network that requests services (files, print capability) from another member of the network.

Client devices. Clients are end users. Wi-Fi client devices include PC Cards that slide into laptop computers, mini-PCI modules embedded in laptop computers and mobile computing devices, as well as USB radios and PCI/ISA bus Wi-Fi radios. Client devices usually communicate with hub devices like access points and gateways.

Collision avoidance. A network node characteristic for proactively detecting that it can transmit a signal without risking a collision.

Crossover cable. A special cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. Instead of the signals transferring in parallel paths from one set of plugs to another, the signals "crossover." If an eight-wire cable was being used, for instance, the signal would start on pin one at one end of the cable and end up on pin eight at the other end. They "cross-over" from one side to the other.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The principle medium access method employed by IEEE 802.11 WLANs. It is a "listen before talk": method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states collision avoidance method rather than collision detection must be used, because the standard employs half duplex radios—radios capable of transmission or reception—but not both simultaneously. Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission.

CSMA/CD (Carrier Sense Multiple Access/Collision Detection). A method of managing traffic and reducing noise on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect a collision and retransmit after a random time delay.

DC power module. Modules that convert AC power to DC. Depending on manufacturer and product, these modules can range

from typical "wall wart" transformers that plug into a wall socket and provide DC power via a tiny plug to larger, enterprise-level Power Over Ethernet systems that inject DC power into the Ethernet cables connecting access points.

DHCP (Dynamic Host Configuration Protocol). A utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT Manager would have to manually enter in all the IP addresses of all the computers on the network. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it.

Dial-up. A communication connection via the standard telephone network, or Plain Old Telephone Service (POTS).

Diversity antenna - A type of antenna system that uses two antennas to maximize reception and transmission quality and reduce interference.

DNS (Domain Name System, or Service, or Server). A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.

DSL (Digital Subscriber Lines). Various technology protocols for high-speed data, voice and video transmission over ordinary twisted-pair copper POTS (Plain Old Telephone Service) telephone wires.

Encryption key. An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read.

ESSID (Extended Service Set ID). The identifying name of an 802.11 wireless network. When you specify your correct ESSID in your client setup you ensure that you connect to your wireless network rather than another network in range. (See SSID.) The ESSID can be called by different terms, such as Network Name, Preferred Network, SSID or Wireless LAN Service Area.

Ethernet. International standard networking technology for wired implementations. Basic 10BaseT networks offer a bandwidth of about 10 Mbps. Fast Ethernet (100 Mbps) and Gigabit Ethernet (1000 Mbps) are becoming popular.

Firewall. A system that secures a network and prevents access by unauthorized users. Firewalls can be software, hardware or a combination of both. Firewalls can prevent unrestricted access into a network, as well as restrict data from flowing out of a network.

Gateway. In the wireless world, a gateway is an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

HotSpot. A place where you can access Wi-Fi service. This can be for free or for a fee. HotSpots can be inside a coffeeshop, airport lounge, train station, convention center, hotel or any other public meeting area. Corporations and campuses are also implementing HotSpots to provide wireless Internet access to their visitors and guests. In some parts of the world, HotSpots are known as CoolSpots.

Hub. A multiport device used to connect PCs to a network via Ethernet cabling or via WiFi. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multigigabyte speeds per second. A hub transmits packets it receives to all the connected ports. A small wired hub may only connect four computers; a large hub can connect 48 or more. Wireless hubs can connect hundreds.

HZ (Hertz). The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535—1605 kHz, the FM broadcast radio frequency band is 88—108 MHz, and wireless 802.11b LANs operate at 2.4 GHz.

IEEE (Institute of Electrical and Electronics Engineers), New York, www.ieee.org. A membership organization that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.

IEEE802.11. A set of specifications for LANs from The Institute of Electrical and Electronics Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5, the specification for token ring networks. 802.11 defines the standard for wireless LANs encompassing three incompatible (non-interoperable) technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared. WECA's focus is on 802.11b, an 11 Mbps high-rate DSSS standard for wireless networks.

Infrastructure mode. A client setting providing connectivity to an AP. As compared to Ad-Hoc mode, whereby PCs communicate directly with each other, clients set in Infrastructure Mode all pass data through a central AP. The AP not only mediates wireless network traffic in the immediate neighborhood, but also provides communication with the wired network. See Ad-Hoc and AP.

Internet appliance. A computer that is intended primarily for Internet access, is simple to set up and usually does not support installation of third-party software. These computers generally offer customized web browsing, touch-screen navigation, e-mail services, entertainment and personal information management

applications. An Internet appliance can be Wi-Fi enabled or it can be connected via a cable to the local network.

IP (telephony). Technology that supports voice, data and video transmission via IP-based LANs, WANs, and the Internet. This includes VoIP (Voice over IP).

IP address. A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.

IPX-SPX (Internetwork Packet Exchange-Sequenced Packet Exchange). IPX is a networking protocol used by the Novell NetWare operating systems. Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as SPX and NCP, are used for additional error recovery services. SPX is a transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks. The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications. Whereas the IPX protocol is similar to IP, SPX is similar to TCP. Together, therefore, IPX-SPX provides connection services similar to TCP/IP.

ISA (Industry Standard Architecture). A type of internal computer bus that allows the addition of card-based components like

modems and network adapters. ISA has been replaced by PCI and is not very common anymore.

ISO Network Model (International Standards Organization). A network model developed by the ISO that consists of seven different levels, or layers. By standardizing these layers, and the interfaces in between, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are:

- Physical
- Data Link
- Network
- Transport
- Session
- Presentation
- Application

The IEEE 802.11 Standard encompasses the physical layer (PHY) and the lower portion of the data link layer. The lower portion of the data link layer is often referred to as the Medium Access Controller (MAC) sublayer.

ISS (Internet Security Services). A special software application that allows all PCs on a network access to the Internet simultaneously through a single connection and Internet Service Provider (ISP) account.

LAN (Local Area Network). A system of connecting PCs and other devices within the same physical proximity for sharing resources

such as an Internet connections, printers, files and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN.

MAC (Medium Access Controller). Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.

Mapping. Assigning a PC to a shared drive or printer port on a network.

NAT (Network Address Translation). A network capability that enables a houseful of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network. NAT provides a type of firewall by hiding internal IP addresses.

Network name. Identifies the wireless network for all the shared components. During the installation process for most wireless networks, you need to enter the network name or SSID. Different network names are used when setting up your individual computer, wired network or workgroup.

NIC (Network Interface Card). An expansion board you insert into a computer so the computer can be connected to a network. A NIC is

a type of PC adapter card that either works without wires (Wi-Fi) or attaches to a network cable to provide two-way communication between the computer and network devices such as a hub or switch. Most office wired NICs operate at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available. See PC Card.

PC Card. A removable, credit-card-sized memory or I/O device that fits into a Type 2 PCMCIA standard slot, PC Cards are used primarily in PCs, portable computers, PDAs and laptops. PC Card peripherals include Wi-Fi cards, memory cards, modems, NICs, hard drives, etc.

PCI (Peripheral Component Interconnect). A high-performance I/O computer bus used internally on most computers. Other bus types include ISA and AGP. PCIs and other computer buses enable the addition of internal cards that provide services and features not supported by the motherboard or other connectors.

PCMCIA (Personal Computer Memory Card International Association). Expansion cards now referred to as “PC Cards” were originally called “PCMCIA Cards” because they met the standards created by the PCMCIA.

Peer-to-peer network. A wireless or wired computer network that has no server or central hub or router. All the networked PCs are equally able to act as a network server or client, and each client computer can talk to all the other wireless computers without having to go through an access point or hub. However, since there is no central base station to monitor traffic or provide Internet access, the various signals can collide with each other, reducing overall performance.

PHY (Physical Layer). The lowest layer within the OSI Network Model. It deals primarily with transmission of the raw bit stream over the PHYsical transport medium. In the case of wireless LANs, the transport medium is free space. The PHY defines parameters such as data rates, modulation method, signaling parameters, transmitter/receiver synchronization, etc. Within an actual radio implementation, the PHY corresponds to the radio front end and baseband signal processing sections.

Proxy server. Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.

Range. How far will your wireless network stretch? Most Wi-Fi systems will provide a range of a hundred feet or more. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to mile.

Residential gateway. A wireless device that connects multiple PCs, peripherals and the Internet on a home network. Most Wi-Fi residential gateways provide DHCP and NAT as well.

RJ-45. Standard connectors used in Ethernet networks. Even though they look very similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Roaming. Moving seamlessly from one AP coverage area to another with no loss in connectivity.

Router. A device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another. Based on routing tables and routing protocols, routers can read the network address in each transmitted frame and make a decision on how to send it via the most efficient route based on traffic load, line costs, speed, bad connections, etc.

Server. A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.

SSID (Service Set Identifier). A 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. (Also called ESSID.) The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific

WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet, it does not supply any security to the network. An SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.

SSL (Secure Sockets Layer). Commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session.

Subnetwork or Subnet. Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

Switch. A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a networks traffic cop: rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.

TCP (Transmission Control Protocol). A protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP

takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet. For example, when a web page is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as a single file.

TCP/IP (Transmission Control Protocol/Internet Protocol). The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.

UPnP. A networking architecture that provides compatibility among networking equipment, software and peripherals of the 400+ vendors that are part of the Universal Plug and Play Forum. UPnP works with wired or wireless networks and can be supported on

any operating system. UPnP boasts device-driver independence and zero-configuration networking.

USB (Universal Serial Bus). A high-speed bidirectional serial connection between a PC and a peripheral that transmits data at the rate of 12 megabits per second. The new USB 2.0 specification provides a data rate of up to 480 Mbps, compared to standard USB at only 12 Mbps. 1394, FireWire and iLink all provide a bandwidth of up to 400 Mbps.

VoIP (VoiceOver Internet Protocol). Voice transmission using Internet Protocol to create digital packets distributed over the Internet. VoIP can be less expensive than voice transmission using standard analog packets over POTS (Plain Old Telephone Service).

VPN (Virtual Private Network). A type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

WAN (Wireless Area Network). A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone

networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks (WLANs).

WEP (Wired Equivalent Privacy). Basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.

Wi-Fi (Wireless Fidelity). An inter-operability certification for wireless local area network (LAN) products based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard.

WLAN (Wireless Local Area Network). Also referred to as LAN. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

WPA-Enterprise (Wi-Fi Protected Access™ – Enterprise). It is Wi-Fi's encryption method that protects unauthorized network access by verifying network users through a server.

WPA-Personal (Wi-Fi Protected Access™ – Personal). It is Wi-Fi's encryption method that protects unauthorized network access by using a set-up password.

Troubleshooting

Basic Functions

1 If you are using a cable or DSL modem and are experiencing problems connecting to the Internet, do the following:

- Power off your cable or DSL modem, PC, and the router.
- Power on your modem and wait a few minutes until the modem has established a connection with your ISP.
- Power on the router.
- Power on your PC and attempt to connect to the Internet. For most users, the router's default values should be satisfactory. Some users may need to enter additional information in order to connect to the Internet through their ISP or broadband (cable or DSL) carrier. For example, some cable providers require a specific MAC address for connection to the Internet. To learn more about this, click the Advanced tab and then the MAC Address Clone tab.

2 My Wireless Access Point Router will not turn on. No LED's light up.

- The power is not connected.
- Connect the power adapter to your AP and plug it into the power outlet.

IMPORTANT! Only use the power adapter that came with your AP. Using any other adapter may damage your AP Router.

3 LAN Connection Problems I can't access my router.

- Make sure your router is powered on.
- There is no network connection.
- The computer you are using does not have a compatible IP Address. Be sure that the IP Address used on your computer is set to the same subnet as the router. For example, if the router is set to 192.168.1.1, change the IP address of your computer to 192.168.1.15 or another unique IP Address that corresponds to the 192.168.1.X subnet.
- Press the Reset button located on the rear of the router to revert to the default settings.

4 I can't connect to other computers on my LAN.

- The IP Addresses of the computers are not set correctly. Make sure that each computer has a unique IP Address. If using DHCP through the AP Router, make sure that each computer is enable DHCP function and restart the computer.
- Network cables are not connected properly. Make sure that the Link LED is on. If it is not, try a different network cable.
- Windows network settings are not set correctly. Check each computer for correct network settings.

Wireless Troubleshooting

1 I can't access the Wireless AP Router from a wireless network card.

- Out of range. Make sure that your computer is within range and free from any strong electrical devices that may cause interference.
- IP Address is not set correctly. Make sure that the Mode, SSID, Channel and encryption settings are set the same on each wireless adapter.
- Check your IP Address to make sure that it is compatible with the Wireless AP Router.

2 What if I forgot my password.

x
x
x
x
x
TBD

3 *What picture formats can I show with my ViewSonic Wireless Media Gateway?*

- .JPG, GIF, TIF, and BMP

Compliances

FCC Interference Statement

FCC (Federal Communication Commission) Interference Statement

Class B Regulations

USA

This equipment complies with the limits for a class B digital device as specified in Part 15 of FCC Rules which provide reasonable protection against harmful interference in a residential area. This equipment generates and uses radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. In the unlikely event that there is interference to radio or television reception (which can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorienting or relocating the receiving antenna (radio or television).

- Relocating the equipment with respect to the receiver.
- Consult your dealer or an experienced radio/television technician.
- Any changes or modifications to the equipment not expressly approved by the manufacturer could void the user's authority to operate this equipment.
- Use of a shielded interface cable is required to comply with the Class B limits of Part 15 of FCC rules.

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Canada

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Canada (IC):

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le ministère des Communications.



This product is in compliance with the standards that the Wi-Fi Alliance has certified.

Cleaning & Maintenance

- To clean the Wireless Media Gateway, make sure the Wireless Media Gateway is turned off.
- Clean the Wireless Media Gateway in a well-vented room. Allow enough room for air to circulate through the air holes on the Wireless Media Gateway. Do not pile or stack things on top of or around the unit to prevent air from circulating. This increases the chance of over-heating.
- Never spray or pour any liquid directly onto the Wireless Media Gateway. Do not immerse in water or any liquid.
- Wipe the Wireless Media Gateway with a clean, soft, lint-free cloth to remove dust and other particles. Dust often.
- If still not clean, apply a small amount of non-ammonia, non-alcohol based glass cleaner onto a clean, soft, lint-free cloth, and wipe the screen.
- Do not attempt to use the Wireless Media Gateway in a metal closet that prevents the antenna from sending and receiving signals.

Customer Support

Before contacting ViewSonic Customer Support, check the **Troubleshooting** section for possible solutions to any setup problems you have. For Customer Support or product service, you will need to provide the product serial number.

Country/Region	Website	T = Telephone F = FAX
United States	www.viewsonic.com/support	T: (800) 688-6688 F: (909) 468-1202
Canada	www.viewsonic.com/support	T: (866) 463-4775 F: (909) 468-1202

Limited Warranty

Wireless Router Products

What the warranty covers:

ViewSonic® warrants its Wireless Router products to be free from defects in material and workmanship during the warranty period. If a ViewSonic Wireless Router product proves to be defective in material or workmanship during the warranty period, ViewSonic will, at its sole option, repair or replace the product with a like product. Replacement product or parts may include remanufactured or refurbished parts or components.

VIEWSONIC AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

ANY SOFTWARE THAT MAY BE INCLUDED WITH THIS PRODUCT IS PROVIDED FREE OF CHARGE AND ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION ANY WARRANTIES THAT IT IS FREE OF DEFECTS, MERCHANTABILITY, FIT FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR COMPATIBLE WITH ANY OTHER SOFTWARE. FOR YOUR SPECIFIC RIGHTS AND DUTIES, PLEASE SEE THE END-USER LICENSE AGREEMENT (EULA) CONTAINED WITHIN THE SOFTWARE FOR YOUR PRODUCT.

How long the warranty is effective:

ViewSonic Wireless Router products are warranted for one (1) year for all parts and one (1) year for all labor from the date of the first consumer purchase.

Who the warranty protects:

This warranty is valid only for the first consumer purchaser.

What the warranty does not cover:

1. Software
2. Any product on which the serial number has been defaced, modified or removed.
3. Damage, deterioration or malfunction resulting from:
 - a. Accident, misuse, neglect, fire, water, lightning, or other acts of nature, unauthorized product modification, or failure to follow instructions supplied with the product.
 - b. Repair or attempted repair by anyone not authorized by ViewSonic.
 - c. Damage to or loss of any programs, data or removable storage media.
 - d. Software or data loss occurring during repair or replacement.
 - e. Any damage of the product due to shipment.
 - f. Removal or installation of the product.
 - g. Causes external to the product, such as electrical power fluctuations or failure.
 - h. Use of supplies or parts not meeting ViewSonic's specifications.
 - i. Normal wear and tear.
 - j. Any other cause which does not relate to a product defect.
4. Removal, installation, and set-up service charges.

(Page 1 of 2)

How to get service:

1. For information about receiving service under warranty, contact ViewSonic Customer Support. You will need to provide your product's serial number.
2. To obtain service under warranty, you will be required to provide (a) the original dated sales slip, (b) your name, (c) your address, (d) a description of the problem, and (e) the serial number of the product.
3. Take or ship the product freight prepaid in the original container to an authorized ViewSonic service center or ViewSonic.
4. For additional information or the name of the nearest ViewSonic service center, contact ViewSonic.

Limitation of implied warranties:

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, WHICH EXTEND BEYOND THE DESCRIPTION CONTAINED HEREIN INCLUDING THE IMPLIED WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Exclusion of damages:

VIEWSONIC'S LIABILITY IS LIMITED TO THE COST OF REPAIR OR REPLACEMENT OF THE PRODUCT. VIEWSONIC SHALL NOT BE LIABLE FOR:

1. DAMAGE TO OTHER PROPERTY CAUSED BY ANY DEFECTS IN THE PRODUCT, DAMAGES BASED UPON INCONVENIENCE, LOSS OF USE OF THE PRODUCT, LOSS OF DATA, LOSS OF TIME, LOSS OF PROFITS, LOSS OF BUSINESS OPPORTUNITY, LOSS OF GOODWILL, INTERFERENCE WITH BUSINESS RELATIONSHIPS, OR OTHER COMMERCIAL LOSS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
2. ANY OTHER DAMAGES, WHETHER INCIDENTAL, CONSEQUENTIAL OR OTHERWISE.
3. ANY CLAIM AGAINST THE CUSTOMER BY ANY OTHER PARTY.

Effect of state law:

This warranty gives you specific legal rights, and you may also have other rights which vary from state to state. Some states do not allow limitations on implied warranties and/or do not allow the exclusion of incidental or consequential damages, so the above limitations and exclusions may not apply to you.

ViewSonic Wireless Router Products Warranty (V1.0)

Release Date: June 3, 2004

(Page 2 of 2)