

ViewSonic®

WAPBR-100 802.11g 3-in-1 Access Point

- User Guide



Table of Contents

Product Registration.....	1
Regulatory Information.....	2
Chapter 1: Getting Started.....	4
Overview.....	4
Package Contents.....	6
Safety Notice.....	7
Chapter 2: Installation.....	8
Front of Access point.....	8
Back of Access point.....	8
Chapter 3: Setting up the Access Point.....	9
Step 1. Connect the Access point.....	10
Step 2. Configure your PC.....	11
For Windows® 2000 or XP.....	11
For Windows® 98 or Me.....	14
Chapter 4: Web Management Settings.....	16
Start Up & Login.....	16
4.1. Primary Setup.....	17
4.2. System.....	22
4.3. Operating Mode.....	23
4.4. Status.....	24
4.5. Traffic Log.....	25
4.6. Access Control.....	26
4.7. Advanced Wireless.....	27
4.8. SNMP INFO.....	29
4.9. Firmware Upgrade.....	30
Appendix.....	32
Specifications.....	33
Wireless Security & Glossary.....	34
Troubleshooting.....	46
Customer Support.....	48
Limited Warranty.....	49

Copyright© ViewSonic Corporation, 2004. All rights reserved.

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

Microsoft and Windows 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

Product Name:	ViewSonic 802.11g 3-in-1 Access Point WAPBR-100
Model Number:	VS10408
Document Number:	A-CD-WAPBR-100-1-UG
Serial Number:	_____
Purchase Date:	_____

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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.

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.

ViewSonic declares that Wireless 802.11g Access Point (FCC ID: GSS-VS10407) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

Canada (Industry Canada)

The device is certified to the requirements of RSS-210 for 2.4 GHz spread spectrum devices.

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.

Health Canada's address is: 775 Brook field Road, Ottawa, Ontario Canada K1A 1C1; Tel: (613) 954-6699 / Fax: (613) 941-1734; e-mail: alice_mackinnon@hc-sc.gc.ca

Chapter 1: Getting Started

This chapter provides an Overview of the ViewSonic WAPBR-100 Wireless 3-in-1 Access point, Package Contents, and Safety Notice.

Overview

Congratulations on purchasing the **ViewSonic 802.11g 3-in-1 Access point!**

The WAPBR-100 is capable of operating in one of 4 different modes to meet your wireless networking needs. The WAPBR-100 can operate as an Access Point mode; Bridging mode; Repeater mode; Wireless Client mode.

Finally, networking made easy

Networking your home or small business is easy with ViewSonic's WAPBR-100 3-in-1 Access point. The WAPBR-100 functions as the CENTRAL Access point IN YOUR HOME OR OFFICE NETWORK, allowing you to share your broadband, files and printers with any PC in your office or home. The WAPBR-100 boasts a stylish, compact design that offers high performance wireless 802.11g, 802.11b and wired Ethernet connectivity. The WAPBR-100 3-in-1 Access Point 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 WAPBR-100 AP and share a single high-speed broadband connection, files, printers and other peripherals among all your computers.
- **Robust security keeps your data secure**
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.
- **Supports 125 High Speed Mode™ ***



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.

The **WAPBR-100 3 in 1 Access Point** performs at 125 High Speed Mode only with wireless adapters that support this protocol, such as the **ViewSonic WPCC100 Wireless PC Card**. If your wireless adapter does not support this protocol, however, the **WAPBR-100 3-in-1 Access Point** will still work at standard 802.11g speed.

When operating at highest speeds, the **WAPBR-100 3-in-1 Access Point** achieves a 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 such as the **ViewSonic WPCC100 PC Card Adapter**.

- **Easy set up**

User-friendly set up wizard on the Network Companion CD makes installation a snap. Using the AP 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 802.11g 3-in-1 Access Point**.

Package Contents

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

- ViewSonic 802.11g WAPBR-100 3-in-1 Access Point
- Quick Start Guide
- Network Companion CD
- Power Adapter-DC 12V, 500mA
- Cradle
- Ethernet Cable



WAPBR-100
3-in-1 Access Point



Quick Start Guide



Network
Companion CD



AC Power Adapter



Cradle



Ethernet Cable

If any of the above items are missing, please contact your reseller.

Note: Using a power supply with a different voltage rating than the one included with the WAPBR-100 will cause damage and void the warranty for this product.

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

Safety Notice

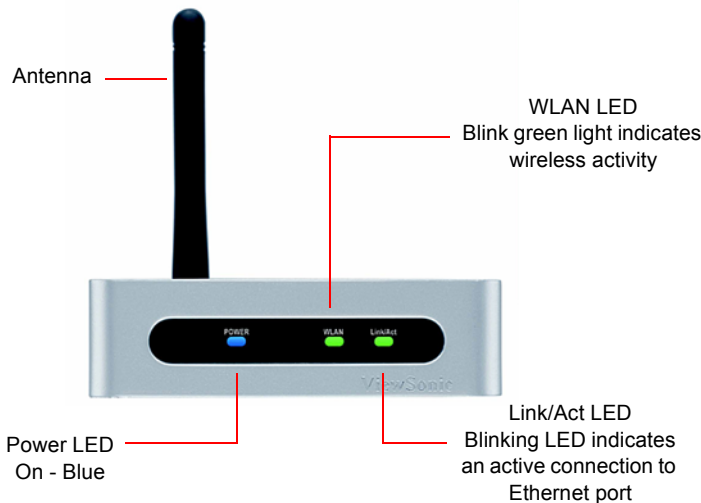
To ensure safe operation, following these simply rules:

- 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.

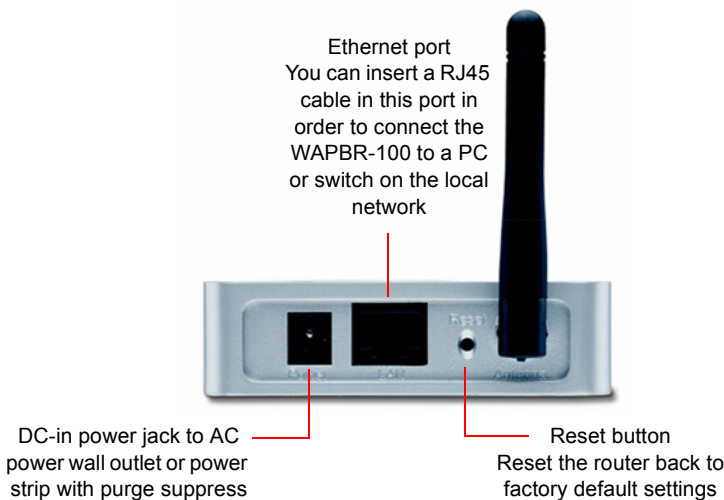
Chapter 2: Installation

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

Front of Access point



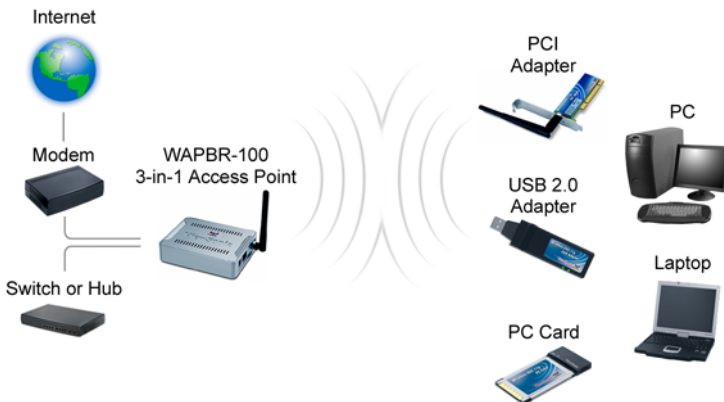
Back of Access point



Chapter 3: Setting up the Access Point

This guide shows how to set up the ViewSonic 3-in-1 Access Point to work with multiple devices in three steps:

1. Connect the Access Point.
2. Configure your PC.
3. Configure the Access Point. A typical setup may look like the following:

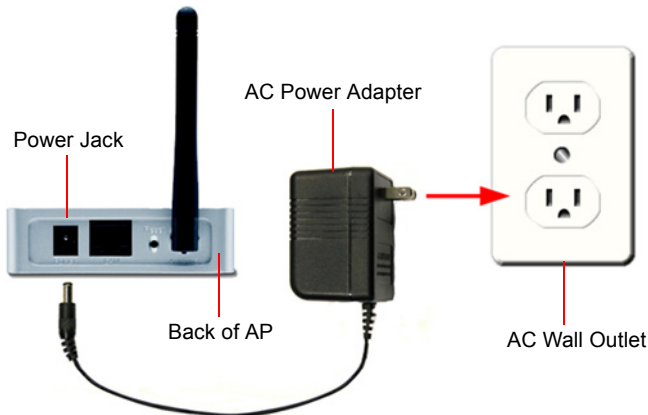


Step 1. Connect the Access point.

1. Make sure you have all the setup information from your Internet Service Provider (ISP).
2. Make sure that all network hardware is turned off, including the Router, computer(s), and cable or DSL modem.
3. Connect a standard Ethernet network cable to the Access Point. Connect the other end of the Ethernet cable to a Switch or Router. The Access Point will then be connected to your 10/100 Network.



4. Connect the AC power adapter from the power jack on the back of the Access Point to an AC wall outlet as shown or to a power strip with surge protection. The power LED on the front of the AP turns blue when there is power.

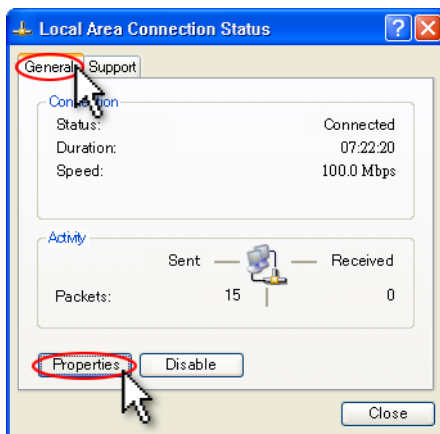


Step 2. Configure your PC

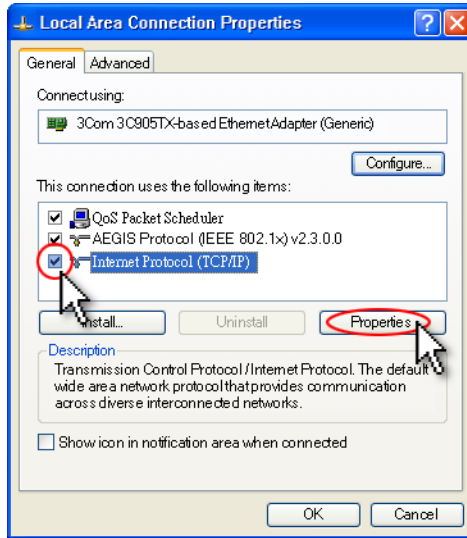
Make sure that your computer is set to Static IP as follows:

For Windows® 2000 or XP

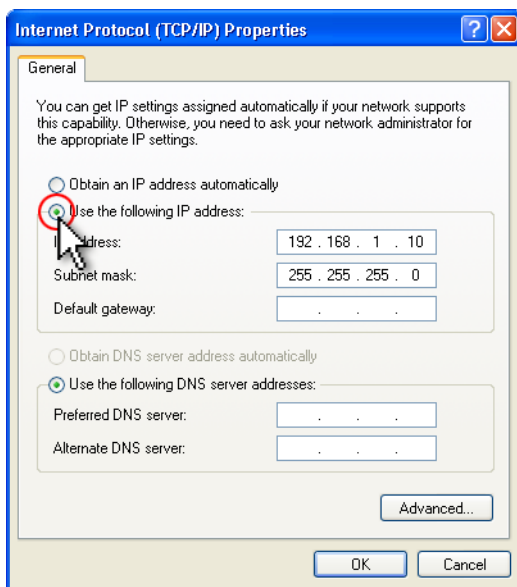
1. Click the **Windows® Start** button > **Control Panel** > **Network and Internet Connections** > **Local Area Connection**. The **Local Area Connection Status** screen appears as shown on the right.
2. From the **General** tab (usually appears selected by default), click **Properties**. The **Local Area Connection Properties** screen appears in the next step.



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 as shown in the next step.

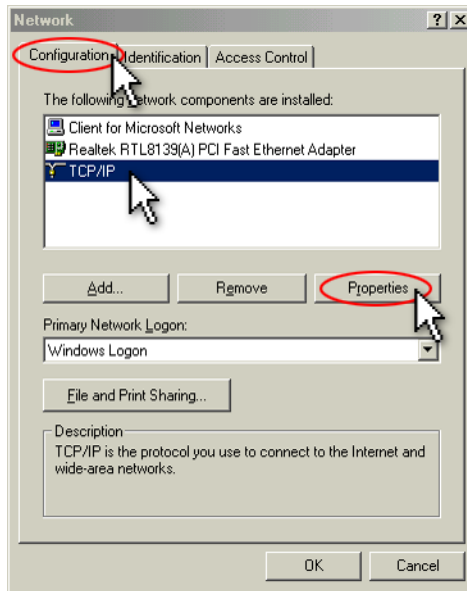


4. Select **Use the follow IP address** and set IP address as **192.168.1.X**
Subnet mask:**255.255.255.0** Click **OK** > **OK** > Close to complete the PC configuration.

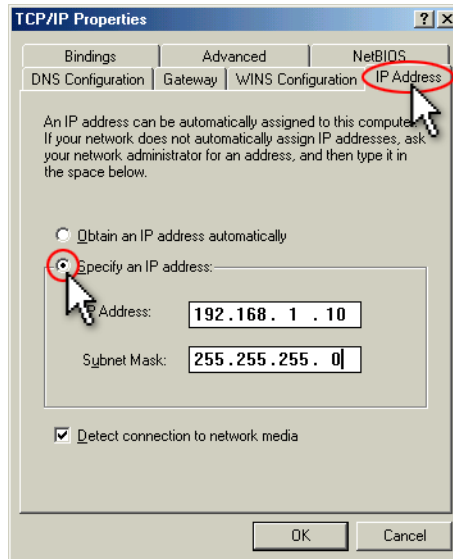


For Windows® 98 or Me

1. Click the **Windows® Start** button > Select **Settings** > Click **Control Panel** > double-click on **Network**. The **Network** screen appears as shown on the right.
2. Select the Configuration tab if it is not already selected by default. In the list of installed network components, click the TCP/IP line for the applicable Ethernet adapter. Click **Properties**. The **TCP/IP Properties** screen appears as shown in the next step.



3. From the **TCP/IP Properties** screen, select the **IP Address** tab.
4. Select **Specify an IP address and set IP address as 192.168.1.X subnet mask:255.255.255.0** and Click **OK > OK**.

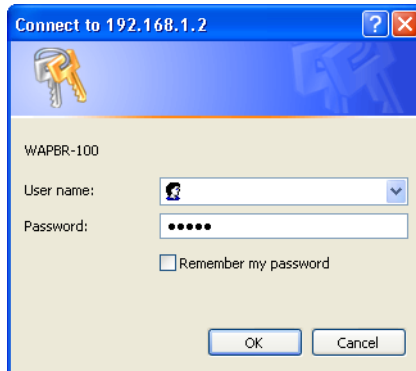
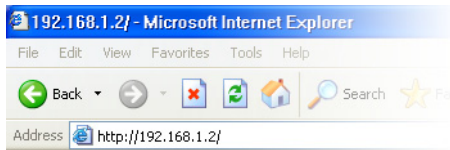


5. Windows may ask you for the original Windows installation disk or additional files. Look for those files on **C:\windows\options\cabs** or insert your Windows CD-ROM into your CD-ROM drive and check the correct file location: for example if your CD-ROM is D, go to D:\win98, or D:\win9x.
6. Restart your PC if prompted.

Chapter 4: Web Management Settings

Start Up & Login

Open Microsoft Internet Explorer (IE) web browser. In the address field, enter **http://192.168.1.2** and press **Enter**. A logon window appears like the one shown on the next page.



User name: leave it blank.

Password: Enter the default password "**admin**" in all lowercase letters.

Later on, we recommend you change the default to your own password for added security.

Click **OK**.

The **Primary Setup** screen appears as shown in the next step.

4.1. Primary Setup

Make Correct Network Settings Of Your Computer.

To change the configuration, use Microsoft Internet Explorer (IE) Communicator to connect the WEB management **192.168.1.2**

Primary Setup:

This screen contains all of the AP's basic setup functions.

The screenshot shows the 'Primary Setup' web interface for a ViewSonic device. The interface has a blue header with the ViewSonic logo and navigation tabs: Primary, System, Operating Mode, Status, Traffic Log, and Advanced Setting. The 'Primary Setup' tab is selected. Below the header, there is a section titled 'Primary Setup' with a description: '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.' The 'AP Name' field is set to 'WAPBR-100'. Below this, there is a 'LAN' section with a 'MAC Address' of '00:90:4c:60:04:00'. The 'Configuration type' is set to 'Static IP Address'. The 'IP Address' is '192.168.1.2', the 'Subnet Mask' is '255.255.255.0', and the 'Gateway' is '192.168.1.1'. Below the LAN section, there is a 'Wireless' section with a 'MAC Address' of '00:90:4C:60:04:00'. The 'Mode' is set to '11b+g', the 'SSID' is 'viewsonic', the 'Channel' is '6', and the 'Domain' is 'USA'. The 'Security' is set to 'Disable'. The 'SSID Broadcast' is set to 'Enable'. There is a 'Configure Security' button. At the bottom, the 'Firmware Version' is 'v1.0.05, Aug 23, 2004'. There are 'Apply', 'Cancel', and 'Help' buttons at the bottom.

ViewSonic

Primary System Operating Mode Status Traffic Log 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.**

AP Name: WAPBR-100

LAN MAC Address: 00:90:4c:60:04:00

Configuration type: Static IP Address

IP Address: 192 . 168 . 1 . 2 This is the IP Address, Subnet Mask and

Subnet Mask: 255 . 255 . 255 . 0 Default Gateway of the Access Point as it is

Gateway: 192 . 168 . 1 . 1 seen by your local network.

Wireless MAC Address: 00:90:4C:60:04:00

Mode: 11b+g

SSID: viewsonic SSID Broadcast: Enable

Channel: 6

Domain: USA

Security: ☐ Enable ☒ Disable [Configure Security](#)

Firmware Version: v1.0.05, Aug 23, 2004

[Apply](#) [Cancel](#) [Help](#)

Most users will be able to configure the AP and get it working properly using the settings on this screen.

LAN IP Address and Subnet Mask:

This is the AP's IP Address and Subnet Mask as seen on the internal LAN. The default value is 192.168.1.2 for IP Address and 255.255.255.0 for Subnet Mask.

LAN MAC Address: 00:90:4c:60:04:00

Configuration type:

IP Address: 192 . 168 . 1 . 2 This is the IP Address, Subnet Mask and

Subnet Mask: 255 . 255 . 255 . 0 Default Gateway of the Access Point as it is

Gateway: 192 . 168 . 1 . 1 seen by your local network.

Wireless:

This section provide the Wireless Network settings for your WLAN Wireless Settings.

Wireless MAC Address: 00:90:4C:60:04:00

Mode:

SSID: SSID Broadcast:

Channel:

Domain: USA

Security: ☐ Enable ☒ Disable

Firmware Version: v1.0.05, Aug 23, 2004

- **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 APs that will be communicating with mobile wireless stations.
- **Channel:** Select the appropriate channel from the list provided to correspond with your network settings. You shall assign a different channel for each AP to avoid signal interference.

- **Security:** There are 3 types of security to be selected. To secure your Wireless Networks, it is strongly recommended to 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."

Security

The Access Point supports 3 different types of security settings. There are: WPA Pre-Shared Key, WPA RADIUS and WEP. Please see the help tab for more details on the different types of security settings.

Security Mode: WEP

Default Transmit Key: 1 2 3 4

WEP Encryption: 64 bits 10 hex digits

Passphrase: Generate

Key 1:

Key 2:

Key 3:

Key 4:

Apply Cancel Help

Important Notice

In order to make right use of WPA, please ensure that your current Wireless Adapter's driver, and Wireless Utility can support it, 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. The rest of the OS must installed 3er party's client software such as Funk ODySSey. User's Guide 9.

WPA-Pre-shared key:

There are two encryption options for WPA Pre-Shared Key, TKIP and AES. TKIP stands for Temporal Key Integrity Protocol. TKIP utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. AES stands for Advanced Encryption System, which utilizes 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 Algorithms	Please choose your algorithms method. You can select between TKIP or AES.
WPA Shared Key	Please input the Pre-Shared Key. The key should be 8 characters or 63 characters in alphanumeric.
Group Key Renewal	Please input the period of renewal time. The default selection is 300 seconds.

Security

The Access Point supports 3 different types of security settings. There are: WPA Pre-Shared Key, WPA RADIUS and WEP. Please see the help tab for more details on the different types of security settings.

Security Mode: WPA Pre-Shared Key ▾

WPA Algorithms: TKIP ▾

WPA Shared Key:

Group Key Renewal: 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.

Security

The Access Point supports 3 different types of security settings. There are: WPA Pre-Shared Key, WPA RADIUS and WEP. Please see the help tab for more details on the different types of security 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	Please choose your algorithms method. You can select between TKIP or AES.
Radius Server Address	Please input your RADIUS Server IP address.
Radius Server Port	Please input the Authentication port of your RADIUS server. The default port being used is 1812
Radius Shared Key	The RADIUS server will accept the authentication if both Shared Key matched.
Group Key Renewal	Please input the period of renewal time. The default selection is 300 seconds.

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

4.2. System

The screenshot shows the 'System' configuration page of a ViewSonic 3-in-1 Access Point. The page has a blue header with the ViewSonic logo and navigation tabs: Primary, System (selected), Operating Mode, Status, Traffic Log, and Advanced Setting. The main content area is light blue and contains the following sections:

- System:** A text block stating: "It is strongly recommended to change the default password for you Access Point in order to avoid any security risks. In this section you can also Restore and Backup the Setting to a Profile."
- AP Password:** Two password input fields, each with a label "(Re-enter to Confirm)".
- Restore Factory Defaults:** Radio buttons for YES and NO (selected). Below them is a note: "Note: If YES, all setting will be restored as factory default setting."
- Backup/Restore Setting:** Two buttons: "Backup Setting" and "Restore Setting". Below them is a note: "Note: Click on 'Backup Setting' to create and save the setting on your local hard drive. Click on 'Restore Setting' to load the setting profile from your hard drive."
- Firmware Upgrade:** A section showing "Current Version: v1.0.05, Aug 23, 2004" and a "Firmware Upgrade" button.

At the bottom of the page are three buttons: "Apply", "Cancel", and "Help".

- **AP Password:** Changing the password for the AP is as easy as typing the password into the **Enter New Password** field. Then, type it again into the Re-enter to confirm.
- Click the **Apply** button to save the setting.
- Use the default password when you first open the configuration pages, after you have configured these settings, you should set a new password for the AP (using the Password screen). This will increase security, protecting the AP from unauthorized changes.
- **Restore Factory Defaults:** Click the Yes button to reset all configuration settings to factory default values. Note: 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.
- **Backup/Restore Setting:** Click Backup to store the Access Point's configuration on your local PC. Click Restore to restore Access Point's configuration from your local PC. Check all the settings and click Apply to save them.

4.3. Operating Mode



Primary

System

Operating Mode

Status

Traffic Log

Advanced Setting

Operating Mode

Please assign the operating mode to the device. You can select between "AP", "AP Client", "AP Repeater" or "Wireless Bridge" mode. The default operating mode of the device is "AP". For further understanding on Operating Mode selection, please refer to the User Guide.

LAN MAC Address: 00:90:4c:60:04:00

☒ **Access Point (Default Selection)**

☐ **AP Client**

Please input the MAC Address of the remote AP:

☐ **AP Repeater**

Please input the MAC Address of the remote AP:

☒ **Enable LAN port**

Note: Please leave the option "Enable LAN port" selected. This will allow your wired PC to join the remote AP's network. In other case, you will only be able to configure the unit through Wireless Interface.

☐ **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.

- **Access Point:** This mode provides access for wireless stations to wired LANs and from wired LANs to wireless stations.
- **AP Client:** AP Client or Wireless Client mode allows the WAPBR-100 to become a wireless client to another AP. In essence the AP has now become a wireless adapter card. You would use this mode to allow an AP to communicate with another AP. Wireless cards will not communicate with access points in AP Client / Wireless Client mode.
- **AP Repeater:** This mode allows the AP to keep the AP function role and at the same time performing a communication with other 802.11g AP to establish and extend your Wireless Network cover. Please enter the Remote Access Point's MAC address to enable this feature.
- **Wireless Bridge:** This mode allows the connection of one or more remote LANs with a central LAN.
- Click **Apply** to save your settings.

4.4. Status



[Primary](#) [System](#) [Operating Mode](#) [Status](#) [Traffic Log](#) [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.

AP Name: WAPBR-100

Firmware Version: v1.0.05, Aug 23, 2004

Wireless client connected status

Refresh

LAN

MAC Address: 00:90:4c:60:04:00

Configuration Type:	Static IP Address
IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0

Wireless

MAC Address: 00:90:4C:60:04:00

SSID:	viewsonic
Mode:	11b+g
Channel:	6
Security:	Disable
Send	Good Packets: 47
	Dropped Packets: 0
Received	Good Packets: 0
	Dropped Packets: 0

Note: In wireless transmission, some dropped packets occurrence is normal.

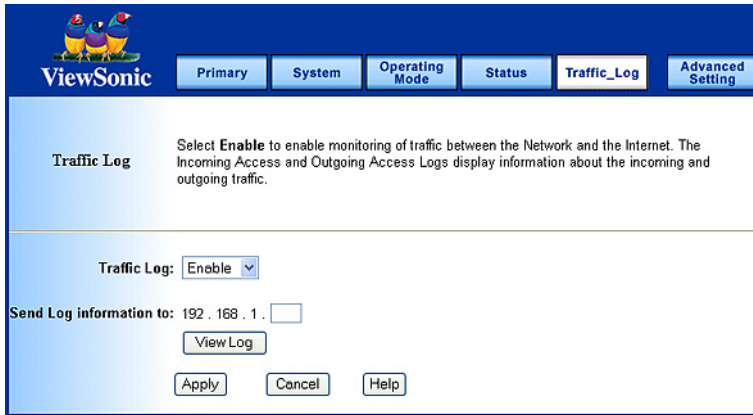
Refresh Help

This screen displays the IEEE 802.11g AP's current status and settings. This information is read-only.

This page will auto re-flash every 5 seconds to keep most update information.

- **LAN:** Displays all information related on AP, such as the IP address and the current configuration type.
- **Wireless:** Displays information related on the Wireless interface, such as SSID, Channel, Encryption and statistics of network traffic.
- Click the **Refresh** button to refresh the AP's status and settings.

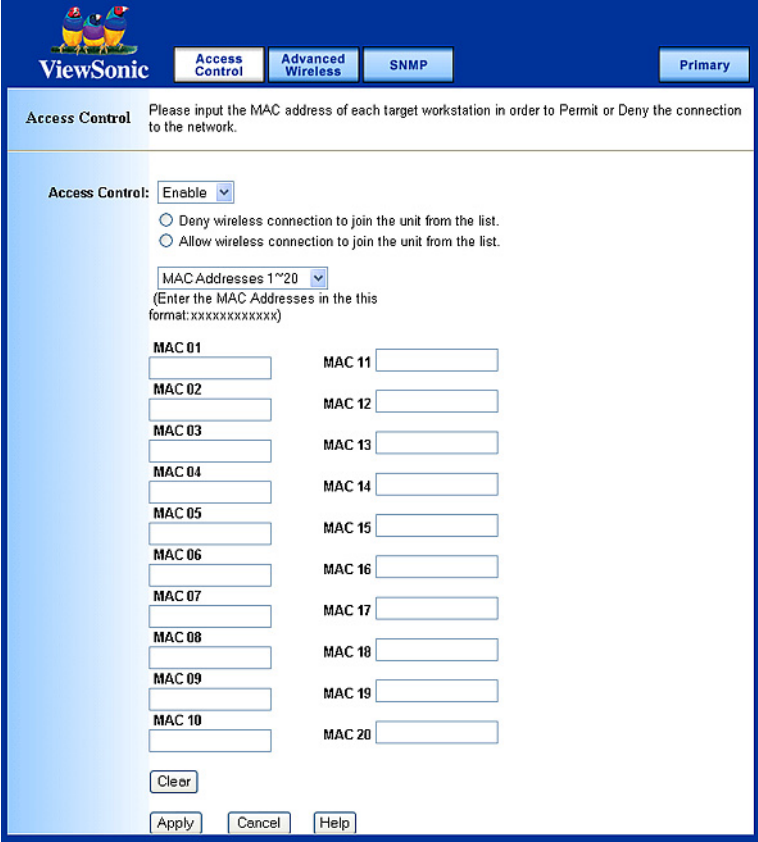
4.5. Traffic Log



The screenshot shows the ViewSonic web interface with a blue header. The header contains the ViewSonic logo and a navigation bar with buttons: Primary, System, Operating Mode, Status, Traffic_Log (highlighted), and Advanced Setting. Below the header, the page is titled "Traffic Log". A text block explains: "Select **Enable** to enable monitoring of traffic between the Network and the Internet. The Incoming Access and Outgoing Access Logs display information about the incoming and outgoing traffic." Below this, there is a "Traffic Log:" label followed by a dropdown menu set to "Enable". Underneath, the "Send Log information to:" field is followed by the IP address "192 . 168 . 1 ." and a small empty input box. A "View Log" button is positioned below the IP address. At the bottom of the form are three buttons: "Apply", "Cancel", and "Help".

- **Traffic Log:** The AP can keep logs of all incoming or outgoing traffic for your network traffic. 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 AP will send updated logs to that PC.
- To see a temporary log of the AP's most recent traffic, click the **View Log** button.
- Click the **Apply** button to save the setting.

4.6. Access Control



The image shows the 'Access Control' configuration page of a ViewSonic device. At the top, there is a navigation bar with the ViewSonic logo and three tabs: 'Access Control' (selected), 'Advanced Wireless', and 'SNMP'. A 'Primary' button is also present. Below the navigation bar, the 'Access Control' section is active. It contains a text box with the instruction: 'Please input the MAC address of each target workstation in order to Permit or Deny the connection to the network.' Below this, there is a section for 'Access Control' with a dropdown menu set to 'Enable'. Two radio buttons are available: 'Deny wireless connection to join the unit from the list.' and 'Allow wireless connection to join the unit from the list.' Below the radio buttons, there is a dropdown menu for 'MACAddresses 1~20' and a text box for entering MAC addresses in the format 'xxxxxxxxxxxx'. Below this, there is a table with 20 rows, each containing a label (MAC 01 to MAC 20) and an input field. At the bottom, there are three buttons: 'Clear', 'Apply', and 'Help'.

ViewSonic

Access Control **Advanced Wireless** **SNMP** **Primary**

Access Control Please input the MAC address of each target workstation in order to Permit or Deny the connection to the network.

Access Control: **Enable**

☐ Deny wireless connection to join the unit from the list.
☐ Allow wireless connection to join the unit from the list.

MACAddresses 1~20

(Enter the MAC Addresses in the this format:xxxxxxxxxxxx)

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

- **Access Control:** This function will allow administrator to have access control by enter MAC address of client stations. When **Enable** this function, two new options will show up. Depend on the filtering propose, it can be selected to **Deny** or **Allow**.
- Fill the client stations MAC list to complete the configuration. The table could store up to **40** different MAC addresses. Please follow the format that it required when an address is input.
- Click **Apply** to save your settings.

4.7. Advanced Wireless



Access Control **Advanced Wireless** SNMP Primary

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

Authentication Type: (Default: Auto)

Transmission Rates: (Default: Auto)

RTS/CTS: (Default: Disable)

Antenna Selection: (Default: Diversity)

Beacon Interval: (Default: 100, Milliseconds, Range: 20-1000)

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

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

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

Xpress mode: (Default: Enable)

- **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 AP automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the AP and a wireless client. The default setting is **AUTO**.
- **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 AP 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 AP 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.
- **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.
- Click **Apply** to save your settings.

4.8. SNMP INFO



Access Control

Advanced Wireless

SNMP

Primary

SNMP INFO

Based on Simple Network Management Protocol, you can quickly control and monitor any network device. Please fill out the correspond information on this page to start the monitoring.

SNMP V1/V2c:

Enable

Information: Contact:

Unit Name and description:

Physical Location:

SNMP Community:

public

private

Read-Only

Read-Only

Apply

Cancel

Help

The SNMP screen allows you to customize the Simple Network Management Protocol (SNMP) settings. SNMP is a popular network monitoring and management protocol.

SNMPv2c		To enable the SNMP support feature, select Enable. Otherwise, select Disable.
Identification	Contact	In the contact field, enter contact information for the AP.
	Unit Name and description	In the Unit Name and description field, enter the name of the AP or AP description.
	Physical Location	In the Physical Location field, specify the area or location where the AP resides.
SNMP Community	Public	You may change the SNMP Community's name from its default, public. Then configure the community's access as either Read-Only or read-Write.
	Private	You may change the SNMP Community's name from its default, public. Then configure the community's access as either Read-Only or read-Write.

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

4.9. Firmware Upgrade

The screenshot shows the ViewSonic web interface with a blue header. The 'System' tab is selected among 'Primary', 'System', 'Operating Mode', 'Status', 'Traffic Log', and 'Advanced Setting'. The 'System' section contains a warning about changing the default password, fields for 'AP Password' (with 'Re-enter to Confirm' text), a 'Restore Factory Defaults' section with 'YES' and 'NO' radio buttons (where 'NO' is selected), and a 'Backup/Restore Setting' section with 'Backup Setting' and 'Restore Setting' buttons. A note explains the backup/restore process. At the bottom, the 'Firmware Upgrade' section shows the 'Current Version: v1.0.05, Aug 23, 2004' and a 'Firmware Upgrade' button. 'Apply', 'Cancel', and 'Help' buttons are at the very bottom.

To perform the firmware upgrade action, please go to the System section.

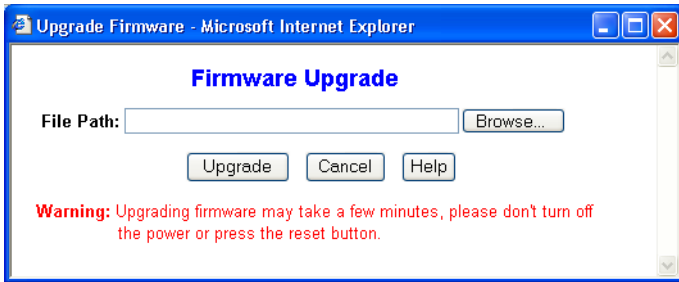
Firmware Upgrade: Click the Firmware Upgrade button to load new firmware onto the AP. If the AP is not experiencing difficulties, then there is no need to download a more recent firmware version, unless that version has a new feature that you want to use.

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

To upgrade the AP's firmware:

1. Download the firmware upgrade file from the internet.
2. Extract the firmware upgrade file.
3. Click the Firmware Upgrade button.

4. On the Firmware Upgrade screen, click the Browse button to find the firmware upgrade file.



5. Double-click the firmware upgrade file.
6. Click the Upgrade button, and follow the on-screen instructions.

Note: Do not power off the AP or press the Reset button while the firmware is being upgraded.

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, 1Mbps
Operating Channels	1-11 United States, Canada
Antenna	Single external antenna - Color is Black
Modulation	802.11g: OFDM; 802.11b: CCK (11 Mbps, 5.5 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps)
Channel Selection	802.11b US =11 Channel 801.11g US = 11 Channel
Output Power	Max. 100 mW (after antenna)
Coverage area	Indoor environment estimated at 30 - 50m. Receive sensitivity dependent upon user environment.
Main Board Memory	SDRAM:8 Mbytes Flash:2 Mbytes
Networking Interface	1 Ethernet port IEEE 802.11g (2.4Ghz-DSSS)
Ethernet Interface	IEEE 802.3 10-base T, IEEE 802.3u 100-base T
Power Source and Cord	An external linear power adapter (12V, 500mA) will be applied to North America area.
LED	The Device shall contain the following activity lights: • Power • Wireless LAN Link Status • Ethernet port Status
Dimension	Product:L:108mm x W:84.6mm x H:23.8mm Packaging:L:242mm x W:224mm x H:74mm
Weight	Net:0.26 lb(119 g) Gross:1.547 lb(700 g)
Wireless Security	64/128 bit WEP Encryption, WPA/WPA-PSK (Windows XP, SP1 and Windows 2000 SP4 only), and MAC address filtering
OS support needed	Microsoft Windows 2000 Microsoft Windows XP (Home and Pro)

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 subnet works 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. 8bits 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 operatively 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 "cross-over." 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 ACK knowledge 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 coffee shop, 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 Cool Spots.

Hub. A multipart 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 multi-gigabyte 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 (Internet work 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) sub layer.

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 base band 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.

Sub network 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 (Voice Over 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

My Wireless AP will not turn on. No LED's light up.

Cause:

- The power is not connected.

Resolution:

- Connect the power adapter to your AP and plug it into the power outlet.
Note: Only use the power adapter provided with your AP. Using any other adapter may damage your AP.

LAN Connection Problems I can't access my AP.

Cause:

- The unit is not powered on.
- There is not a network connection.
- The computer you are using does not have a compatible IP Address.

Resolution:

- Make sure your AP is powered on.
- Make sure that your computer has a compatible IP Address. Be sure that the IP Address used on your computer is set to the same subnet as the AP. For example, if the AP is set to 192.168.1.2, 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.
- Use the Reset button located on the rear of the AP to revert to the default settings.

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

Cause:

- The IP Addresses of the computers are not set correctly.
- Network cables are not connected properly.
- Windows network settings are not set correctly.

Resolution:

- Make sure that each computer has a unique IP Address. And the IP must be in the same subnet as the AP.
- Make sure that the Link LED is on. If it is not, try a different network cable.
- Check each computer for correct network settings.

Wireless Troubleshooting I can't access the Wireless AP from a wireless network card**Cause:**

- Out of range. IP Address is not set correctly.

Resolution:

- Make sure that the Mode, SSID, Channel and encryption settings are set the same on each wireless adapter.
- Make sure that your computer is within range and free from any strong electrical devices that may cause interference. Check your IP Address to make sure that it is compatible with the Wireless AP.

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 (with email address)	T = Telephone F = FAX
United States	service.us@viewsonic.com	T= (800) 688 6688 F= (909) 468 1202
Canada	service.us@viewsonic.com	T= (886) 463 4775 F= (909) 468 1202
United Kingdom	service.eu@viewsoniceurope.com	T= (0800) 833 648 F= +44 (0) 1293 643 910
Europe, Middle East, Baltic countries, and North Africa	service.eu@viewsoniceurope.com	(Contact your reseller)
Taiwan (VSTW)	www.viewsonic.com.tw/support/ service@tw.viewsonic.com	T= +886 (2) 2246 3456 F= +886 (2) 8242 3668 Toll Free: 0800 061 198
China (VSCN)	www.viewsonic.com.cn/service/ service_index.asp service.cn@cn.viewsonic.com	T= +86 (21) 6237 5252 F= +86 (21) 6237 5373 Toll Free= 800 820 3870
Australia and New Zealand	www.viewsonic.com.au/support/ service@au.viewsonic.com	+ 61 2 9906 6277
Singapore, Southeast Asia, and India	service@sg.viewsonic.com	+ 65 273 4018
Other Asia, Pacific countries, and Indian Peninsula	service.ap@viewsonic.com	+ 886 (2) 2246 3456

The websites shown above provide the most current email addresses for your Customer Support queries.

Limited Warranty

Wireless Access Point Product

What the warranty covers:

ViewSonic® warrants its Wireless Access Point products to be free from defects in material and Workmanship during the warranty period. If a ViewSonic Wireless Access Point 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 YOU'RE 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:
 - Accident, misuse, neglect, fire, water, lightning, or other acts of nature, unauthorized product modification, or failure to follow instructions supplied with the product.
 - Repair or attempted repair by anyone not authorized by ViewSonic.
 - Damage to or loss of any programs, data or removable storage media.
 - Software or data loss occurring during repair or replacement.
 - Any damage of the product due to shipment.
 - Removal or installation of the product.

- Causes external to the product, such as electrical power fluctuations or failure.
 - Use of supplies or parts not meeting ViewSonic's specifications.
 - Normal wear and tear.
 - Any other cause which does not relate to a product defect.
4. Removal, installation, and set-up service charges.

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 Network Adapter Products Warranty (V1.0)

