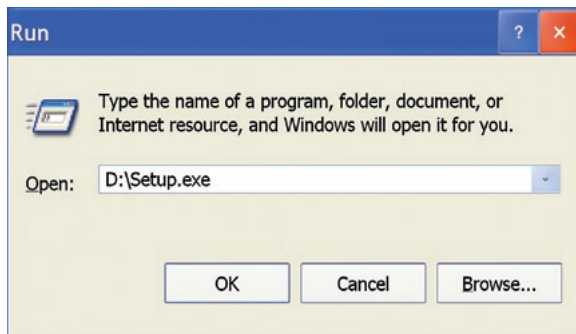
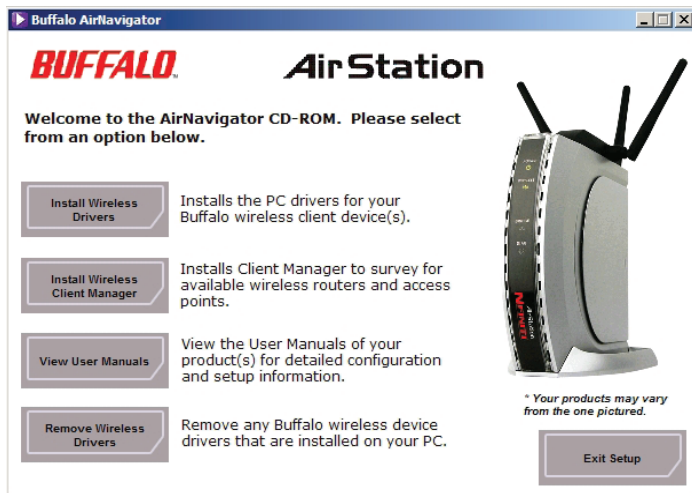




User Manual
125* High Speed Mode™
Wireless PCI Adapter
WLI2-PCI-G54S

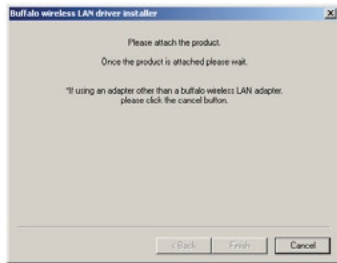
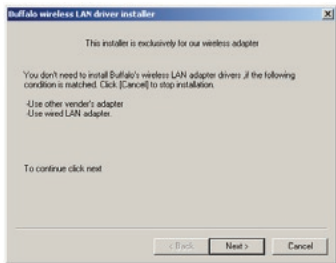


- Insert the AirNavigator CD into the CD-ROM drive of your computer. The AirNavigator Setup Wizard should launch automatically.
- To launch the AirNavigator Setup Wizard manually, click *Start*, then *Run*. Type “D:\Setup.exe”, where D is the drive letter assigned to your CDrom.
- Click *OK* to launch the wizard.

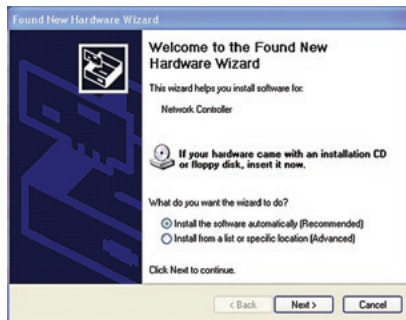


- Select *Install Wireless Drivers*.

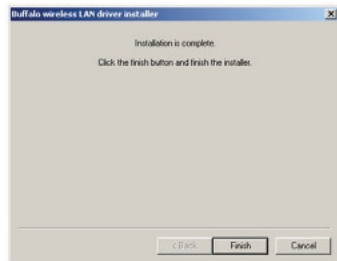
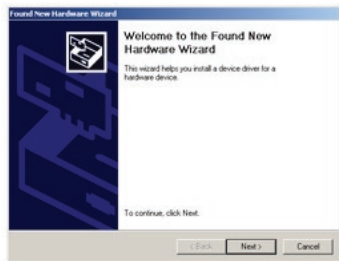
Installing Wireless Drivers



- Click *Next* to install a driver for the PCI adaptor.
- Select *Agree* and click *Next* to continue the process after reviewing the license agreement.
- A window will appear prompting the installation of the Wireless PCI Adapter into the PC. You will need to shut down your PC to install the wireless PCI card. Press *Cancel* if necessary and shut down your PC.

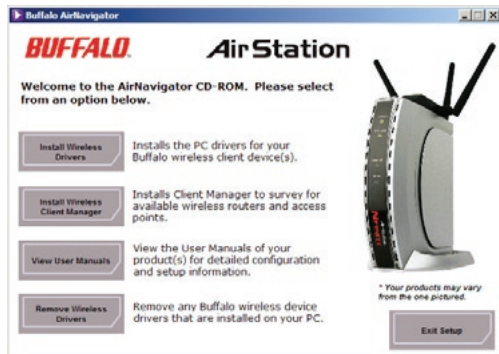


- Power off the desktop PC. Insert the **Wireless PCI Adapter** into an available PCI slot. PCI slots are located inside the desktop computer. Please consult the PC Manufacturer's documentation for PCI installation instructions. Once the Wireless PCI Adapter is installed correctly, attach the included antenna on the back of the PCI card, start the PC and let it boot into Windows. Then, the **Found New Hardware Wizard** will launch automatically. If the Found New Hardware Wizard does not launch, turn off the computer, remove the Wireless PCI Adapter, reinsert it into another PCI slot, and restart the computer.
- Select **Install the software automatically**. Click the **Next** button.



- When the 'Found New Hardware Wizard' launches, click *Next*.
- If the 'Digital Signature Not Found' page opens, click *Yes*.
- When the Wireless PCI Adapter is successfully installed, click *Finish*. Restart your computer if prompted.

Connecting Wireless Clients to your Network



Buffalo supports three different methods for connecting your wireless client device to your network.

If your AP supports it, use the simple, utterly secure AOSS to connect. Install the Client Manager from your AirNavigator CD (page 8) and turn to page 11.

You may also use the Client Manager software from your AirNavigator CD to configure your network manually. See page 16 for more on Client Manager.

If you're running Windows XP on your PC, you may use its built-in Zero Configuration tool to connect to your router/AP. See page 21 for more on Zero Configuration.

Client Manager can be used to survey and connect to available access points, configure WPA/WEK encryption, and create connection profiles.

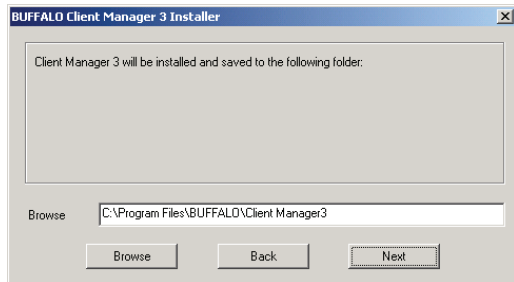
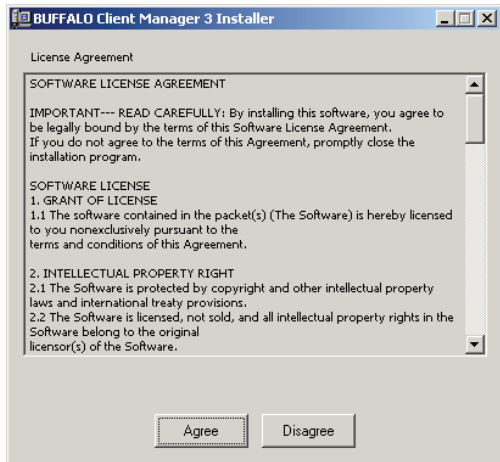
Note: When Client Manager is installed, Windows XP Wireless Zero Configuration is automatically disabled.



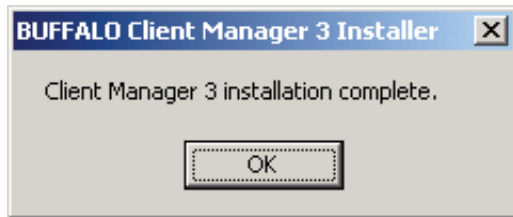
Installing Client Manager

Insert the AirNavigator CD into the CD-ROM drive of your computer. If the AirNavigator Setup Wizard does not launch automatically, launch it manually by clicking *Start* and then *Run*. Enter `D:\Setup.exe` in the dialog box that appears.

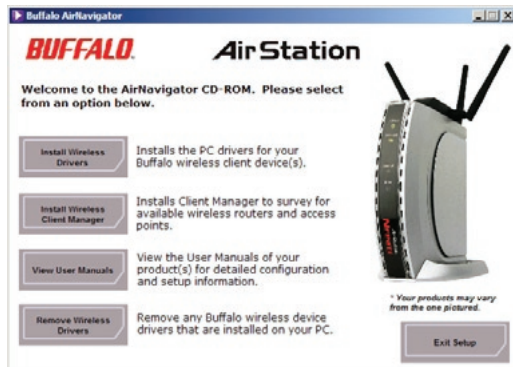
Click *OK*. Select *Install Wireless Client Manager*.



- Once the Client Manager Installer launches, click *Next*.
- Press *Agree* to accept the license agreement and continue installation.



- Click *OK* when Client Manager installation is complete.



- Press *Exit Setup* to exit AirNavigator.

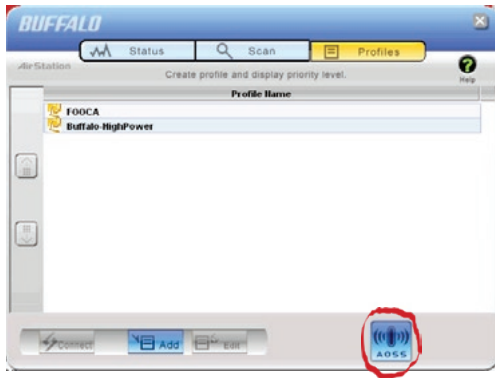
- Client Manager is now installed and running. Right-click on its icon (the black antenna) to use it.



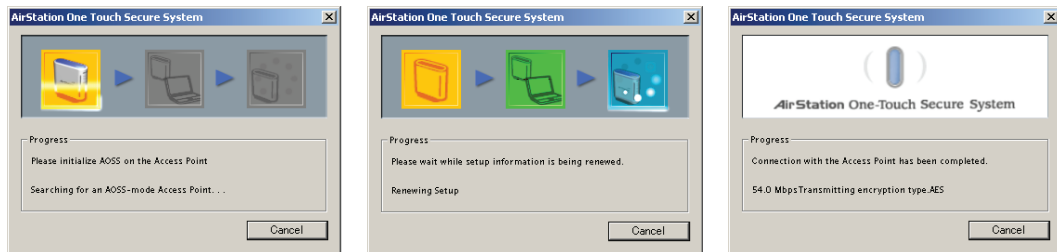


AOSS (AirStation One-Touch Secure System) is a simple, one-touch setup for connecting wireless clients to an access point while enforcing the most secure possible connection encryption type. Users no longer need to worry about choosing the proper security protocols, IP addresses, or SSID. AOSS determines the optimal connection and configures itself in seconds. If your router doesn't support AOSS, turn to page 6 to configure your connection manually with Client Manager or Wireless Zero Config.

The AOSS button for this wireless client is in its Client Manager software. Start Client Manager by right clicking on the black antenna icon in your System Tray, or by launching the Client Manager from your Start Menu: Programs >> Buffalo >> AirStation Utility >> Client Manager.



- From the Status Screen, select the *Profiles* tab.
- Initiate AOSS by clicking the blue AOSS button on the Client Manager's screen. The AOSS wizard will appear.
- Now, press the AOSS button on the Access Point. Hold it down until the AOSS LED begins to flash.



Once AOSS is complete (about 30 seconds), the connection is archived as a profile for later use. To minimize Client Manager to the system tray, click the 'X' in the top right corner.

Notes:

AOSS will scan for an AOSS partner for about two minutes. If it times out before finding one, just press the AOSS buttons again.

Output power is reduced to 25% of normal during AOSS for security reasons. If you're having trouble making an AOSS connection, temporarily move the devices closer together.

AOSS will automatically use the highest level of security available for all currently connected wireless devices.

If you have trouble connecting with AOSS, temporarily disable all personal firewalls on your PC, such as ZoneAlarm or Microsoft Personal Firewall. These programs may be re-enabled after AOSS has finished.

You may use Client Manager to configure your wireless network. Client Manager consists of the Status page, the Survey page, and the Profiles page. You can access each page by clicking the corresponding button on Client Manager. In addition to these pages, several dialog boxes are also available. You can access the Edit Profile dialog box, New Profile dialog box, IP Configuration dialog box, or WEP Configuration dialog box using the Client Manager pages. You may also initiate AOSS.

Status Page



Click *Status* to open this page. By default, this page is displayed when you start Client Manager. Details of connection status are displayed.

This page only displays connection information; no changes to settings are made here.

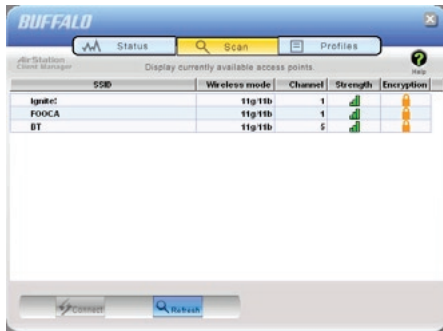
This page includes the following components:

- **Adapter Name** – Displays the part number of the wireless adaptor that is being used.

- **Network Type** - Displays whether network is in Ad-Hoc or Infrastructure mode.
- **Rate** – The speed of communication between wireless devices. If the Client Manager is not connected to a remote wireless device (access point or another client), no rate will be displayed.
- **Channel** – The channel that the two wireless clients are using for communication. If the Client Manager is not connected to a remote wireless device, no channel will be displayed. Channels 1-11 may be used.
- **Security** – The type of encryption in use. If the Client Manager is not connected to a remote wireless device, then 'No Encryption' will be displayed.
- **IP Address** – The IP address of the machine the Client Manager is installed on. If the Client Manager is not connected to a network with DHCP, then no IP address will be displayed.
- **MAC Address** – The MAC address of the wireless client device inside the computer Client Manager is installed on. If no wireless device is present in the computer, then no MAC Address will be displayed.
- **Signal Strength** – Displays the signal strength of the peak signal level the wireless adapter receives from the wireless device to which it is connected. Next to the signal level is the wireless hardware being used for this measurement.

Click the *Scan* tab to open this page. Here, you can survey the area, display available access points, and connect to available access points.

This page includes the following components:



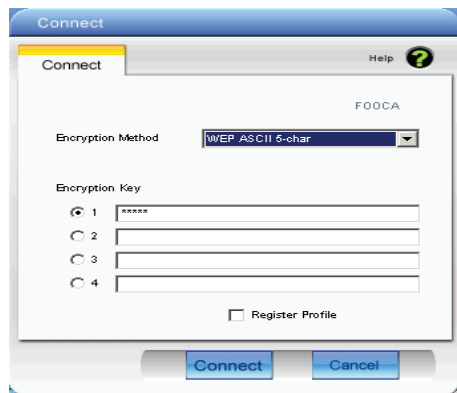
The screenshot shows the Buffalo Client Manager interface. At the top, there are tabs for 'Status', 'Scan', and 'Profiles'. Below the tabs, the text 'Display currently available access points' is visible. A table lists three access points: 'Ignitel', 'FOUCA', and 'BT'. Each row includes columns for 'Wireless mode', 'Channel', 'Strength', and 'Encryption'. The 'Strength' column contains signal strength icons, and the 'Encryption' column contains lock icons. At the bottom of the window, there are 'Connect' and 'Refresh' buttons.

SSID	Wireless mode	Channel	Strength	Encryption
Ignitel	11g/11b	1		
FOUCA	11g/11b	1		
BT	11g/11b	5		

- **Wireless SSID** – The SSID is the “name” of a wireless network. Each wireless device on a network must use identical SSIDs to successfully communicate.
- **Wireless Mode** – Displays available modes for each available remote wireless device.
- **Strength** – Displays the relative signal strength of the wireless networks.
- **Encryption** – Displays whether the wireless network is using any sort of encryption.

Click *Connect* to connect to a highlighted SSID, or *Refresh* to update the list of available wireless devices.

This dialog will open for you to enter any necessary encryption information.



The correct encryption type should already be selected automatically in the *Encryption Method* drop down list. Only change this setting if necessary.

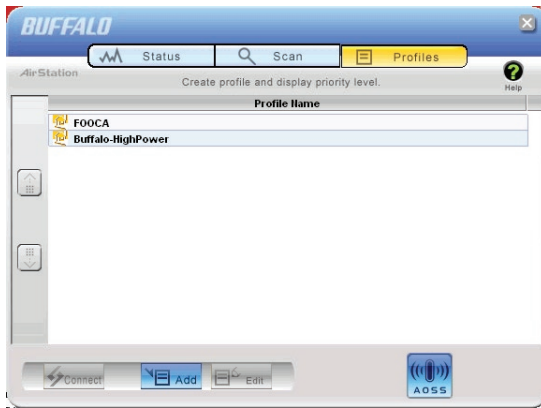
The *Encryption Key* is where the actual key for the wireless network should be entered. Some wireless networks allow you to enter multiple keys; four separate fields are available for this. If your network only uses one encryption key, then please use the first field (#1) to enter your key.

The *Register Profile* option will store this wireless network in your profiles. You will then automatically connect to this network when inside its range. This is recommended if you plan

on using this wireless network again.

Press the *Connect* button once you have completed entering encryption information.

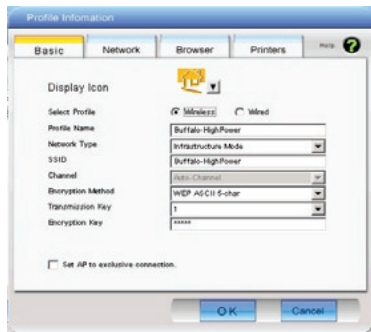
Profiles Page



Click the *Profiles* tab to open this page. Use this page to access your profiles. Profiles allow you to save the information associated with a specific wireless network so you can quickly and easily connect to that network when you are in that location. The Profiles page allows you to add, delete, and edit your profiles, as well as import and export data.

- **Connect** – Click the *Connect* button to connect to the selected profile and return to the Status page.
- **Edit** – Click the *Edit* button to edit the selected profile's settings. The Edit button also allows you to delete profiles that are no longer used or required.
- **Add** – Click the *Add* button to add a profile manually. You will need important information such as SSID, encryption settings, and network type.

New Profile Dialog Box



- **Select Profile** – Select whether the profile is for a wireless or wired connection.
- **Profile Name** – Enter the name you want to associate with the new profile.
- **Network Type** – Select the network mode you want to associate with the new profile. Select *Infrastructure* if your network consists of both wired and wireless devices that communicate through a central device, such as an access point. Select *Ad-hoc* if your network consists of only wireless devices that communicate with each other directly.
- **Network Name SSID** – Enter the *SSID* of your network. The SSID is the name of your wireless network. All wireless

devices on a network must use identical SSIDs to successfully associate with other devices on the network. MYSSID is an example of a valid SSID.

- **Channel** – The channel setting is only used for Ad-hoc connections. When using an Ad-hoc connection, select a channel and make sure the other Ad-hoc devices are configured to use the same channel. Otherwise, use *Auto-Channel*.
- **Encryption Method** – Displays the types of encryption available. Once encryption is selected, you will be required to enter an Encryption Key. For the Transmission Key Number, 1 is recommended.
- **OK** – Click *OK* to save your specifications and return to the Profiles page.

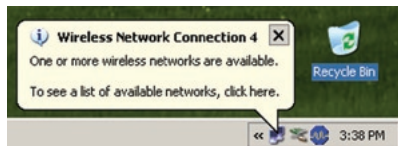
Advanced Profile Options

- **Network Tab** – Displays the network information tab. A static IP can be specified for this wireless profile here. It is not recommended to change any of these settings unless specified by an administrator.
- **Browser Tab** – Displays settings to change your browser preferences for this wireless profile. A specific home page can be specified when connected to this wireless profile as can specific proxy server addresses.
- **Printers Tab** – Displays the printers tab. A specific default printer can be associated to this profile. Thus, when connected to this profile, a specific printer will be used as the default printer.
- **OK** – Click the *OK* button to save your specifications and return to the Profiles page.



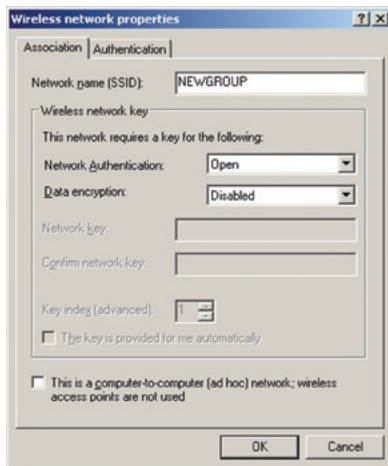
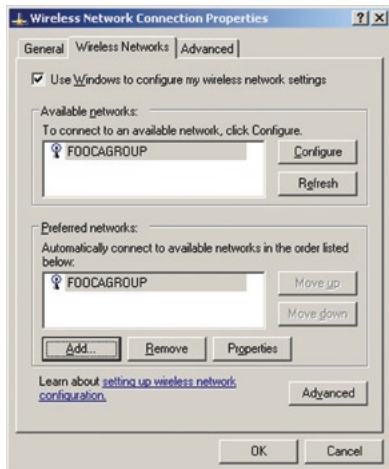
- **AOSS Icon** – To automatically add the USB wireless client to your network, just click this icon and then hold down the AOSS button on your wireless router for a few seconds.

Check your package for an AOSS Manual, which will give more information on using AOSS.

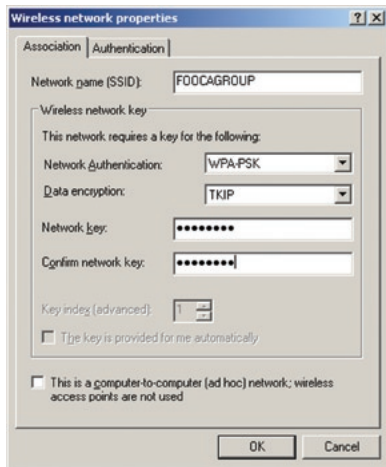


Windows XP includes the Zero Configuration Service, a built in service to configure your wireless clients from within Windows. Turn to page 7 if you would rather use Buffalo's Client Manager to configure your wireless client.

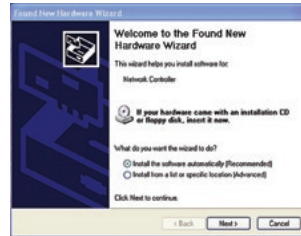
- If the Wireless Zero Configuration Service is activated, Windows will scan for available wireless access points once the Wireless PCI Adapter is properly installed. If Windows detects one or more access points, a networking icon appears within the system tray. "One or more wireless networks are available" will appear as a caption accompanying the icon.
- To start Wireless Zero Configuration manually, click *Start >> Control Panel >> Administrative Tools >> Services*. Select *Automatic* in the Startup Type field of Wireless Zero Configuration Service.
- Right click the networking icon in the taskbar and select *View Available Wireless Networks*. Select an SSID and click *Connect*. You may need to check the box indicating you are connecting to an unsecured network. See page 21 if you need to enter an SSID network name or WEP/WPA encryption key.



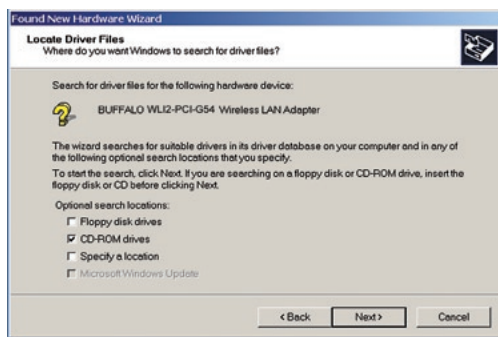
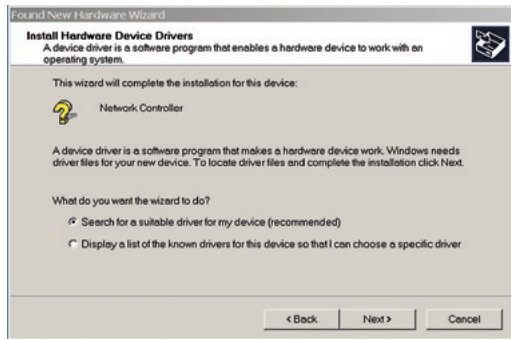
- Click the *Advanced* tab to enter an SSID network name or WEP/WPA encryption key if necessary. To add an SSID network name that is not listed, click *Add*.



- To configure a WEP/WPA encryption key, select the wireless network and click *Configure*.
- From the pull down menu, select the Network Authentication and Data Encryption types for the wireless network. Enter and confirm the Network Key and Key Index. Click *OK* when finished.



- After powering off the PC, insert the **Wireless PCI Adapter** into an available PCI slot. PCI slots are located inside the desktop computer. Please consult the PC Manufacturer's documentation for PCI installation instructions. Once the Wireless PCI Adapter is installed correctly, attach the included antenna on the back of the PCI card, start the PC and let it boot into Windows. Then, the **Found New Hardware Wizard** will launch automatically. If the Found New Hardware Wizard does not launch, turn off the computer, remove the Wireless PCI Adapter, reinsert it into another PCI slot, and restart the computer.



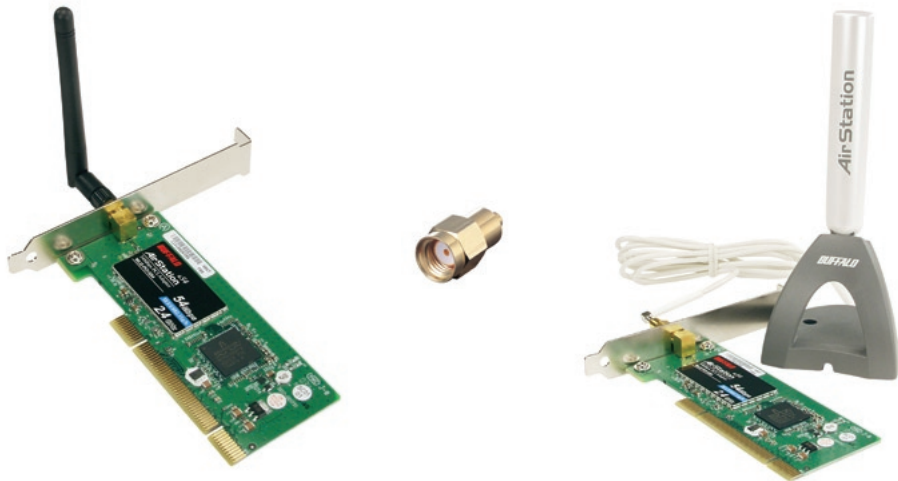
- **Insert the AirNavigator CD.** Click **Next** at the **Welcome to the Found New Hardware Wizard**. Select **Search** for a suitable driver for my device. Click the **Next** button to continue.
- Select only the **CD-ROM drives checkbox**, and **clear any other checkboxes** that are selected. Click the **Next** button to continue.

- Windows will display a driver you can use with the Wireless Desktop PCI Adapter. Click the **Next** button to continue.



- Windows 2000:** If the **Digital Signature Not Found** page opens, informing that no digital signature exists for the driver you are installing, click the **Yes** button to continue the installation process. When the Wireless Desktop PCI Adapter is successfully installed, click the **Finish** button. **Restart** your computer if prompted.

See the **Installing Client Manager** section to install the **Client Manager**.



- The WL12-PCI-G54S comes with a detachable omni directional antenna. However, for increased range a more powerful antenna can be purchased. Use the included antenna adapter (small brass piece) to connect it to an optional Buffalo MC Connector antenna.

Wireless Zero Configuration Service (Windows XP)

Windows XP offers the Wireless Zero Configuration Service to support 802.11b and 802.11g wireless networking. This service automatically polls the area for available wireless access points. If an available wireless access point is found, Windows attempts to connect to the access point. If no available wireless access points are found, you must manually add the access points.

Note: The Wireless Zero Configuration Service and Client Manager do not function properly together. If you want to use Client Manager, you must disable the Wireless Zero Configuration Service.

Enabling the Wireless Zero Configuration Service

Select **Start»Control Panel»Administrative Tools»Services** to open the Services window. Select **Automatic** in the Startup Type field of Wireless Zero Configuration Service to enable the Wireless Zero Configuration Service.

Note: The default Startup Type value of Wireless Zero Configuration Service is Automatic.

Disabling the Wireless Zero Configuration Service

Select **Start»Control Panel»Administrative Tools»Services** to open the Services window. Select **Disabled** in the Startup Type field of Wireless Zero Configuration Service to disable the Wireless Zero Configuration Service.

Wireless LAN Interface

Standards Compliance	IEEE 802.11g
Communication Protocol	Direct Sequence Spread Spectrum (DS-SS), Half Duplex
Frequency Range	2.412-2.462Mhz
Transmission Rates	802.11g: 1, 2, 5.5, 11, 18, 24, 36, 48, 54 125* Mode: 13, 20, 27, 40, 54, 80, 110, 125
Access Mode	Infrastructure mode, Ad-Hoc
Security	WEP 128/64 bit, 802.1x, WPA-TKIP/AES

Others

Interface	PCI
Power Consumption	1550mw
Environmental Operation	0-55°C, 20-80% (non-condensing)

Communication Range

Speed	Indoor	Outdoor
54Mbps	165 ft. (50m)	525 ft. (160m)
11Mbps	300 ft. (90m)	1310 ft. (400m)
1Mbps	375 ft. (115m)	1750 ft. (550m)

All distances are estimated. Wireless connections may be affected as physical conditions and circumstances vary.

Troubleshooting / FAQ

Use this section to locate answers to frequently asked questions.

What should I do if I already have a version of Client Manager on my PC?

Update your Client Manager to the version on the CD. If you do not update your Client Manager, there could be a loss of functionality, as some versions of Client Manager will not work properly with the G54 Wireless 54Mbps Desktop PCI Adapter. Before updating Client Manager, you must uninstall all previous versions of Client Manager. To update your Client Manager, load the Air Navigator CD and select Install Client Manager.

Why won't all my network clients work?

Some operating systems support only a limited number of network clients.

Windows 98/Me: These operating systems support only four network clients. If you install more than four network clients, only the first four clients you install will work.

Will Client Manager support all operating systems?

Client Manager and the G54 Wireless 54Mbps Desktop PCI Adapter currently support only Windows 98/ME/2000/XP. They do not currently support Windows NT, Mac OS, or Linux. For more information, refer to the Mac OS and Linux page in the Troubleshooting section of this help file.

Where can I attach my external antenna?

Insert your external antenna into the antenna connector, located on the back of the G54 Wireless PCI Adapter.

Why won't Client Manager function properly?

Windows XP – The Wireless Zero Configuration Service conflicts with Client Manager. Select **Start»Control Panel»Administrative Tools»Services** to open the Services window. Select **Disabled** in the Startup Type field of Wireless Zero Configuration Service to disable the Wireless Zero Configuration Service.

I have more than one Air Navigator CD. Do I need more than one CD?

No. You receive the same Air Navigator CD with each Buffalo Technology access point and wireless adapter. The CDs are identical and you only need one copy.

10BaseT or 100BaseTx: 802.3 based Ethernet network that uses UTP (Unshielded twisted pair) cable and a star topology. 10 is 10 Mbps and 100 is 100 Mbps.

802.1x: The standard for wireless LAN authentication used between an AP and a client. 802.1x with EAP will initiate key handling.

Ad-Hoc Network: The wireless network based on a peer-to-peer communications session. Also referred to as AdHoc.

Bandwidth: The transmission capacity of a computer or a communication channel, stated in Megabits per second (Mbps).

BSS (Basic Service Set): An 802.11 networking framework that includes an Access Point.

Bus Mastering: A system in which the specified Input/Output device (e.g. NIC Card) can perform tasks without the intervention of the CPU.

Client: A PC or workstation on a network.

Cross-Over Wiring: A UTP cable that has its transmit and receive pair crossed to allow communications between two devices.

DCE (Data Communications Equipment): Hardware used for communication with a Data Terminal Equipment (DTE) device.

Default Gateway: The IP Address of either the nearest router or server for the LAN.

Default Parameter: Parameter set by the manufacturer.

Destination Address: The address portion of a packet that identifies the intended recipient station.

DHCP (Dynamic Host Configuration Protocol): Based on BOOTP, it uses a pool of IP addresses, which it assigns to each device connected to it, and retrieves the address when the device becomes dormant for a period of time.

DNS (Domain Name System): System used to map readable machine names into IP addresses

Driver: Software that interfaces a computer with a specific hardware device.

DSSS (Direct Sequence Spread Spectrum): Method of spreading a wireless signal into wide frequency bandwidth.

DTE (Data Terminal Equipment): Device that connects 10BaseT or 100BaseTx: 802.3 based Ethernet network that uses UTP (Unshielded twisted pair) cable and a star topology. 10 is 10 Mbps and 100 is 100 Mbps.

802.1x: The standard for wireless LAN authentication used between an AP and a client. 802.1x with EAP will initiate key handling.

Ad-Hoc Network: The wireless network based on a peer-to-peer communications session. Also referred to as AdHoc.

Bandwidth: The transmission capacity of a computer or a communication channel, stated in Megabits per second (Mbps).

BSS (Basic Service Set): An 802.11 networking framework that includes an Access Point.

Bus Mastering: A system in which the specified Input/Output device (e.g. NIC Card) can perform tasks without the intervention of the CPU.

Client: A PC or workstation on a network.

Cross-Over Wiring: A UTP cable that has its transmit and receive pair crossed to allow communications between two devices.

DCE (Data Communications Equipment): Hardware used for communication with a Data Terminal Equipment (DTE) device.

Default Gateway: The IP Address of either the nearest router or server for the LAN.

Default Parameter: Parameter set by the manufacturer.

Destination Address: The address portion of a packet that identifies the intended recipient station.

DHCP (Dynamic Host Configuration Protocol): Based on BOOTP, it uses a pool of IP addresses, which it assigns to each device con-

nected to it, and retrieves the address when the device becomes dormant for a period of time.

DNS (Domain Name System): System used to map readable machine names into IP addresses

Driver: Software that interfaces a computer with a specific hardware device.

DSSS (Direct Sequence Spread Spectrum): Method of spreading a wireless signal into wide frequency bandwidth.

DTE (Data Terminal Equipment): Device that controls data flowing to and from a computer.

Dynamic IP Address: An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server.

ESS (Extended Service Set): A set of two or more BSSs that form a single sub-network. ESS-ID is user identification used in the ESS LAN configuration.

Ethernet: The most widely used architecture for Local Area Networks (LANs). It is a shared-

media network architecture. The IEEE 802.3 standard details its functionality.

Ethernet cable: A wire similar to telephone cable that carries signals between Ethernet devices.

File and Print Sharing: A Microsoft application that allows computers on a network to share files and printers.

Firmware: Programming inserted into programmable read-only memory, thus becoming a permanent part of a computing device.

Frame: A fixed block of data, transmitted as a single entity. Also referred to as packet.

Full-Duplex: To transmit on the same channel in both directions simultaneously.

Gbps (Giga Bits per second): One billion bits per second.

Half-duplex: To transmit on the same channel in both directions, one direction at a time.

Hub: A device which allows connection of computers and other devices to form a LAN.

IEEE (Institute of Electrical and Electronics Engineers): The professional organization which promotes development of electronics technology.

IP (Internet Protocol) Address: A unique 32-bit binary-digit number that identifies each sender or receiver of information sent in packets.

Infrastructure: A wireless network or other small network in which the wireless network devices are made a part of the network through the Access Point.

ISP (Internet Service Provider): A company that provides access to the Internet and other related services.

IV (Initialization Vector): The header section of a message packet.

LAN (Local Area Network): A group of computers and peripheral devices connected to share resources.

LED (Light Emitting Diode): The lights on a hardware device representing the activity through the ports.

MAC (Medium Access Control) Address: A unique number that distinguishes network cards.

Mbps (Mega Bits Per Second): A measurement of millions of bits per second.

MDI/X (Media Dependent Interface/Crossover): Port on a network hub or switch that crosses the incoming transmit lines with the outgoing receive lines.

MHz (MegaHertz): One million cycles per second.

MIB II: A database containing performance information and statistics on each device in a network.

MIPS (Million Instructions Per Second): A measurement of processing speed.

NAT (Network Address Translation): An internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set for external traffic.

NIC (Network Interface Card): An expansion card connected to a computer so the computer can be connected to a network.

Packet: A block of data that is transferred as a single unit, also called a frame or a block.

Packet Filtering: Discarding unwanted network traffic based on its originating address or its type.

PCI (Peripheral Component Interconnect): A bus that is connected directly to the CPU.

PCMCIA (Personal Computer Memory Card International Association) Card: Removable module that adds features to a portable computer.

Ping (Packet Internet Groper): An Internet utility used to determine whether a particular IP address is online.

Plug and Play: Hardware that, once installed (“plugged in”), can immediately be used (“played”), as opposed to hardware that requires manual configuration.

PoE (Power over Ethernet): A mechanism to send DC power to a device using a CAT5 Ethernet cable.

PPPoE (Point-to-Point Protocol over Ethernet): A specification for connecting users on an Ethernet line to the Internet through a common broadband medium.

Protocol: A standard way of exchanging information between computers.

RADIUS (Remote Authentication Dial In User Service): A server that issues authentication key to clients.

RAM (Random Access Memory): Non-permanent memory.

Repeater Hub: A device that collects, strengthens and transmits information to all connected

devices, allowing the network to be extended to accommodate additional workstations.

RC4: The encryption algorithm that is used in WEP.

RJ-45 connector: An 8-pin connector used between a twisted pair cable and a data transmission device.

ROM (Read Only Memory): Permanent memory.

Router: Device that can connect individual LANs and remote sites to a server.

Roaming: The ability to use a wireless device while moving from one access point to another without losing the connection.

Script: A macro or batch file containing instructions and used by a computer to perform a task.

Server: Any computer that makes files or peripheral devices available to users of the network and has a resident Network OS.

SMTP (Simple Mail Transfer Protocol): The protocol used to define and deliver electronic mail (E-mail) from one location to another.

SNMP (Simple Network Management Protocol): An application layer protocol that outlines the formal structure for communication among network devices.

Static IP Address: A permanent IP address is assigned to a node in a TCP/IP network. Also known as global IP.

STP (Shielded Twisted Pair): Twisted Pair cable wrapped in a metal sheath to provide extra protection from external interfering signals.

Subnet Mask: An eight-byte address divided into 4 parts separated by periods.

TCP/IP (Transmission Control Protocol/Internet Protocol): Protocol used by computers when communicating across the Internet or Intranet.

TFTP (Trivial File Transfer Protocol): Simple form of FTP (File Transfer Protocol), which

Uses UDP (User Datagram Protocol), rather than TCP/IP for data transport and provides no security features.

TKIP (Temporal Key Integrity Protocol): An encryption method replacing WEP. TKIP uses random IV and frequent key exchanges.

Topology: The shape of a LAN (Local Area Network) or other communications system.

Twisted Pair: Cable that comprises 2 or more pair of insulated wires twisted together.

UDP (User Datagram Protocol): A communication method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network. UDP is used as an alternative to TCP/IP.

Uplink: Link to the next level up in a communication hierarchy.

UTP (Unshielded Twisted Pair) cable: Two or more unshielded wires twisted together to form a cable.

WAN (Wide Area Network): A networking system covering a wide geographical area.

WEP (Wired Equivalent Privacy): An encryption method based on 64 or 128-bit algorithm.

Web Browser: A software program that allows viewing of web pages.

Wi-Fi (Wireless Fidelity): An organization that tests and assures interoperability among WLAN devices.

Wire Speed: The maximum speed at which a given packet can be transferred using Ethernet and Fast Ethernet standard specifications.

WLAN (Wireless LAN): A LAN topology using wireless devices.

VPN (Virtual Private Network): A security method to connect remote LAN users to a corporate LAN system.

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.

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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.

IMPORTANT NOTE:

FCC RF Radiation Exposure Statement:

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

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

R&TTE Compliance Statement

This equipment complies with all the requirements of the DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this manual and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries intended for use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Norway, The Netherlands, Portugal, Spain, Sweden, Switzerland and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU Countries Not intended for use

None.

Potential restrictive use

France: Only channels 10,11,12, and 13.

Buffalo Technology (USA), Inc. products comes with a two-year limited warranty from the date of purchase. Buffalo Technology (USA), Inc. warrants to the original purchaser the product; good operating condition for the warranty period. This warranty does not include non-Buffalo Technology (USA), Inc. installed components. If the Buffalo product malfunctions during the warranty period, Buffalo Technology (USA) Inc. will, replace the unit, provided the unit has not been subjected to misuse, abuse, or non-Buffalo Technology (USA), Inc. authorized alteration, modifications or repair.

All expressed and implied warranties for the Buffalo Technology (USA) Inc. product line including, but not limited to, the warranties of merchantability and fitness of a particular purpose are limited in duration to the above period.

Under no circumstances shall Buffalo Technology (USA), Inc. be liable in any way to the user for damages, including any lost profits, lost savings or other incidental or consequential damages arising out of the use of, or inability to use the Buffalo products.

In no event shall Buffalo Technology (USA), Inc. liability exceed the price paid for the product from direct, indirect, special, incidental, or consequential damages resulting from the use of the product, its accompanying software, or its documentation. Buffalo Technology (USA), Inc. does not offer refunds for any product.

@ 2004 Buffalo Technology (USA) Inc.

ADDRESS

Buffalo Technology (USA), Inc.
4030 West Braker Lane, Suite 120
Austin, TX 78759-5319

GENERAL INQUIRIES

Monday through Friday
8:30am-5:30pm CST

Direct: 512-794-8533

Toll-free: 800-456-9799

Fax: 512-794-8520

Email: *sales@buffalotech.com*

TECHNICAL SUPPORT

North American Technical Support by phone is available 24 hours a day, 7 days a week. (USA and Canada).

Toll-free: (866) 752-6210

Email: *info@buffalotech.com*

BUFFALO™

4030 W. Braker Ln. Suite 120
Austin, Texas 78759
Tel: 800-456-9799
Fax: 512-794-8606

Technical Support is available 24 hours a day, 7 days a week
(USA / Canada)

Toll-Free: 866-752-6210
email: info@buffalotech.com

©2004, Buffalo Technology (USA), Inc.