NFINITI *Wireless Router & AP*

Work and play - further and faster! Your AirStation Nfiniti combines gigabit networking with extended wireless range and speed. For best performance, use with Nfiniti wireless clients.

System Requirements:

• A high-speed (Broadband) Internet connection or existing local area connection.
• A computer with a network connection (wired or wireless) and a good web browser. The screenshots in this manual were taken with Firefox, but Netscape and Internet Explorer are also supported in versions 4.5 or later, and Safari 1.0 and later are supported with Macintosh OS X 10.2 and later.

Package Contents:

• WZR-AG300NH AirStation with antenna assembly
• Stand for vertical placement
• AC adapter and power cable
• CAT5 LAN cable
• Utility CD with Manual
• Quick Setup Guides
• Warranty Statement

Begin by finding a good place to set up your router/access point. Some things to consider:

• You'll need to be able to plug your internet connection into it, so it should go within reach of the LAN cable from your DSL or Cable modem. You'll also want a power outlet nearby.

• Keep the access point as central in your work area as possible. Signal strength and speed fall off with distance.

• Higher is often better. For instance, set it up on the top shelf of a bookcase rather than the bottom one, if possible.

Do you need a password or other information to log in to your internet connection? Many DSL connections require information like global IP address, subnet mask address, default gateway address, DNS server address, or PPPoE parameters in order to connect. Cable modems usually don't require extra information. If you have a DSL internet connection, make sure that you have any necessary information handy before you continue. Your Internet Service Provider can give you this information if you don't know it.

Your AirStation may be used horizontally or vertically.

For horizontal placement, leave the silver base attached to the antennas. The antennas will usually work best if oriented vertically.

For vertical placement, attach the stand to base of the router as shown at left. Remove the silver base from the antennas. The antennas may then be attached to the top of the AirStation.

Power to outlet or
power strip

PC

Cable or DSL Modem
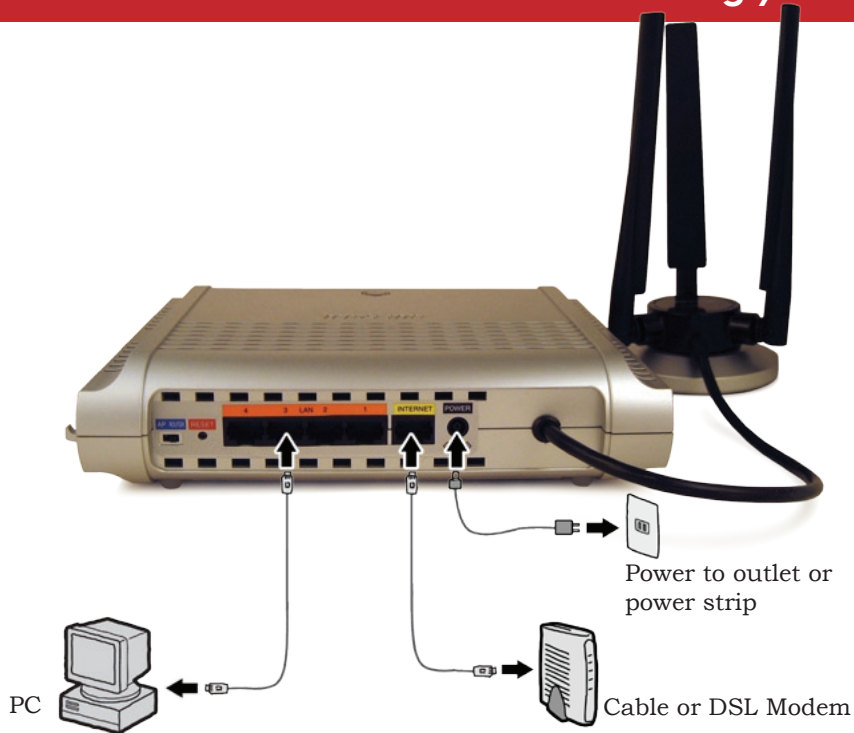
To initially configure your router, you'll use a wired connection to your computer. Once you've connected to the internet through the router, you may switch to a wireless connection if desired.

The computer used to configure the AirStation should be set to obtain an IP address automatically using a DHCP server (this is the default). The WZR-AG300NH has a default LAN IP address of 192.168.11.1 and Subnet Mask of 255.255.255.0.

1. Power down the Cable or DSL modem and the computer which will be used to configure the AirStation router.

2. Plug the Cable or DSL modem's Ethernet cable into the AirStation's WAN port. Initially, you may need to unplug this cable from your computer, hub or other router.

3. Plug the provided Ethernet cable into a LAN port on the AirStation and plug the other end into your computer's Ethernet adapter (NIC).

4. *Important: turn everything on in the correct order!!* Power on your cable or DSL modem and wait one full minute, then power on the AirStation router and wait one full minute, and finally power on the computer which will be used to configure the AirStation.

Launch a web browser on the computer that you're using to configure the AirStation.

Enter *192.168.11.1* into the URL field. Naturally, if you change your AirStation's IP address, you'll have to enter the new address instead.
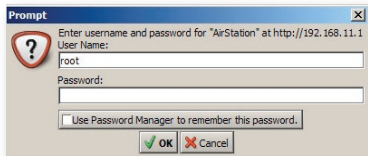
A window will open, prompting you to enter a User ID and Password.

Enter *root* as the User name and leave the password field *blank*.

Your AirStation's SmartRouter technology will determine the type of internet connection you have automatically, and ask you for any needed information. If your ISP assigns IPs automatically (most cable providers do), their DHCP server will give your router an IP address. If additional login information is required to connect to the internet, the wizard will ask for it. Enter any required login information if asked. Contact your DSL provider for any missing login information.
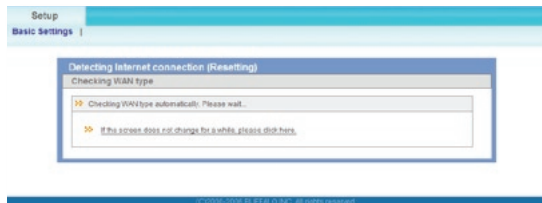
If you need to relaunch the Internet Connection Wizard, just click on *Run Internet Connection Wizard* under *Basic Settings.*

Congratulations! You are now connected to the internet. Open a familiar web page to make sure everything is working correctly.

To connect wireless devices to the AirStation, you may either enter the SSID and encryption key manually, or you can use AOSS. For more information on AOSS, see pages 14 and 15.

Consult your wireless clients' manuals for instructions on configuring them manually. You can get SSID and encryption information from the AirStation's initial setup screen, as shown above. By default, the SSID is "*macaddress_A*" for wireless A channels and "*macaddress_G*" for wireless G and B channels. By default, encryption is *not enabled* ("open").

If you prefer to use encryption and/or a different SSID, you may change these default settings under *Basic Settings* at the top left of the page.
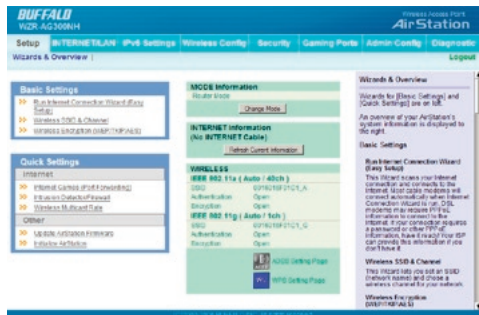
You can get back to the Setup page from anywhere in the configuration screens by clicking on the *Setup* tab in the top left corner. From here, you can rerun the Internet Connection Wizard, change your wireless SSID and channel, and choose your encryption type under Basic Settings. The *Wireless* section shows your SSID and encryption settings.

You can also configure *port mapping* for your internet games, turn on UPnP for *Windows (MSN) Messenger*, configure your *Firewall*, set up *Encryption*, choose your *Multicast Rate*, update your AirStation's firmware, and reset your AirStation to factory settings. As you explore the configuration tool, you'll see that context sensitive help is available on the right side of each page.

The menus in the Configuration Tool let you change your AirStation's settings. To navigate settings, choose a *category* at the top of the page and then a *submenu* below. Settings will appear on the left, help files on the right. This example shows the WAN/LAN category with the WAN submenu item selected.

Categories

Submenus

Individual Settings
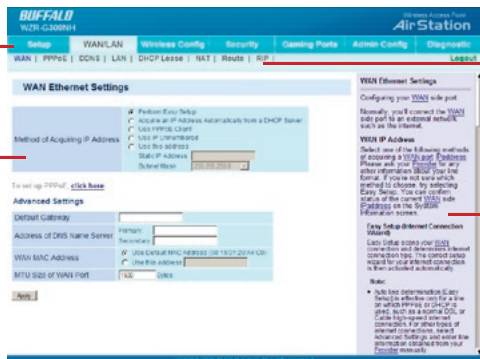
Help and Instructions

The following pages show examples of some screens from the configuration utility.
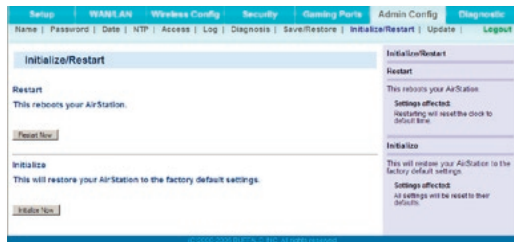
The Initialize/Restart page can be reached by choosing the *Admin Config* catagory tab and then clicking on the *Initialize/Restart* submenu.

Click *Restart Now* from this page to restart your AirStation. Click *Initialize Now* to restore your AirStation to factory defaults and restart it.

You may also initialize your AirStation by holding down the *Reset* button for 3 seconds.

You can get to this page by selecting the *Wireless Config* category and choosing the *AOSS* submenu.

The blue AOSS button at the top left of the page has the same function as the physical AOSS button on the top of the router: it initiates the AOSS process.

If all your clients support AOSS, it's very simple to set them up. Press the AOSS button on the router, or the one on this page, and then push the AOSS button on the client device.

Each client device will have to be set up seperately. Wait for each AOSS process to finish before starting the next one.

You can also activate AOSS by pushing the button on the top of your AirStation (see page 15). Consult your client device's documentation for the location of its AOSS button.

If you've used AOSS to configure some wireless clients, and now want to add other wireless clients that don't support AOSS to your network, this screen will give you the information you need to connect them manually.

AOSS (AirStation One-Touch Secure System) is a simple system for configuring your wireless network securely. If your router and your client device are installed and both support AOSS, then making a secure wireless connection between them is very easy.

Push the AOSS button on the top of your router and hold it in for a few seconds. The AOSS light will begin to flash amber. You now have two minutes to push the AOSS button on your client device and finish the connection.

If you have a *standalone client device*, it will probably have a little red button labled "AOSS" on it. Push the button! About 15 seconds later, you'll have a secure network connection.

If your client device is a PC card, CardBus, or PCI adaptor, the AOSS button will probably be in its *Client Manager Software*. Check your client device's user manual for instructions on where to push or click the AOSS button.

standalone client device	PC card	Client Manager Software

After you've pressed both buttons, it will take about 15 seconds for the connection to complete. When it's finished, the AOSS light witll glow a solid amber. You now have a secure network connection!

Some things to keep in mind with AOSS:

- Only one AOSS wireless client adapter can be configured with the AOSS router at a time. The buttons will need to be re-pressed to connect each additional AOSS wireless client adapter.
- It is not necessary to AOSS client devices that have already been configured via AOSS, unless significant changes have been made to the wireless network.
- Do not attempt to configure two separate AOSS networks at the same time, as it may cause undesired configurations.
- If an undesired client has connected via AOSS, it can be disconnected from within the WZR-AG300NH's advanced configuration menus.
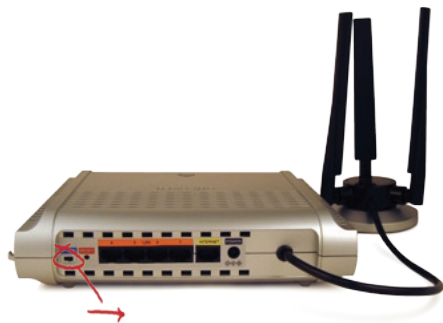
This AirStation supports quickly changing the product from a wireless router to a conventional access point.

Put your Airstation into Access Point Mode by moving the switch on the bottom of your AirStation from ROUTER to AP. This changes the default IP address of the AirStation from 192.168.11.1 to 192.168.11.100, and DHCP, NAT, and the WAN port are disabled.

Access Point Mode might be desirable if you're adding wireless capability to an existing network with a router. It is not suitable for most home configurations. If you plan to use the AirStation as an normal wireless router, make sure that this switch is in the normal (ROUTER) position!
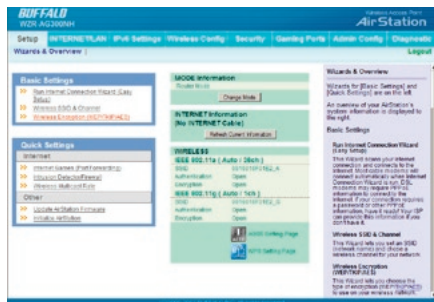
By default, encryption is not enabled on the AirStation unless you used AOSS to perform your setup. Anyone within range can easily connect to your wireless network. This might not be what you want.

Buffalo recommends enabling encryption and setting a password for access to your network. This is easy to configure from within the AirStation's configuration tool. From the opening page, select *Wireless Encryption* from the left-side menu.
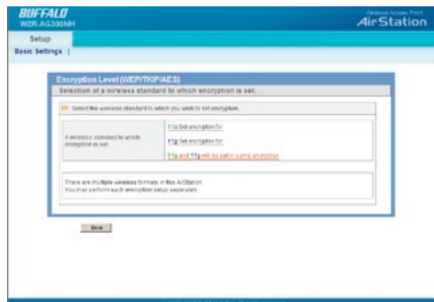
You may set encryption for 11a and 11g at once or separately.

Many kinds of encryption are available. WEP works with almost everything. WPA2-PSK is much more secure. Choose the strongest method of encryption that works with all of your wireless devices.
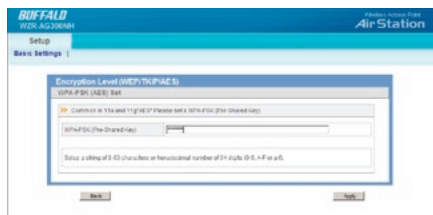
Enter a network key ("password") twice. Write down your password and put it in a safe place. You will not be able to connect wireless devices to your network without this password.

Click *Apply* to change your AirStation's settings.
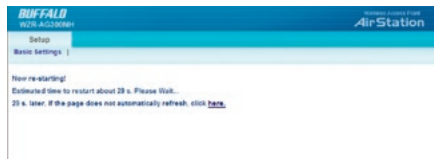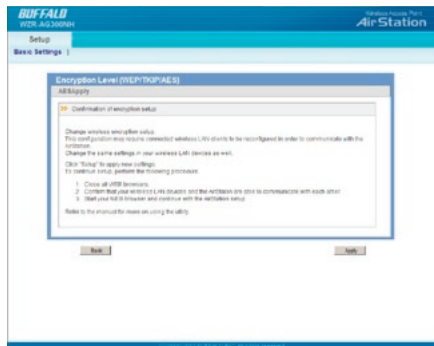
It will take about 30 seconds for the changes to take effect.
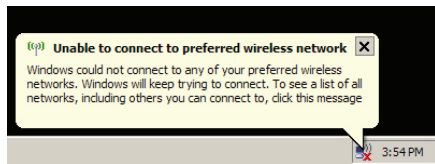
Each of your wireless clients will need your password to connect to the network. Click on the wireless icon in your computer's systray, or this message if it pops up.
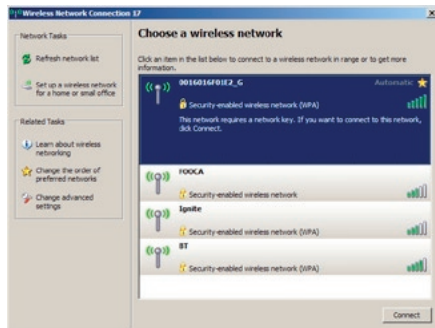
Any wireless networks available in the area will be listed as available. Click on your wireless network SSID so that it turns blue and the click on *Connect* at the bottom right.
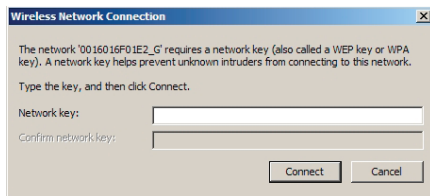
Enter your network key ("password") twice and click *Connect.*
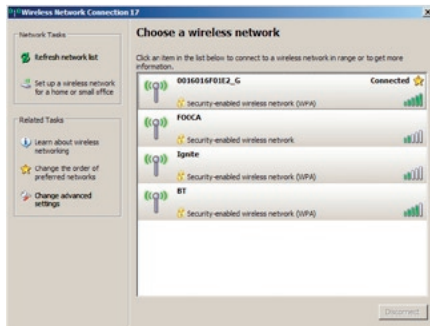
Repeat for each Windows XP computer that connects to your network wirelessly.

Other wireless devices may have different configuration requirements. Consult their documentation for instructions on how to enter your network key and connect them to your wireless network.

Add an AirStation without changing your existing LAN configuration

1. Set the AirStation into Access Point Mode by moving the switch from *ROUTER* to *AP*.

2. Connect one of the AirStation's LAN ports to an existing router or switch on your network. Nothing should be plugged into the WAN ("Internet") port.

3. Open LAN Settings - LAN Port Settings and configure the following settings:

   IP Address =[192.168.11.137] (Specify an unused network address from the existing LAN.)

   Subnet Mask=[255.255.255.0] (Use the same Subnet Mask as the existing LAN.)

   DHCP Server Function=[Disable]

4. Restart PC.

For more information, FAQ's, and updates, consult the AirStation website at
http://www.buffalotech.com.

WZR-AG300NH AirStation Specifications

Physical Specifications

Dimensions 2.0" x 6.9" x 8.3" (51 x 175 x 211mm)
Weight .88 lb. (400g)

Temperature & Humidity

Operation 32˚ to 104˚ F, 0˚ to 40˚ C
Maximum humidity 80%
Transit/Storage 0˚ to 40˚ C maximum humidity 80% (no condensation)

Power Characteristics
Power Supply: 100-240V AC Universal, 50/60 Hz.
Power Output: 12V DC
Power Consumption about 10 Watts (Max)

Regulatory Information

Wireless communication is often subject to local radio regulations. Although AirStation wireless networking products have been designed for operation in the license-free 2.4 GHz band, local radio regulations may impose limitations on the use of wireless communication equipment.

Network Compatability

Draft-N support built off of the Draft Specification 1.0 for 802.11n.
IEEE802.11g/b Standard for Wireless LANs; 125* High Speed Mode also Available (Turbo G).

Host Operating System

Microsoft Windows® 98SE/ME/NT4.0/2000/XP, Unix, Linux and MacOS
Media Access Protocol
Wired - CSMD/CD (Collision Detection)
Wireless - CSMD/CA (Collision Avoidance) with Acknowledgment (ACK)

AirStation IEEE 802.11 Channel Sets

The range of the wireless signal is related to the Transmit Rate of the wireless communication. Communications at a lower Transmit range may travel longer distances.

Center Channel ID FCC

1 2412 2 2417 3 2422 4 2427 5 2432 6 2437 7 2442 8 2447 9 2452 10 2457
11 2462 11 default channel

Common Problems

• Out of range, client cannot connect to the AirStation.
• Configuration mismatch, client cannot connect to the AirStation.
• Absence or conflict with the Client Driver.
• Conflict of another device with the AirStation hardware.

LED Activity

Monitoring LED activity helps identify problems.

• Power LED should be Green,
• Wireless LED should be Green if the line is active. If is it blinking Green, wireless communication is active.
• Ethernet LED should be Blue (1000Mbps), Green (100Mbps), or Amber (10Mbps) while the communication is active.
• The Red Diag LED will flash during boot and firmware updates.

DIAG LED Activity

Unplug the power for three seconds. Plug the power back in to monitor the Diag LEDs during start-up.

DIAG LED Activity Table

DIAG LED Display	Time	Description/Action
Continuous Red	Starting	RAM Error Red flash, 2 times Starting Flash ROM Error
Red flash, 3 times	Starting	A problem on the wired LAN side
Red flash, 4 times	Starting	A problem on the wireless LAN side

LEDs Work But Client PC Cannot Connect to Network

If the LEDs indicate that the network is working properly (Power LED is on, Transmit/Receive LED blinks), check the TCP/IP settings of the network.

Changing Client TCP/IP Settings in Windows

Consult the LAN Administrator for correct TCP/IP settings.

To add or change TCP/IP Settings:

1. On the Windows task bar, click Start.
2. Select Settings, then Control Panel.
3. Double-click on the Network icon to view Network Properties.
4. From the list of installed components, verify the TCP/IP => wireless LAN adapter protocol is installed.

- If the wireless adapter protocol is not yet installed, click the *Add* button and select the TCP/IP protocol from the list. Refer to Windows Help for more information.
- If the wireless adapter protocol is installed, select the protocol and click the *Properties* button. Verify that the parameters match the settings provided by your LAN Administrator. Make changes if necessary, and click OK.

5. If prompted, restart your computer.

Other Problems

Please refer to **www.buffalotech.com** for further reference materials.

10BaseT: 802.3 based Ethernet network that uses UTP (Unshielded twisted pair) cable and a star topology. 10 Mbps data tansmission speed.

100BaseT: 802.3 based Ethernet network that uses UTP (Unshielded twisted pair) cable and a star topology. 100 Mbps data tansmission speed.

1000BaseT: 802.3 based Ethernet network that uses UTP (Unshielded twisted pair) cable and a star topology. 1000 Mbps data tansmission speed.

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

Access Point: A hardware device that acts as a communication hub for *Clients* (users of wireless devices) to connect to a wired LAN.

Ad-Hoc Network: A network based on peer-to-peer communication rather than a router, switch, or hub.

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

Bridge: A device which forwards traffic between network segments with a common network layer address, based on data link layer information.

Client: A PC, workstation, or other device that connects to a network wirelessly through an *Access Point.*

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

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

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.

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

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. It is designed to connect a single device's NIC to a router, switch, or hub. See also *Crossover cable.*

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

Firmware: Computer programming instructions that are stored in a read-only memory unit rather than being implemented through software.

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

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

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-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 an encrypted 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: The unique number that distinguishes every network interface card.

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

MDI/X (Media Dependent Interface/ Cross-over): 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.

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.

Peer-to-peer: This simple network is formed by connecting computers directly, without use of routers or hubs. A *crossover cable* is plugged into an Ethernet port in each computer, connecting them directly.

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

Plug and Play: Hardware that, once physically installed, finishes its installation automatically and may immediately be used, as opposed to hardware that requires further 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 keys 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. See also *Bridge*.

RC4: The encryption algorithm used by WEP.

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

ROM (Read Only Memory): Memory hardware that allows fast access to permanently stored data but prevents addition to or modification of the data.

Router: A device in a network that handles message transfer between computers. Similar to a *hub*, but with added functionality and efficiency.

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

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.

SSID: The "name" of your wireless network. You can get it from the Setup page of the configuration utility.

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.

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): A security protocol for wireless local area networks defined in the 802.11b standard, using a 64 bit or 128 bit key. WEP was designed to provide the same level of security as that of a wired LAN. However, it has been found that WEP is not as secure as once believed.

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 Warning

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for uncontrolled equipment and meets the FCC radio frequency (RF) Exposure Guidelines in Supplement C to OET65. This equipment should be installed and operated with at least 20cm and more between the radiator and person's body (excluding extremities: hands, wrists, feet and legs). This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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.

Europe – EU Declaration of Conformity
This device complies with the essential requirements of the R&TTE Directive 1999/5/EC.
The following test methods have been applied in order to prove presumption of compliance with the R&TTE Directive 1999/5/EC:

• EN 60950: 2000 Safety of Information Technology Equipment

• EN 300 328-2 V1.2.1 (2001-12) Technical requirements for spread-spectrum radio equipment

• EN 301 489-17 V1.1.1 (2000-09) EMC requirements for spread-spectrum radio equipment

Taiwan:
SAR compliance has been established in typical laptop computer(s) with CardBus slot, and product could be used in typical laptop computer with CardBus slot. Other application like handheld PC or similar device has not been verified, may not comply with related RF exposure rules, and such use shall be prohibited.

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.

Intended use

This device is a 2.4 GHz & 5 GHz wireless LAN transceiver, intended for indoor home and office use in USA, Canada, all EU and EFTA member states.

EU Countries intended for use

This device is intended for indoor home and office use in the following countries: Austria, Belgium, Germany, Denmark, Spain, Greece, France, Finland, Italy, Ireland, Luxembourg, The Netherlands, Portugal, Sweden, United Kingdom, Cyprus, Czech Republic, Estonia, Hungry, Latvia, Lithuania, Malta, Poland, Slovak Republic and Slovenia.

The device is also authorised for use in all EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU countries not intended for use

None

Potential restrictive use

This device is a 2.4 GHz & 5 GHz wireless LAN transceiver, intended for indoor home and office use in all EU and EFTA member states, except in France, Belgium and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain an authorization to use the device for setting up outdoor radio links.

In Belgium there is a restriction in outdoor use. The frequency range in which outdoor operation in Belgium is permitted is 2460 – 2483.5 MHz.

In France only channels 10,11,12 and 13 are available.

This device may not be used for setting up outdoor radio links in France. For more information see **http://www.anfr.fr/** and/or **http://www.art-telecom.fr**

- The equipment that you have purchased has required the extraction and use of natural resources for its production.

- The equipment may contain hazardous substances that could impact health and the environment.

- In order to avoid the dissemination of those substances in our environment and to diminish the pressure on the natural resources, we encourage you to use the appropriate take-back systems.

- The take-back systems will reuse or recycle most of the materials of your end life equipment in a sound way.

- The crossed-out wheeled bin symbol invites you to use those systems.

- If you need more information on the collection, reuse and recycling systems, please contact your local or regional waste administration.

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

All expressed and implied warranties for the Buffalo Technology (Melco 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/(Melco 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/(Melco 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 (Melco Inc.) does not offer refunds for any product.

@ 2003-2007 Buffalo Technology (Melco, Inc.)

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 Technology UK Ltd.
176 Buckingham Avenue,
Slough, Berkshire, SL1 4RD
United Kingdom

GENERAL INQUIRIES

Email: *sales@buffalo-technology.com*

TECHNICAL SUPPORT

Phone (UK only): 08712 50 12 60*
Phone: +353 61 70 80 50
Email: *helpdesk@buffalo-technology.ie*
*Calls cost 8.5p per minute

Technical Support Operating Hours
Monday - Friday (GMT)
9:00 AM - 6:00 PM Monday-Thursday
9:00 AM - 4:30 PM Friday

Thank you for your interest in Buffalo products. Our GPL software delivery policy is outlined below.

For each individual product and revision, please send one individually packaged self addressed padded CD shipping envelope, containing a blank CD-R to the following address:

Buffalo Technology USA Inc.
4030 W. Braker Lane Suite 120
Austin, TX 78759
Attn. GPL Department

Within the envelope containing the self addressed padded CD shipping envelope, please include a bank draft or money order for $20 (USD) (Made out to: Buffalo Technology) to cover our handling fee, postage and CD preparation. The CD-R should have the name of the product and revision number clearly written on the actual CD-R (not on the insert).

We do not send GPL source in bulk on a DVD. And order confirmation is not required by the GNU General Public License.

We are more than happy to comply with your request; however, we must ask you to comply with our GPL distribution policy, which complies with the GNU General Public License.

Sincerely,
Buffalo Technology GPL Department

Thank you for your interest in Buffalo products. Our GPL software delivery policy is outlined below.

For each individual product and revision, please send one individually packaged self addressed padded CD shipping envelope, containing a blank CD-R to the following address:

Buffalo Technology Ireland Ltd
Free Zone East, Shannon, Co. Clare
Ireland
Attn. GPL Department

Within the envelope containing the self addressed padded CD shipping envelope, please include a bank draft or money order for €20 (Euro) (Made out to: Buffalo Technology) to cover our handling fee, postage and CD preparation. The CD-R should have the name of the product and revision number clearly written on the actual CD-R (not on the insert).

We do not send GPL source in bulk on a DVD. And order confirmation is not required by the GNU General Public License.

We are more than happy to comply with your request; however, we must ask you to comply with our GPL distribution policy, which complies with the GNU General Public License.

Sincerely,
Buffalo Technology GPL Department

* When operating in High-Speed Mode, this Wi-Fi device achieves an actual throughput of up to 34.1 Mbps, which is equivalent to the throughput of a system following 802.11g protocol and operating at a signaling rate of 125 Mbps.

300 Mbps is the link speed when using Draft-N mode. It represents actual wireless data speeds, including overhead. Because the overhead is not available for user data transfer, usable wireless throughput will be substantially slower.