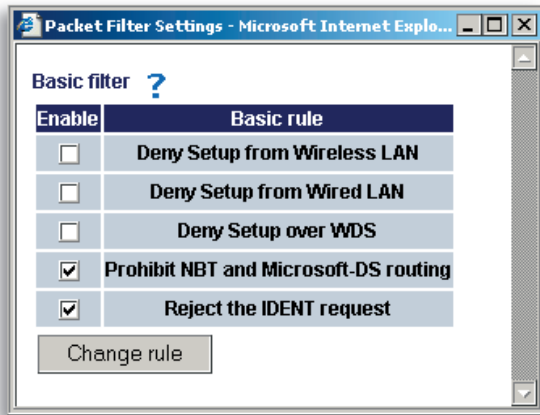


Basic Filter
Setting



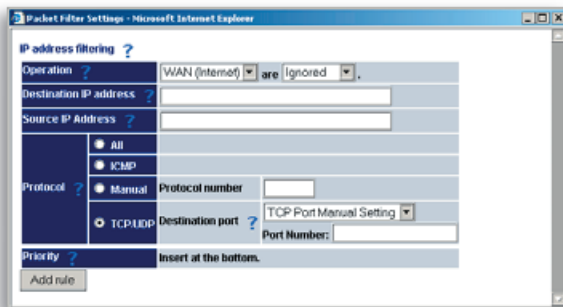
FTP and WEB.

* If IDENT requests are forwarded to a LAN side client by address translation setting (DMZ or TCP port :113), this basic rule is ignored.

IP Filter Settings - Up to 32 rules may be made to limit the type of packets allowed to pass between the WAN and LAN. Each rule may specify that packets meeting specific criteria (source or destination IP Address, Protocol, etc.) from either the WAN or the LAN are **ignored**, **rejected**, or **accepted**. You may choose that packets from the:

- WAN side (packets coming from the WAN side will be filtered)
 - LAN side (packets from the LAN side will be filtered)
- are:
- Ignored (stops the packet and does not route it)

IP Filter
setting



filtered, leave this box blank.

Warning: If administrator makes a rule that all packets from LAN are **Ignored** or **Rejected**, they will no longer have access to the AirStation configuration screens. This rule prohibits further setup from a wireless or wired computer. The AirStation can be returned to the factory default settings by holding down the INIT button on the back of the unit for five seconds or until the red DIAG light becomes solid.

Protocol - You may also choose to filter **all** protocols, **ICMP**, arbitrary **protocol number**, or **TCP/UDP** protocol number.

- **All** - Selects all IP protocols.

- **Rejected** (returns the rejected packet to the point of origin)
- **Accepted** (passes the packet through)

with each rule. You may also choose:

- **Destination IP Address** - The IP address to be filtered.
- **Source IP Address** - The IP address designated for filtering. If all IP addresses must be

- **ICMP** - Network Diagnostic Protocol (1).
- **Manual** - Enter protocol number (0-65535).
- **TCP/UDP Destination Port** - Select TCP or UDP, then enter port number.

Priority - Specify the priority an item. The smaller the number, the higher the priority.

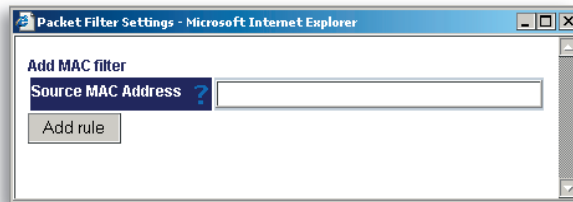
MAC Filter - Click Enter MAC filter to enter MAC address.

Source MAC address -The MAC address of the source of the packets that will be filtered may be set. Click Add rule when complete.

■ **Note:** If configuring from a wireless computer, add your MAC address to the list of authorized wireless LAN PCs. The MAC address must be in two-digit groups separated by colons.

Example: 00:40:26:00:11:22

Add MAC
Filter
setting



Click **Apply** when settings are complete.

Intrusion Detector

The Intrusion Detector guards against unauthorized access from the WAN (Internet). This function also records information on unauthorized access attempts

Intrusion Detector - Select **Disable**, **Enable**, or **Enable (Apply Packet filter setting for Intrusion Detector setting)**.

IP Spoofing - Check **Block** to prevent IP spoofing.

Threshold Value - Enter the number (1-999) of suspect packets to be received before the notification occurs.

Intrusion Detector Setup

The screenshot shows the 'Intrusion Detector Setup' window of a Buffalo AirStation. The left sidebar contains a navigation menu with options: LAN Settings, WAN Settings, Network Settings, Firewall Settings, Advanced Settings, Management, and Logout. The 'Intrusion Detector' option is selected. The main content area is titled 'Intrusion Detector Setup' and includes a description: 'Intrusion Detector detects and blocks unauthorized access or suspicious traffic coming from the Internet.' The settings are organized into sections: 'Basic Settings' (Intrusion Detector: On/Off, IP Spoofing: On/Off, Detection Value: 5), 'Email Alert Notification' (checkbox), and 'Pop-up notification' (checkbox). The 'Email Alert Notification' section includes fields for Local Address to Alert, Sender Email Address, SMTP Server Address, Hostname Email Server, SMTP Service Address, User Name, Password, and Confirm Password. The 'Pop-up notification' section includes a checkbox and a field for IP addresses for pop-up notification.

Basic Settings

Intrusion Detector: ☐ On/Off

IP Spoofing: ☐ On/Off

Detection Value: 5

☐ Email Alert Notification

Local Address to Alert:

Sender Email Address:

SMTP Server Address:

Hostname Email Server:

SMTP Service Address:

User Name:

Password: Confirm Password:

Send Mail:

☐ Pop-up notification

IP addresses for pop-up notification:

Notify by email:

Notification email address - Enter destination email address.

Sender email address - Enter the email address that will send the email. This is the name that will appear as the sender when the email is read. This email can be made up (e.g. DETECTOR@AIRSTATION).

Sender email server address - Enter the SMTP Server address.

Receiving email server authorization - Enter the POP3 Server address, User name and Password.
This is only required if your SMTP server requires POP verification before it allows email to be sent.
Consult your ISP or mail server support for more information.

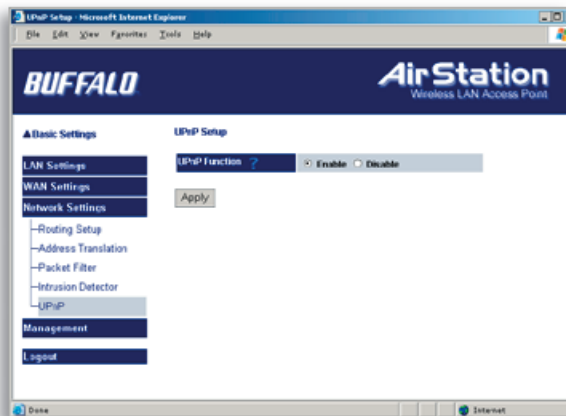
Send test - Click **Send** to test notification; this will also save and commit the entries.

Pop-up notification - Pop-up window alert of unwanted activity. Client Manager must be installed and running on a client machine to use this feature.

Destination IP address - Enter the IP address to be notified. The LAN computer with this IP address must have Buffalo's Client Manager software installed and running for the verification to occur. If the machine is off the verification will not be received, and the AirStation will NOT resend information.

Intrusion Detector information - displays log activity detected by the Intrusion Detector service.

UPnP
Setting



UPnP

Select **Enable** to enable UPnP (Universal Plug and Play). When a computer with UPnP support connects to the AirStation, that computer automatically receives configuration information from the AirStation.

System
Information



Management -

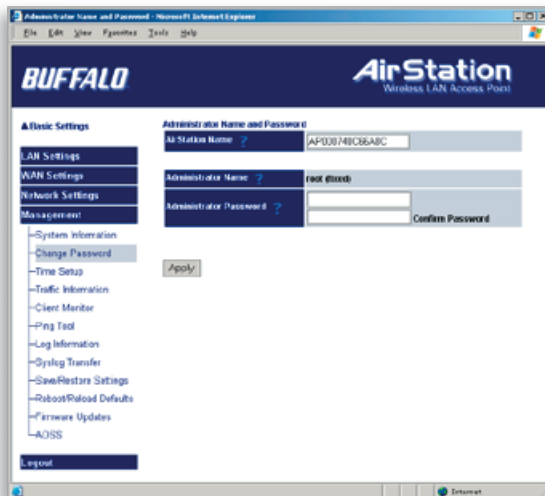
- **System Information** - System information of the AirStation is obtained here.
- **Model name** - Displays model and firmware version.
- **AirStation Name** - Displays AirStation host name.
- **DHCP Server function** - Displays whether DHCP is On or Off.
- **Wireless** - Displays such wireless LAN settings as wireless MAC address and wireless firmware. The wireless MAC address is required for setting up WDS with other access points. This is the best place to determine the wireless MAC address. If 125* Mbps AfterBurner mode is enabled, then the [AfterBurner]

color will be red or grey. When it is red, 125* Mbps AfterBurner is running. When it is grey, 125* Mbps AfterBurner is enabled but not running due to a client being connected at 54 Mbps or another access point is running on the same channel.

- **LAN** - Displays the AirStation LAN settings
- **WAN** - Displays the AirStation WAN settings

- **Default Gateway** - Displays the default gateway settings
- **WAN side IP address auto acquisition** - This acquires an IP address from the WAN (Internet) side DHCP server. Press **Release** to release current DHCP WAN information. Press **Renew** to obtain WAN information from the DHCP server. **NOTE:** If a manual IP is assigned to the WAN port, this feature is not displayed.

Name and
Password
Setup



alphanumeric characters (case sensitive).

Admin Name and Password

- **AirStation name** - When using multiple AirStations, select a unique name to make it easier to identify each AirStation through the AirStation Manager utility.
- **Administrator name** - "root"; cannot be changed.
- **Administrator password** - Allows the administrator to enter an administrator password to restrict access to the setting screens.
- **New Password** - Enter new password. Enter up to eight

- **Confirm Password** - Reenter the new password for confirmation.

Time Setup
Screen

Time setup

Time setup - Enter the current date and time, and click **Set**.

NTP - Network Time Protocol. Select **Use** or **Do not use**.

■ **Note:** If NTP is used, time is set automatically.

NTP server name - Enter the NTP server name.

Update Time - Enter the time interval (in hours) for the time check frequency.

Time Zone - Select local time zone.

Click **Apply**.

Packet Traffic Information

The screenshot shows the Buffalo AirStation configuration interface in a Microsoft Internet Explorer browser window. The page title is "Packet Traffic Information". On the left is a navigation menu with categories: "Basic Settings" (containing LAN Settings, WAN Settings, Network Settings, and Management), "System Information", "Change Password", "Time Setup", "Traffic Information" (which is currently selected), "Client Monitor", "Ping Tool", "Log Information", "Syslog Transfer", "Save/Restore Settings", "Reboot/Reload Defaults", "Firmware Updates", and "AOS". At the bottom of the menu is a "Logout" button. The main content area is titled "Packet Traffic Information" and displays a table of network statistics. The table has columns for the interface type, direction (Sent/Received), and packet counts (Packets, Error Packets). The data is as follows:

Interface	Direction	Packets	Error Packets
Wired WAN	Sent	32	0
	Received	0	0
Wired LAN	Sent	5126	0
	Received	8837	0
Wireless LAN	Sent	152	0
	Received	0	0

Below the table is a "Refresh" button. The browser's status bar at the bottom shows "Done" and "Internet".

Packet Traffic Information

Displays number of packets sent and received for:

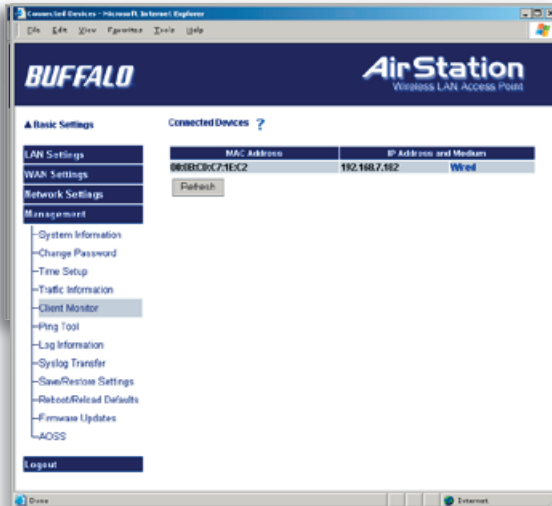
Wired WAN

Wired LAN

Wireless LAN

Click **Refresh** to update the transfer packet log.

Client
Monitor
Screen



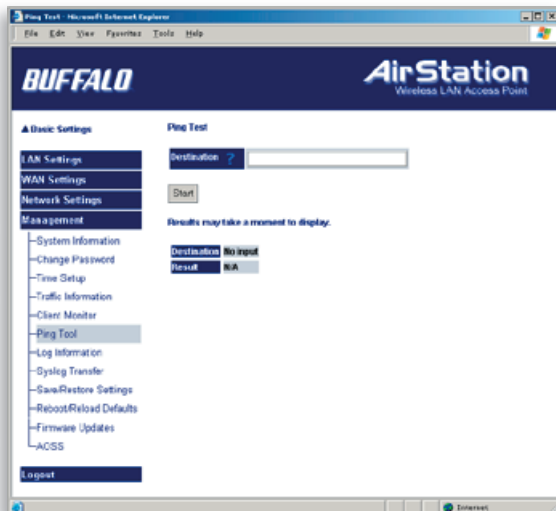
Client Monitor

Displays the wired and wireless clients (computers) that are accessing the AirStation.

- **MAC address** - Shows the client's MAC address.
- **IP Address and Medium** - Shows the IP address that is assigned to the client from the DHCP server. The network medium is shown as 'wireless' or 'wired' depending on how the client is accessing the AirStation.

■ Note: The Client Monitor only shows clients that have received an IP address from the AirStation's DHCP server. Clients that have static IP addresses will not appear in the Client Monitor.

PING Test



PING Test

Performs a PING test from the AirStation to a LAN or WAN address.

Enter the target IP address and click **OK** (e.g. **192.168.11.2** - OR- **www.buffalotech.com**)

If the test results in an error, then verify you correctly inputted the address and check your connections.

Log
Information
Screen



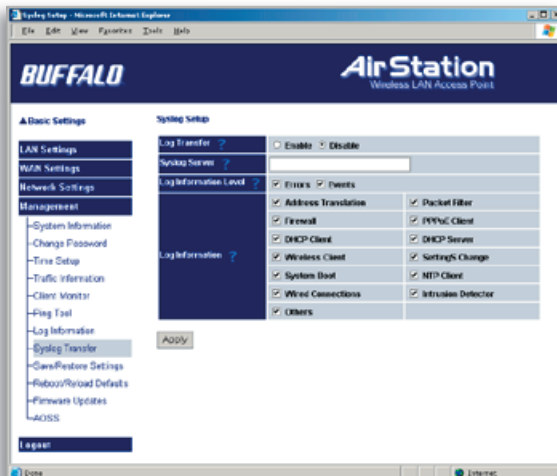
Log Information

Display log info level - Select **Error** and/or **Notify** to specify the types of reports to be logged by the AirStation.

Display log info - Select the specific reports to be logged.

Log information - Displays recorded logs.

Syslog
Transmitting
Screen



Syslog Transfer

Select **Use** or **Do not use** to enable or disable the AirStation's ability to transmit information to a Syslog server.

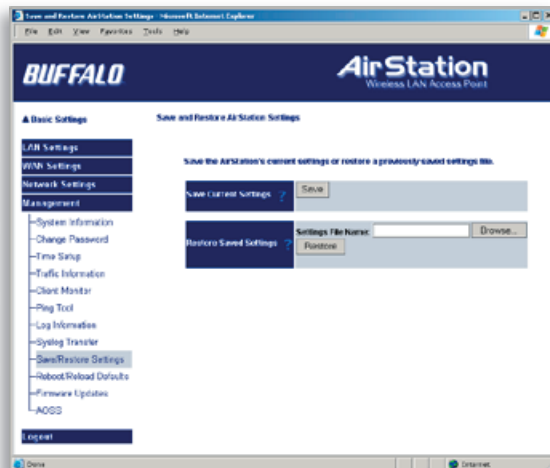
- **Syslog Server** - Enter the IP address of the Syslog server.

- **Log Information Level**
 - Select **Error** and/or **Notice** to specify the types of reports to be sent to the Syslog server.

- **Log Information** - Select the specific reports to be sent to the Syslog server.

■ **Note:** A server on the network running a Syslog service is required for this.

Save/
Restore
Settings
Screen



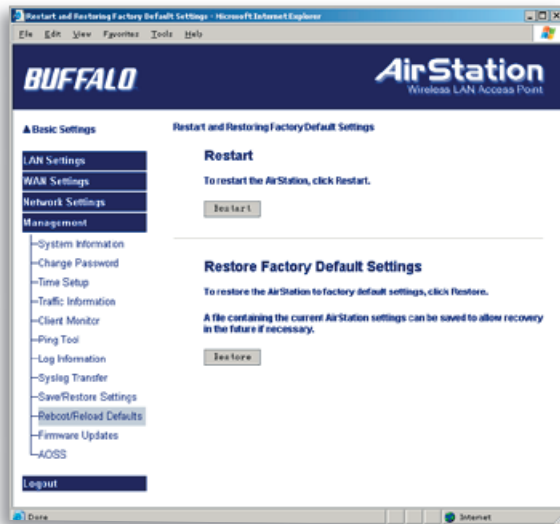
Save/Restore Settings

Save current settings - Click **Save** to open the file saving dialog and save the current AirStation settings to a file.

Restored saved settings
- Restores settings from a file that has been saved. Click **Choose file** to select the saved file and click **Restore**.

■ **Note:** If the setting file is saved by a newer firmware than the current one, the AirStation can't restore the settings.

Initialization/ Reboot



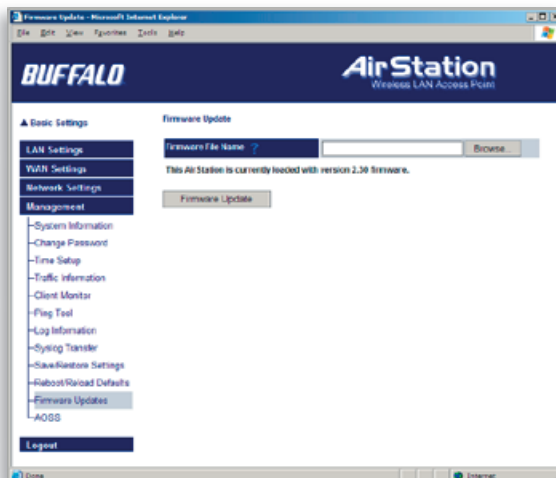
Reboot/Reload Defaults

Click **Restart** to reboot AirStation.

Click **Restore** to reset the AirStation to default factory settings.

■ **Note:** Resetting to default factory settings will erase all settings and passwords previously entered. The AirStation will return to the condition it was in when first purchased.

Firmware Update



Firmware Update

Firmware file name

- Click **Browse** to browse to the path and filename of the new firmware. Click Firmware Update to load firmware to the AirStation.

■ Note: Firmware update does not erase current user settings.

Please visit the Buffalo Technology Web Page to download the latest firmwares free of charge.

<http://www.buffalotech.com/wireless>

AOSS



Manually specify the encryption type - This forces AOSS to use a specified type of encryption. We recommend that you not change this setting. If the setting is changed, then every client that connects must support the specified encryption type.

AOSS Function - Click Enable to allow the AirStation to use AOSS. Click Disable to disable the AOSS system. button on the AirStation.

Start AOSS Process- Click AOSS icon to begin the AOSS sequence. This starts the AOSS process just like pressing the AOSS button.

Stop AOSS Process- Click AOSS icon to stop AOSS operation. Stopping the AOSS function will turn off AOSS and return the router to non-AOSS function.

Additional Information

For more information, please consult:

- The AirStation website at:

<http://www.buffalotech.com> - for frequently asked questions (FAQ's) and Software Updates.

WZR-HP-G54 BASE STATION SPECIFICATIONS

Physical Specifications

Dimensions W3 x H6.75 x D6.1in. (76 x 171 x 155mm)

Weight 1 lb. (620g)

Temperature & Humidity

Operation 0° to 40° C

Maximum humidity 80%

Transit/Storage 0° to 40° C maximum humidity 80% (no condensation)

Power Characteristics

Transmit Mode 1.1A (Nominal),

Power Supply 3.3 V

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.

Networking Characteristics

Compatibility

- IEEE802.11g/b Standard for Wireless LANs (125* High-Speed Mode also Available)
- Wi-Fi (Wireless Fidelity) certified by the Wi-Fi Alliance.

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)

Radio Characteristics

RF Frequency Band 2.4 GHz (2400-2483 MHz)

11 selectable channels (3 non-overlapping)

Modulation Technique Direct Sequence Spread Spectrum

- OFDM for High Transmit Rate
- DQPSK for Standard Transmit Rate
- DBPSK for Low Transmit Rate

Spreading 11-chip Barker Sequence

Nominal Output Power 25.0 dBm

Transmit Rate / Range

High Speed 54 Mbps (125* Mbps in 125* High-Speed Mode)

Medium Speed 36 Mbps (96 Mbps in 125* High-Speed Mode)

Standard Speed 2 Mbps

Low Speed 1 Mbps

Open Office Environment

160 m (525 ft.)

270 m (885 ft.)

400 m (1300 ft.)

550 m (1750 ft.)

Semi-Open Office Environment

50 m (165 ft.)

70 m (230 ft.)

90 m (300 ft.)

115 m (375 ft.)

Closed Office

25 m (80 ft.)

35 m (115 ft.)

40 m (130 ft.)

50 m (165 ft.)

Receiver Sensitivity -83 dBm -87 dBm -91 dBm -94 dBm (depends on data rate)

Delay Spread (at FER of <1%) 65 ns 225 ns 400 ns 500 ns (depends on data rate)

- The range of wireless devices can be affected by metal surfaces, solid high-density materials and obstacles in the signal path.

Table “Radio Characteristics” lists the typical ranges when used indoors:

- In Open Office environments, clients can “see” each other, i.e. there are no physical obstructions between them.
- In Semi-open Office environments, work space is separated by room dividers; client cards are at desktop level.
- In Closed Office environments, workspace is separated by floor-to-ceiling brick walls.

■ **Note:** The range values listed in Table “Radio Characteristics” are typical distances as measured at Buffalo Technology AirStation laboratories. These values are provided for your guidance but may vary according to the actual radio conditions at the location where the AirStation product is installed.

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.

B.1.1 LED Activity B

Monitoring LED activity helps identify problems.

- Power LED should be GREEN,
- Wireless LED should be GREEN if the line is active. If it is blinking GREEN, wireless communication is active.
- Ethernet LED should be GREEN (100Mbps) or AMBER (10Mbps) while the communication is active.

DIAG LED Activity

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

If any symptoms match section B.1.1, call the Buffalo Tech Support line 24 hours a day, 7 days a week at **866-752-6210** or email **info@buffalotech.com**.

Table B.1.1 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

B. 1.2 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 TCP/IP settings.

To add or change the 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 the 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 the parameters match the settings provided by your LAN Administrator. Make changes if necessary, and click OK.

5. When or if prompted, restart your computer.

B. 1.3 Other Problems

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

Troubleshooting WDS (Step-by-Step Instructions)

The most common issue with WDS installations is using the wrong MAC address. The proper MAC Address for the access points is the 'Wireless MAC Address'. The best place to document this is under the 'System Information' section of the configuration web page. For proper setup, please continue reading this document.

Problem:

Communication problems with WDS (wireless bridging/repeating).

Cause:

WDS is a very complex bridging system, and is not part of the 802.11b or 802.11g standards.

Restrictions:

Please verify that the following conditions are met (if just one condition is not satisfied, then WDS cannot be used on the wireless network):

1. All wireless access points in the wireless bridge need to be from the same vendor (e.g. all Buffalo access points).

(At time of publication, the Apple Airport Extreme WILL work in WDS with Buffalo G54 access points.)

2. No single access point can communicate with more than six other access points in the wireless bridge.

The following is a list of good practices with WDS:

1. Start the wireless bridge system with only two access points and then add more access points.
2. Setup all access points in the wireless bridge in close proximity before they are deployed to their proper location.
3. Only one access point in the wireless bridge should be serving DHCP and routing services unless a routed wired network exists.

Proper Setup:

Please follow the following steps to properly setup WDS.

1. It is recommended that all access points in the bridge are reset to their factory default settings. This is done by holding the INIT button on the rear of the access point down for 5-10 seconds.
2. Login to the first access point in the wireless bridge (this should be the DHCP server enabled access point if there is not already a routed wired network).
3. Click on the 'Advanced' button.
4. The wireless settings page will appear. Select the proper settings for the wireless network. Record all settings on a piece of paper. All settings except for the SSID need to be identical amongst all access points in the bridge. If roaming is desired, then make sure the SSID settings are identical as well. Press the 'Apply' button after any changes are made. If the IP address was changed, then reconnecting to the access point for configuration will require accessing it via its new IP address in a web browser (e.g. http://NEW_IP_ADDRESS).
5. Click on the 'LAN port' link on the left.

6. Check that the 'LAN side IP address' values are correct for your network, or leave them as default. Record the 'LAN side IP address'. Press the 'Apply' button if any settings on this page have been changed.
7. Click on the 'Management' link on the left.
8. The System Information page will appear. In the Wireless section of the table record the MAC address, including the colons (i.e. "00:00:0A:1B:2C:DF"). Please make sure the MAC address is recorded from the Wireless section and not the other sections.
9. Logout of the access point by clicking on the 'Logout' link on the left. Close the browser window.
10. Login to the second access point in the wireless bridge.
11. Click on the 'Advanced' button.
12. The wireless settings page will appear. Select the proper settings for the wireless network. Refer to the settings recorded from the first access point. All settings except for the SSID need to be identical for all access points in the bridge. If roaming is desired, then make sure the SSID settings are identical as well.
13. Click on the 'LAN port' link on the left.
14. Make sure that the 'IP address' for the 'LAN side IP address' setting is different from that of the first access point. The IP addresses cannot be the same, but they should be on the same network. It is recommended that the IP address of the second access point is one higher than that of the first access point. Thus, if access point one's address is 1.1.1.1, then access point two's address should be 1.1.1.2. If there is a 'DHCP server function' setting on this page, then make sure to set it to 'Disabled'. Press the 'Apply' button when finished.

15. Click on the 'Wireless bridge (WDS)' link on the left.
16. Enable the WDS function and press the 'Set' button.
17. Enter the Wireless MAC Address of the first access point (which was recorded on Step 8) into the field that say 'MAC Address of AirStation(Wireless)' (include the ':s'). Press the 'Add' button.
18. The Wireless MAC address inputted on the step above will appear in the 'Connected AirStation' table. Please check that the checkbox under enable is checked, and then press the 'Enable marked item' button.
19. At the top of the page, press the 'Apply' button.
20. Once the router has rebooted, click on the 'Management' tab on the left.
21. The System Information page will appear. In the Wireless section of the table record the MAC address (including the ':s'). Please make sure the MAC address is recorded from the Wireless section and not the other sections.
22. Logout of the access point by clicking on the 'Logout' link on the left. Close the browser window.
23. Login to access point one again.
24. Click on the 'Advanced' button.
25. Click on the 'Wireless bridge (WDS)' link on the left.
26. Enable the WDS function and press the 'Apply' button.
27. Enter the Wireless MAC Address of the first access point (which was recorded on Step 21) into the field that say 'MAC Address of AirStation(Wireless)' (include the ':s'). Press the 'Add' button.

29. At the top of the page, press the 'Apply' button.
30. Once the router has rebooted, click on the 'Management' tab on the left.
31. Click on the 'PING test' link on the left.
32. In the 'Destination' field enter the IP address of the second access point and press the 'OK' button.
 - a. If the 'Result' section of the table reports information like, "1st: 64 bytes from IP_ADDRESS" then the WDS bridge is effectively working.
 - b. If the 'Result' section of the table reports "Destination Host Unreachable", then an error has occurred during the setup.

WDS is a complicated bridging system with a lot of variables. If there are still problems with WDS configuration on the network, then please call our 24/7 technical support line at **1-866-752-6210**.

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 Cable: 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 con10BaseT 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.

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. SSID 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 programable 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.

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: 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.

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 infor-

mation 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 receives, strengthens and re-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.

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.

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

This product includes the following certification(s):



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:

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.

FCC RF 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.

BUFFALO declared that WZR-HP-G54 is limited in CH1~11 by specified firmware controlled in USA.

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

Buffalo Technology (Melco Inc.) products comes 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 Buffalo Technology (Melco, 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

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

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

©2005, Buffalo Technology (USA), Inc.