BUFFALO

User Manual for Professional Firmware

WHR-HP-G300N

AirStation NFINITI HighPower Router and Access point

WHR-HP-GN

AirStation Wireless N Technology HighPower Router and Access point

www.buffalotech.com

35011411 ver.01

1. Introduction

1.1. Welcome

This AirStation wireless router comes with two different firmware packages. You may use either the dd-wrt-based Professional firmware or the simple User-friendly firmware. By default, the Professional firmware is installed.

1.2. Device Configuration

From the factory, the router is configured as a network bridge. That means that all network interfaces can communicate with each other using this default bridge. The router is ready to use with a few simple adjustments.

1.2.1. Factory Settings

Because all interfaces are attached to the bridge by default, they all have the same IP configuration:

IP address	192.168.11.1
Subnet Mask	255.255.255.0
DHCP server	enabled
DHCP-Range	192.168.11.2 - 66

The Wireless LAN interface is activated by default with a SSID generated from the device's MAC address. For security, unused interfaces should be disabled. Wireless LAN interfaces that are not disabled should be configured with secure encryption (WPA2 or WPA is recommended) and a secure password.

1.2.2. Initial Operation

Connect your computer to the router with an Ethernet LAN cable and power the router on. It will take about 30 seconds to boot. You can then access it via telnet or web browser at the IP address 192.168.11.1. The DHCP server in the router is enabled by default. If your PC's Ethernet is configured for DHCP it should receive an IP address from the router's DHCP server. If not, please configure the Ethernet interface with an address from the 192.168.11.x subnet.

Because all relevant settings can be made using the web interface, this manual refers to configuration via the web GUI only.

2. Configuration via the Web Interface

The router contains an integrated web server that provides an easy to use web interface. It allows configuration, administration, and status checking in a simple but effective way.

When accessing the web GUI for the first time, change the default username and password. By default, the router's status page can be accessed without authentication, but this can be disabled.

The web interface was successfully tested on the following browsers:
- Internet Explorer 7.x and newer versions
- Firefox 2.x and newer versions
- Safari 2.x und newer versions

2.1. Preparation

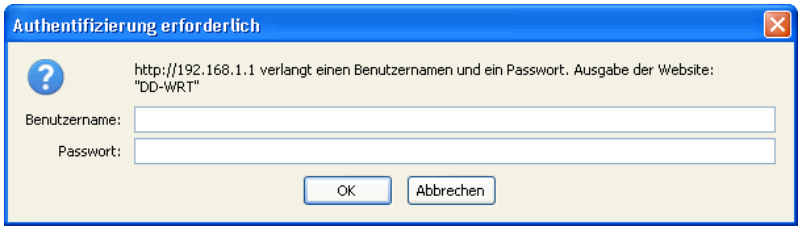
Connect your PC to the router and power the router on as described in 1.4.2. After the router has loaded its operating system, you can communicate with it via your LAN network interface.

The easiest way to test if your PC can communicate with the router is to ping 192.168.11.1.

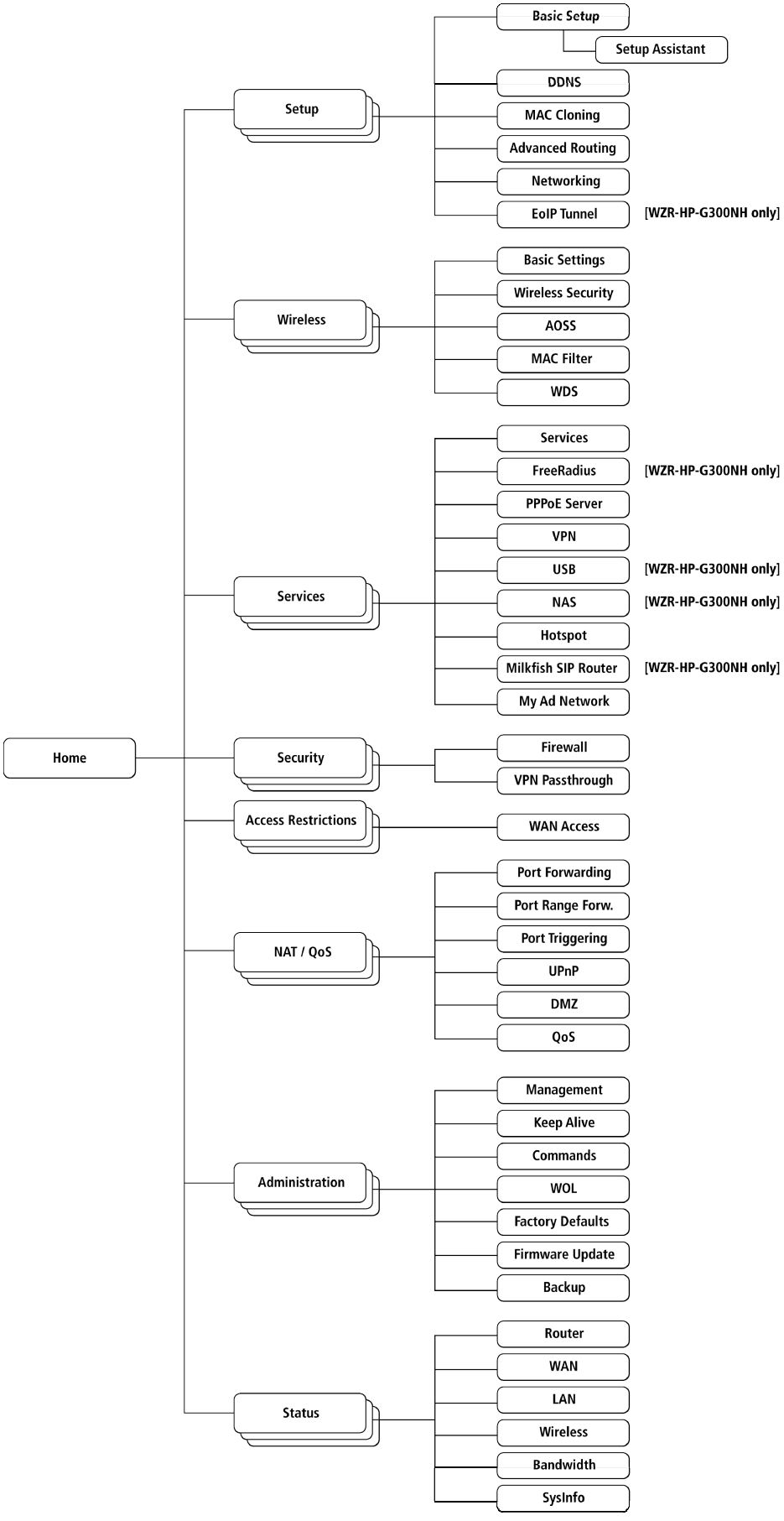
2.2. Web Interface Access

Open a browser window. Enter the address http://192.168.11.1 into the address bar. The status page will be displayed.

When you click on a tab, the login window will pop up. Enter the username and password you previously set.



2.3. Web Interface Structure



2.3.1. Setup

2.3.1.1. Basic Configuration

Setup Assistant
The setup assistant provides a step-by-step interface for basic router configuration. This configures most common settings automatically.

WAN Setup
Here you'll find the most important settings to configure your internet access and WAN port. DHCP is enabled by default, but you can also use PPPoE, PPTP, L2TP, static IP, or HeartBeat Signal. If you don't use a password to log in to your ISP, you may need to enter "0000" for the password. Also, for some ISPs you should not enter the service name, as it will prevent establishing the connection. If you experience connection problems, then leave the service name empty.

WAN Connection Type	Description
Disabled	The WAN port is disabled.
Static IP	A static IP address will be used – enter the IP address, subnet mask, gateway, and server manually.
Automatic Configuration - DHCP	The router obtains its WAN-side IP address from a DHCP server.
PPPoE	Configure as PPPoE-client. For VDSL, check the "VDSL-Tagging" box.
PPTP	Establishes connection via PPTP.
L2TP	Establishes connection via L2TP.
HeartBeat Signal	If you use a HeartBeat connection, consult your ISP for setup information. HeartBeat Signal is used only in Australia.
3G/UMTS [WZR-HP-G300NH only]	Configures Internet Access via 3G/UMTS. Enable USB in the "Services" section and attach a 3g/UMTS USB stick to the router.

Network Setup
Network Setup configures the router's basic settings to match the local network. By default these settings are valid for all network ports except the WAN because they are all attached to the default bridge. If ports are disassociated from the bridge they will have different settings.

2.3.1.2. Dynamic DNS (DynDNS or DDNS)

Dynamic DNS allows the assignment of a DNS record to a dynamically assigned WAN-side IP address. A DynDNS client updates DNS records when your WAN-side IP address changes.

The router's firmware offers presets for the most common DynDNS services plus an option to define individual settings.

DynDNS Service	Description
Disabled	Default, no DynDNS
DynDNS.org	
freedns.afraid.org	
ZoneEdit.com	
No-IP.com	
3322.org	
easyDNS.com	
TZO.com	
DynSIP.org	
Custom	Individual DynDNS service configuration

2.3.1.3. MAC Address Cloning

MAC address cloning lets you assign a different MAC address to the router than the one encoded in the hardware.

2.3.1.4. Advanced Routing

Operating Mode
The default operating mode of the router is *Gateway*. Other routing protocols are available.

Modus	Description
Gateway	Gateway (default)
BGP	BGP Routing
Rip2 Router	Rip2 Routing
Router	Router

Static Routing
The Static Routing section lets you add static routes. The input parameters are equivalent to the parameters of the Linux command "route".

2.3.1.5. Networking

The Networking section allows detailed network configuration.

VLAN Tagging
Use this option to configure VLAN tagging.

Bridging
By default, one bridge (br0) is defined and active. In this section you can define additional bridges and change the interface assignment according to your requirements.

Bonding

Bonding offers the ability to "bond" interfaces together. Bonding can be used to enhance throughput or provide failover capabilities.

Port Setup
The port setup section allows further configuration of the routers network interfaces. Network interfaces can be separated from the bridge and it is possible to assign separate network settings for each interface. If an interface is separated from the bridge, add routing rules to allow communication between the interface and the bridge or other unbridged interfaces.

DHCPD
Besides the default DHCP server, you can define additional DHCP servers.

2.3.1.6. EoIP Tunnel [WZR-HP-G300-NH only]

EoIP (Ethernet over IP) tunnels can transport Ethernet data packages via a tunnel over existing IP connections. You can define up to 10 tunnels that can also be bonded.

2.3.2. Wireless

2.3.2.1. Basic Settings

Each Wireless LAN interface has its own section in the wireless basic settings screen. The wireless interfaces are labelled ath0 and ath0.1 – ath0.4 depending on the number of radios installed. To correctly identify the antenna connectors, please compare the MAC addresses printed on the enclosure with the addresses displayed in the web interface.

Wireless Mode
This parameter is used to define the operating mode of the Wireless LAN interface. You can select among the following modes:

Modus	Description
AP	WLAN Access Point mode (default)
Client	WLAN Client mode
Client-Bridge	Client-Bridge mode allows connecting to another Wireless LAN access point and establishing a network bridge with that access point
AdHoc	AdHoc operating mode, required for building mesh networks
WDS Station	WDS Station is the client in a WDS-AP <-> WDS station bridge. This is a special wireless networking mode that offers better flexibility and security than the classical MAC address based WDS.
WDS AP	WDS AP is the AP side for WDS AP <-> WDS Station. A WDS AP allows connections from WDS Stations and Wireless Clients.

Wireless Network Mode
Defines the IEEE802.11 networking mode.

Mode	Description
Disabled	Interface is disabled
Mixed	2.4 GHz 802.11b / 802.11g / 802.11n mixed mode
B-Only	2.4 GHz 802.11b mode (802.11g and 802.11n devices cannot connect)
G-Only	2.4 GHz 802.11g mode (802.11b, and 802.11n devices cannot connect)
BG-Mixed	2.4 GHz 802.11b & 802.11g mixed mode (802.11n devices cannot connect)
NG-Mixed	2.4 GHz 802.11n & 802.11g mixed mode (802.11b devices cannot connect)
N-Only (2.4 GHz)	2.4 GHZ 802.11n mode (802.11a, 802.11b, and 802.11g devices cannot connect)

Channel Width
Some wireless network modes support wireless channel widths besides the standard 20 MHz. 802.11g & 802.11n offer the option to use 40 MHz channels for enhanced throughput. Both the AP and the client must support 40 MHz channels to use them.

Wireless Channel (AP only)
Set the desired wireless channel, or let the router choose a free channel automatically. If the router is in classic WDS (MAC address based) mode, then the wireless channel must be selected manually.

Wireless Network Name (SSID)
The name of the wireless network the radio transmits or connects to (depending on the wireless mode)

Wireless SSID Broadcast (AP only)
The name of the wireless network (SSID) may be broadcasted or not. This does not prevent the network from being detected by a wireless network sniffer; it just hides the name.

Advanced Settings
Check this box to get access to advanced wireless settings. These advanced parameters should be only modified by experienced users.

2.3.2.2. Wireless Security

Because wireless data packets can easily be sniffed, wireless connections require a greater level of security to ensure that data cannot be read by unauthorized users.

Security Mode

Mode	Description
Disabled	No encryption set (not recommended!)

WPA Personal	WPA encryption with a passphrase (text password)
WPA Enterprise (AP only)	WPA encryption with Radius Client authentication according to 802.1x
WPA2 Personal	WPA2 encryption with a passphrase (text password)
WPA2 Enterprise (AP only)	WPA2 encryption with Radius Client authentication according to 802.1x
WPA2 Personal Mixed	WPA & WPA2 encryption in WPA/WPA2 mixed mode with a passphrase (text password)
WPA2 Enterprise Mixed (AP only)	WPA & WPA2 encryption in WPA/WPA2 mixed with Radius Client authentication according to 802.1x
RADIUS	
WEP	WEP 64 Bit / 128 Bit encryption (insecure; not recommended!)
802.1x (Client only)	Client side mode to connect to AP's working with WPA Enterprise Modes via RADIUS authentication

When using WEP encryption (not recommended), the user can choose between 64 bit and 128 bit keys. Keys can be entered as passphrases that are used to generate the Hex keys. Theoretically 128 bit keys offer a higher level of security but because of design flaws, that's not the case in actual use.

Key length	Description
64 Bit (10 Hexadecimal characters)	Standard
128 Bit (26 Hexadecimal characters)	

With WPA or WPA2 encryption, there are several encryption algorithms to choose from. AES is more secure but TKIP is more widely supported. There is also a TKIP + AES setting, but that does not offer more security than TKIP.

Algorithm	Description
TKIP	TKIP encryption, supported by most clients devices
AES	AES encryption offers a better level of security but might not be supported by a number of client devices and requires less cpu processing power.
TKIP + AES	Mixed mode – offers best compatibility but doesn't work in all environments

If RADIUS security is used, the MAC address format has to be set accordingly.

RADIUS MAC format options	Description
aabbcc-ddeeff	Standard
aabbccddeeff	
aa:bb:cc:dd:ee:ff	
aa-bb-cc-dd-ee-ff	

2.3.2.3. AOSS

AOSS (AirStation Onetouch Secure Setup) is Buffalo Technology's system to automatically connect wireless clients to an access point. AOSS can only be used in AP mode.

Enable AOSS
Enables the AOSS Service. When disabled AOSS cannot be used.

Start AOSS Negotiation
To initiate the AOSS process you can either click the AOSS button in the GUI or hold down the AOSS button on the front of the router for 3 seconds.

Security Modes
You may choose which security modes are offered in the AOSS negotiation process. The use of WEP in general is not recommended due to security concerns.

2.3.2.4. MAC Filter

The MAC Filter defines a list of client MAC addresses that are allowed to connect wirelessly. MAC addresses that aren't on the list aren't allowed to connect.

2.3.2.5. WDS

Wireless Distribution System (WDS) is a special access point mode that allows the connection of several access points to form a combined network. Such a network can be used to extend wireless network coverage.

The MAC addresses of the access points nearest to the current access point are entered as WDS nodes. Avoid creating "double" connections, i.e. A <-> B + A <-> B <-> C. These modes are available to connect WDS nodes:

WDS Client Mode	Description
disabled	Standard
Point-to-Point	Commonly used mode
LAN	

If WDS is enabled, then WDS NAT modes are also available.

WDS NAT Mode	Description
WLAN -> WDS	Standard
WDS -> WLAN	

2.3.3. Services

2.3.3.1. Services

The services section allows the configuration of basic service settings. Telnet and SSH can be configured this way. Remote access options are configured in the *Administration* section.

Available DHCP Server Domains	Description
WAN	Standard
LAN / WLAN	

Rflow / MACupd Interface Options	Description
LAN & WLAN	Standard
LAN	
WLAN	

2.3.3.2. FreeRadius [WZR-HP-G300NH only]

Certain applications (for example, Chillispot hotspot software) benefit from a RADIUS server for management of user credentials and settings.

Server Certificate
This section contains the parameters to generate the RADIUS server certificate. The certificate needs to be generated before clients can be configured to connect to the RADIUS server.

Certificate Status
Displays the server certificate creation status.

Settings
Choose the port that the RADIUS server uses for client communication. The default port is 1812.

Clients
This section is used to define RADIUS clients (required for HotSpot usage).

Users
Lists the users defined in the RADIUS servers. Allows creation and modification of accounts.

2.3.3.3. PPPoE Server

Some applications require a PPPoE server on the router, which can be configured here. The PPPoE server is disabled by default.

2.3.3.4. VPN

The router can also be configured as VPN server or VPN client.

PPTP

When defining the PPTP server's IP range, avoid overlap with the range of IP addresses handed out by DHCP if DHCP is enabled. The IP range is defined using the following syntax:

xxx.xxx.xxx.<start-ip>-<end-ip>

for example

192.168.1.20-30

Enter client login data follows:

<username> * <password> *

for example

testuser * test *

The encryption options can be set as follows

PPTP server type	Settings
DD-WRT Router	mppe required (Standard)
Windows PPTP Server	mppe required,no40,no56,stateless *or* mppe required,no40,no56,stateful

OpenVPN [WZR-HP-G300NH only]

OpenVPN is a powerful and flexible VPN solution. OpenVPN security is based on certificates that cannot created on the router itself. Please refer to OpenVPN's online documentation for instructions on creating certificates and configuring OpenVPN.

2.3.3.5. USB [WZR-HP-G300NH only]

The router's USB port can be used for several purposes. Here the basic and advanced USB parameters are defined. Besides enabling USB and defining the USB hardware standard to use you can also define if printer and storage support for USB shall be enabled.

2.3.3.6. NAS [WZR-HP-G300NH only]

If USB hard drive support is enabled, you can start the integrated ProFTPd server to share data on an attached hard disk via FTP.

The User/Password data are entered as follows:

<username> * <password> *

for example

testuser * test *

Be careful enabling anonymous login. If anonymous login is enabled, everybody accessing your network has permission to read and write data.

2.3.3.7. Hotspot

Most hotspot software requires a server to store user settings and login information. Please note that Sputnik is a commercial hotspot service that requires an agreement with Sputnik for usage.

2.3.3.8. Milkfish SIP Router [WZR-HP-G300NH only]

This package is an implementation of the Milkfish SIP router.

2.3.3.9. My Ad Network

Allows the creation of an AnchorFree Hotspot that can be used to create revenue via AnchorFree.

2.3.4. Security

2.3.4.1. Firewall

Aside from enabling and disabling the firewall, you can also set additional filters, block certain network requests for the WAN interface, and manage logs.

2.3.4.2. VPN Pass-through

VPN settings effect how the firewall handles IPSec, PPTP, and L2TP connections. By default, pass-through is enabled. Please note that disabling pass-through will usually prevent you from establishing VPN connections from computers located in your local network to VPN servers on the internet.

2.3.5. Access Restrictions

2.3.5.1. WAN Access

The WAN access settings allow the definition of time and service related access rules.

2.3.6. NAT / QoS

2.3.6.1. Port Forwarding

Port forwarding allows the assigning of WAN ports to specific internal IP addresses and matching ports. Bidirectional external traffic can be

forwarded to specific internal devices and computers. Each port forwarding entry defines a source port and a target IP address.

Before adding or removing a port forwarding entry, save all changed settings. Any changes not saved will be lost when a port forwarding entry is added or deleted.

2.3.6.2. Port Range Forwarding

Port range forwarding works similarly to port forwarding. Unlike port forwarding, instead of a single port, a range of ports is forwarded to the same range of ports at the internal target IP address.

2.3.6.3. Port Triggering

Port triggering is a kind of port range forwarding where outgoing traffic on specific ports enables previously defined port forwards for the activating device. This temporarily opens required ports when specific applications are opened on computers on the LAN. This offers a greater level of security than port forwarding or port range forwarding because the ports are only opened when needed.

2.3.6.4. UPnP

UPnP allows UPnP capable applications and devices to open and close required ports automatically as needed. This is simple to use and does not require further configuration steps.

2.3.6.5. DMZ

A DMZ computer is a special computer in the internal network that gets all incoming traffic forwarded. The task of that computer is managing this traffic. When the DMZ feature is activated the internal firewall is activated. This can pose a security issue if not handled with care. Furthermore, several services of the router, that have to be accessible from the WAN side, will not work because the associated traffic is forwarded to the DMZ computer.

2.3.6.6. QoS

QoS (Quality of Service) is a procedure to prioritise network traffic by application. Specific services can be assigned specific bandwidth.

Aside from upstream and downstream bandwidth, you can define settings for specific services and IP and MAC address ranges.

2.3.7. Administration

2.3.7.1. Management

The Management section contains settings for remotely accessing the router and other basic settings that are usually not changed. The settings for the language used in the Web GUI are also located here. You may choose between Chinese (simplified & traditional), Dutch, French, German, Hungarian, Italian, Japanese, Polish, Portuguese, Slovenian, Spanish, and Swedish. The default setting is English.

Before using Telnet or SSH, activate the associated service(s) in this section.

2.3.7.2. Keep Alive

Keep-Alive lets you configure monitoring options that automatically reboot the router if a service malfunction causes it to fail to respond.

2.3.7.3. Commands

Entering Linux commands is one of the most powerful ways to access the router's functionality. This enables you to access services and configure options that are not accessible via the Web GUI. Using shell commands can lead to unexpected results. Use them with utmost care.

Aside from executing the shell commands directly you can also save custom start up and firewall scripts.

2.3.7.4. WOL

With Wake-on-LAN, you can send special data packets to compatable devices on your LAN, causing them to exit sleep mode.

WOL data packets can be triggered manually or scheduled automatically.

2.3.7.5. Factory Defaults

With this feature you can reset the router's settings to factory defaults. After a reset, the router will restart.

2.3.7.6. Firmware Upgrade

The firmware upgrade option can be used to install a different firmware version. When doing this you can choose if the router's settings will be restored to factory defaults or kept.

2.3.7.7. Backup

You can use this feature to store your current configuration into a backup file, or to restore from a previously stored configuration. This also makes it simple to set up a number of routers with the exact same configuration.

2.3.8. Status

2.3.8.1. Router

The status screen displays information about the router, such as cpu load, memory consumption, and currently active IP connections. Status is updated automatically.

2.3.8.2. WAN

If the WAN interface is enabled, this screen displays WAN settings and throughput statistics.

2.3.8.3. LAN

Here you can find LAN-related information like active clients and DHCP clients.

2.3.8.4. Wireless

The wireless LAN status screen displays the current wireless LAN interface configuration, wireless LAN clients (in AP modes), and access points (in client modes). If there's more than one wireless LAN interface, you can switch between them via the interface pull down menu.

2.3.8.5. Bandwidth

Bandwidth monitoring displays real time diagrams for incoming and outgoing traffic for each network interface.

2.3.8.6. SysInfo

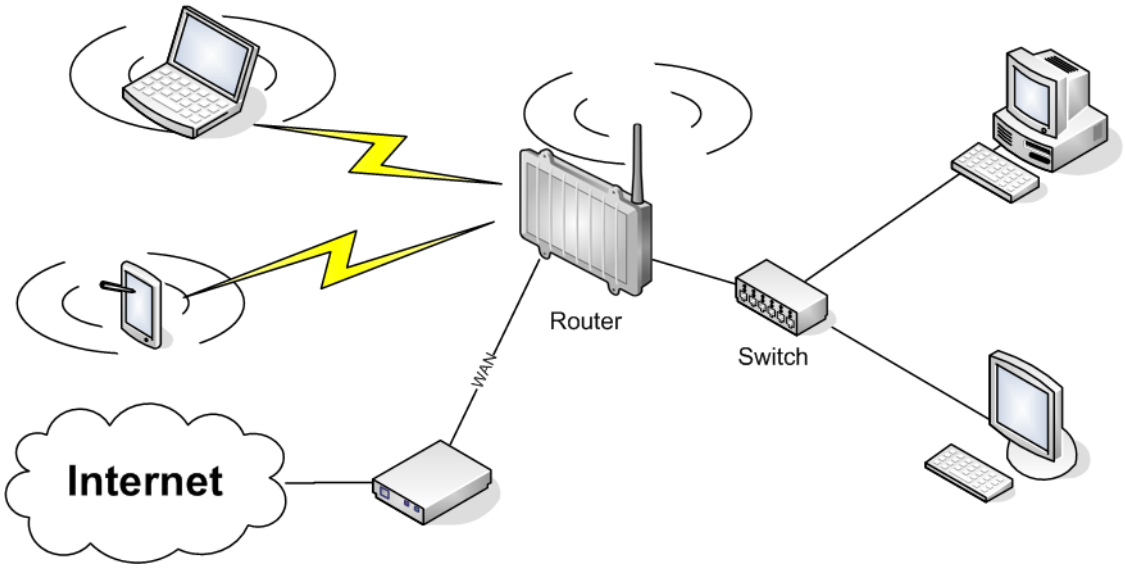
The SysInfo screen combines the most important information of the other status pages. By default, the SysInfo page can be accessed from LAN devices without authentication. That can be changed in the *Management* section of the *Administration* area.

3. Use Cases

The following use cases relate to the most commonly used router configurations. The related router configuration is explained step by step.

3.1. Access Point

Access Point (AP, sometimes also called "Infrastructure Mode") is the mode where the router is also the central wireless hub that connects to the LAN and provides access to wireless devices. These wireless clients of the AP can communicate with each other and with wired devices on the network such as the Internet.



Connect your computer to the router as described in 2.1. and access the web interface according to 2.2.

3.1.1. Access Point with NAT / DHCP

Setup -> Basic Setup

- *WAN Setup*
  - In "Connection Type", choose the type of WAN connection you want to use and complete the related settings.
- *Network Setup*
  - Enter the desired LAN IP address for the router into "Router IP".
  - Set "DHCP Type" to "DHCP Server" (this is the default).
  - "Enable" DHCP Server (this is the default).
  - Adjust the DHCP address range to match your requirements.
- *Time Settings*
  - Choose your time zone.
- Click "Save".

Wireless -> Basic Settings

- Enter your country in "Regulatory Domain"
- In the "Antenna Gain" field, please enter the gain of the antenna on your router. The firmware will adjust the transmit power accordingly to meet regulatory requirements. Please keep in mind that very long cables can dampen the HF signal thus reducing the usable antenna gain.
- Configure "Wireless Mode" to "AP"
- Set your desired wireless mode in "Wireless Network Mode". Please note that mixed modes will lead to reduced performance because of maintaining compatibility.
- Enter a name for your wireless network into "Wireless Network Name (SSID)"
- Click "Save"

Wireless -> Wireless Security

- Choose and configure a security mode. Please note that WEP is insecure and should only be used if no other option is available.
- Click "Apply Settings"

You can now connect the router to the Internet and your local network. After you successfully connect wireless devices, they will then be displayed on the "SysInfo" and "WLAN Status" pages.

3.1.1. Access Point attached to a network / Internet gateway

Setup -> Basic Setup

- *WAN Setup*
  - For "Connection Type", choose "Disabled".
- *Network Setup*
  - Enter the desired LAN-side IP address for the router into "Router IP".
  - Set the "DHCP Type" to "DHCP Server" (this is the default).
  - "Disable" "DHCP Server".
- *Time Settings*
  - Choose your time zone.
- Click "Save".

Wireless -> Basic Settings

- Enter your country in "Regulatory Domain"
- In the "Antenna Gain" field, please enter the gain of the antenna on your router. The firmware will adjust the transmit power accordingly to meet regulatory requirements. Please keep in mind that very long cables can dampen the HF signal thus reducing the usable antenna gain.
- Configure "Wireless Mode" to "AP"
- Choose a wireless mode in "Wireless Network Mode". Please note that mixed modes will lead to reduced performance because of maintaining compatibility.

- Enter a name for your wireless network into "Wireless Network Name (SSID)".
- Click "Save".

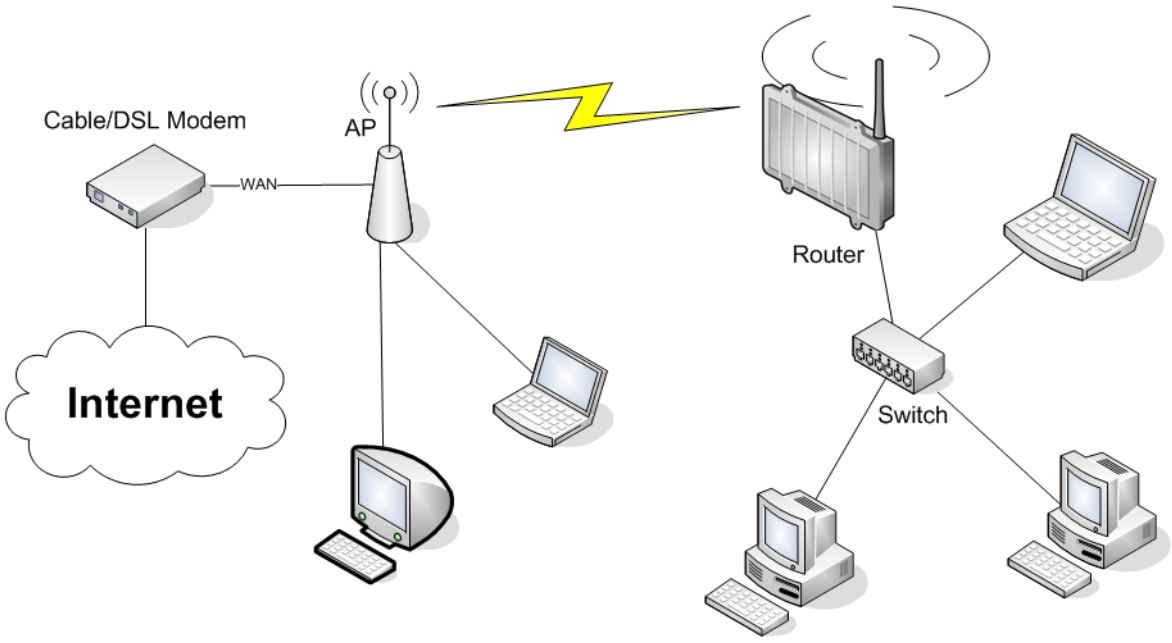
Wireless -> Wireless Security

- Choose and configure your desired security mode. Please note that WEP is insecure and should only be used if no other option is available.
- Click "Apply Settings"

You can now connect the router to the Internet and your local network. If you're running a DHCP server in your LAN, connected wireless devices will get their IP addresses from the server.

3.2. Wireless Client

The router can be also used as a wireless LAN client. This can be useful if you want to connect devices to your wireless LAN that do not have a wireless LAN interface. In this configuration, the wireless LAN interface acts as a wireless client. Attached wired Ethernet devices can also access the WAN through the wireless connection.



Setup -> Basic Setup

- *WAN Setup*
  - Set "Connection Type" to "DHCP" to have the AirStation get its IP address from a DHCP server, or to a "Static IP" if no DHCP server is available.
- *Network Setup*
  - Enter the desired LAN-side IP address for the router in "Router IP".
  - Set the "DHCP Type" to "DHCP Server" (this is the default setting).
  - "Enable" "DHCP Server" (this is the default setting).
  - Adjust the DHCP address range to match your requirements.

- *Time Settings*
  o Choose your time zone.
- Click "Save".

Wireless -> Basic Settings

- Enter your country in "Regulatory Domain"
- In the "Antenna Gain" field, please enter the gain of your AirStation's antenna. The firmware will adjust the transmit power automatically to meet regulatory requirements. Please note that the use of a long extension cable for your antenna will reduce the usable antenna gain.
- Configure "Wireless Mode" to "Client".
- Configure "Wireless Network Mode" to match the capabilities of the access point you want to connect to.
- Enter the network name (SSID) of the AP you want to connect to into "Wireless Network Name (SSID)".
- Click "Save".

Wireless -> Wireless Security

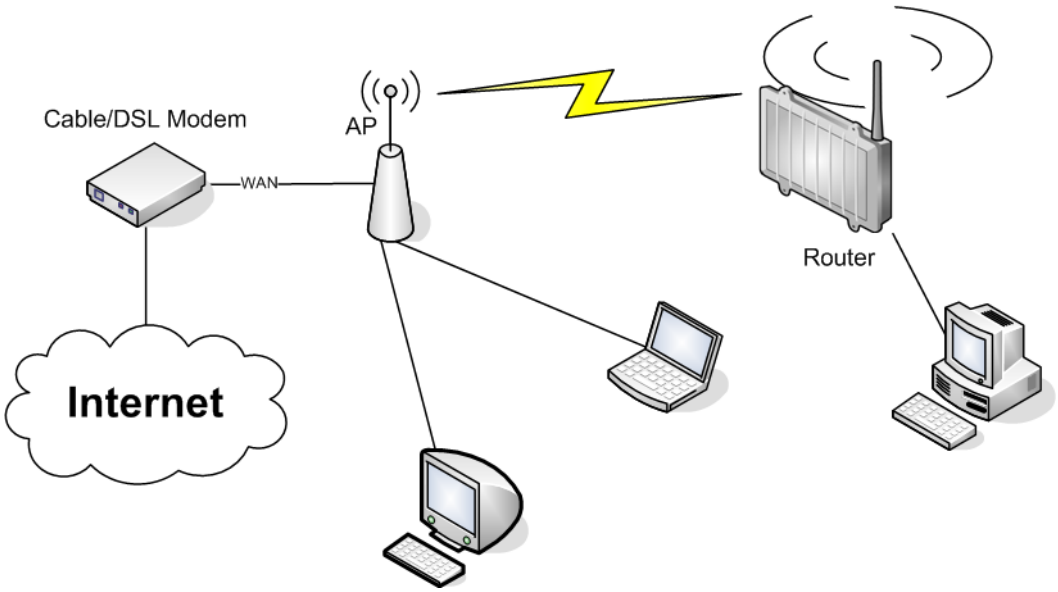
- Configure the security mode to match the security settings of the access point you want to connect to.
- Click "Apply Settings".

After the router reboots, please confirm that it has connected to the access point. If there is a DHCP server available on the access point side, and the router is configured to request an IP address, then it should receive an IP address for its WAN-side interface.

You can now either connect wired clients to the access point or configure another wireless network interface as an access point to grant access to wireless clients.

3.3. Wireless Client Bridge

A wireless client bridge offers the ability to transparently integrate the router's LAN into a different LAN that another access point is connected to. Clients connected to such a router can access devices in both LANs and vice versa. In that configuration the router's WAN interface is disabled.



Setup -> Basic Setup

- *WAN Setup*
  - Choose "Disabled" for "Connection Type" (this will be set automatically).
- *Network Setup*
  - Enter the desired LAN-side IP address for the router into "Router IP".
  - "Disable" "DHCP Server".
- *Time Settings*
  - Choose your time zone.
- Click "Save".

Wireless -> Basic Settings

- Enter your country in "Regulatory Domain".
- In the "Antenna Gain" field, please enter the gain of your AirStation's antenna. The firmware will adjust the transmit power automatically to meet regulatory requirements. Please note that the use of a long extension cable for your antenna will reduce the usable antenna gain.
- Configure "Wireless Mode" to "Client Bridge".
- Set "Wireless Network Mode" to match the access point you want to connect to.
- Enter the network name (SSID) of the AP you want to connect to.
- Click "Save".

Wireless -> Wireless Security

- Configure security to match the security settings of the access point you want to connect to.
- Click "Apply Settings".

After the router reboots, please confirm that it has connected to the access point. If there is a DHCP server available on the access point

side, a pc in the router's LAN configured to request an address from DHCP should receive an IP address.

4. License information

Die Firmware, die in diesem Produkt verwendet wird, beinhaltet Software, die der GNU Public Licenz (GPL) bzw. der GNU Lesser Public License (LGPL) unterliegt. Soweit im Rahmen der GPL und der LGPL anwendbar sind die Bedingungen der GPL und der LGPL sowie die diesbezüglichen Quellcodes vom Hersteller verfügbar. Der der GPL bzw. der LGPL unterliegende Code der Software wird bereitgestellt, ohne dass sich daraus Gewährleistungs- oder Haftungsansprüche ableiten lassen. Weitere Details entnehmen Sie bitte den Bedingung der GPL bzw. der LGPL.

4.1. GNU General Public License

Version 2, June 1991

4.1.1. Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

4.1.2. GNU General Public License - Terms and Conditions or Copying, Distribution and Modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for non-commercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

4.1.3. NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND,

EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

User Manual for User-friendly Firmware

WHR-HP-G300N

AirStation NFINITI HighPower Router and AccessPoint

WHR-HP-GN

AirStation Wireless N Technology HighPower Router and Access point

www.buffalotech.com

35011344 ver.01

Contents

Chapter 4 Configuration 26

Chapter 1
Introduction

Installing Your AirStation

To install your AirStation, insert the software CD from your package into your computer and follow the directions on the screen. For more infomation about installation, turn to chapter 3 of this manual.

Professional or User-friendly?

This AirStation wireless router comes with two different firmware packages. You may use either the dd-wrt-based Professional firmware or the simple User-friendly firmware. By default, the Professional firmware is installed. Turn to page 23 for instructions on switching between the two firmware packages.

Note : Most of this manual documents the User-friendly firmware. For more information on the dd-wrt-based Professional firmware, consult the help files in its web-based configuration interface or go to ***www.dd-wrt.com/wiki***.

Features

Supports IEEE802.11n and IEEE802.11b/g

With support for Wireless-N, Wireless-G, and Wireless-B standards, the AirStations can transfer data to and from all standard 2.4 GHz wireless clients. The WHR-HP-GN is a single stream, single antenna version, while the WHR-HP-G300N is a dual stream, dual antenna version, with faster Wireless-N performance.

Dual speed mode

Dual speed mode makes wireless transmission faster by using 2 channels, allowing 300Mbps transmission.

Support for AOSS and WPS

Both AOSS (AirStation One-touch Secure System) and WPS (Wi-Fi Protected Setup) are supported. These automatic connection standards make connection with compatible wireless devices easier.

Security Features

The AirStations are equipped with the following security features:

- AOSS
- WPS
- WPA-PSK (TKIP/AES)
- WPA2-PSK(TKIP/AES)
- WPA/WPA2 mixed PSK
- WEP(128/64bit)
- Privacy Separator
- MAC filtering
- Stealth SSID
- Firewall with easy rules

Automatic Channel Selection

Monitors wireless interference and automatically assigns the clearest, best channel.

Roaming

You can use multiple AirStations to cover a large area. Wireless clients can automatically switch AirStations for the best signal.

Initialization

To restore settings back to the factory defaults, hold down the Reset button on the bottom of the unit.

Browser Based Administration

These units can be easily configured from a password-protected web page though a browser on your computer.

Auto Mode (Router/Bridge Automatic Recognition)

Auto mode detects whether your network has a router or not and automatically switches to the appropriate router or bridge mode. You can also manually switch between modes.

Air Navigator CD Requirements

The AirStation wireless router and access point works with most wired and wireless devices. The automatic installation program on the CD requires Windows 7, Vista, or Windows XP to run. Client Manager software is included for Windows 7, Vista, and XP. The use of other operating systems may require that the AirStation be manually configured from a browser window.

300/150 Mbps High Speed Mode

With Wireless-N connections, 300 Mbps is the maximum link speed for the WHR-HP-G300N and 150 Mbps is the maximum link speed for the WHR-HP-GN. The speeds are for the total wireless data transferred including overhead. Because the overhead is not available for transfer of user data, the wireless throughput usable by the user will be substantially slower.

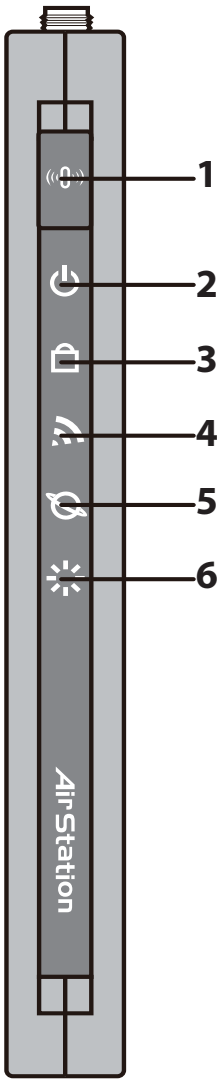
Package Contents

The following items are included with your AirStation. If any of the items are missing, please contact your vender.

- Main unit.....1
- Detachable antenna(s) .....2 for G300N / 1 for GN
- AC adapter.....1
- Stand for vertical/wall-mounting.....1
- Screws for wall-mounting.....2
- LAN cable.....1
- Air Navigator CD.....1
- Quick Setup Guide.....1

Hardware Overview

Front Panel LED's



1 AOSS Button
Hold down this button until the Security LED flashes (approximately. 1 second) to initiate AOSS or WPS mode, allowing the unit to exchange security keys with other AOSS or WPS compatible devices. Power must be on for this to work.

2 Power LED (Green)
On: The AC adapter is connected
Off: The AC adapter is not connected

3 Security LED (Amber)
Indicates security status.
Off: Encryption is not set
On: Encryption has been set
Double blink: The unit is waiting for an AOSS or WPS security key
Blinking: AOSS/WPS error; failed to exchange security keys
Note: When the Security LED is lit, an encryption key has been set. Wireless clients will need the same key to connect.

4 Wireless LED (Green)
Indicates wireless LAN status.
Blinking: Wireless LAN is transmitting
On: Wireless LAN is connected but not active

5 ROUTER LED (Green)
On: Router functionality is enabled
Blinking: Router functionality is disabled

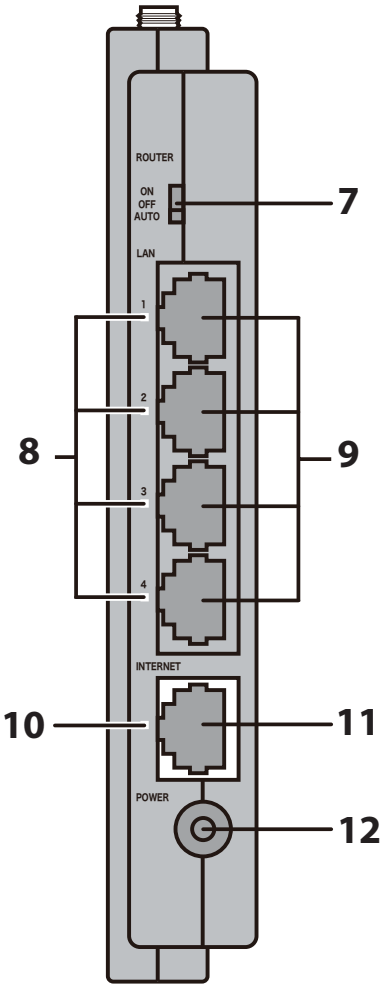
6 DIAG LED (Red)
This indicates the status of the unit by the number of blinks per cycle.
Note: When the unit is first turned on or restarted, the Diag LED will blink for almost a minute during boot. This is normal.

Diag LED status	Meaning	Status
2 blinks *1	Flash ROM error	Cannot read or write to the flash memory.
3 blinks *1	Ethernet (wired) LAN error	Ethernet LAN controller is malfunctioning.
4 blinks *1	Wireless LAN error	Wireless LAN controller is malfunctioning.
5 blinks	IP address setting error	Because the network addresses of both the Internet port (WAN port) and the LAN port are the same, it is not possible to establish communication. Change the LAN side IP address of this unit.
Continuously blinking *2	Updating the firmware Saving settings Initializing settings	Updating the firmware. Saving the settings. Initializing the settings.

*1 Unplug the AC adapter from the wall socket, wait for a few seconds, and then plug it again. If the light still flashes, please contact technical support.

*2 Never unplug the AC adapter while the Diag LED is blinking continuously.

Back Panel



7 Router Switch

Switches router mode between enabled, disabled, and auto.

On: Router is enabled (router mode).
Off: Router is disabled (bridge/AP mode).
Auto: This switches between modes automatically based on whether or not another router is detected on the Internet port. The default setting for this switch is Auto.

8 LAN LED (Green)

On: An Ethernet device is connected.
Flashing: An Ethernet device is communicating.

9 LAN Port

Connect your computer, hub, or other Ethernet devices to these ports. This switching hub supports 10 Mbps and 100 Mbps connections.

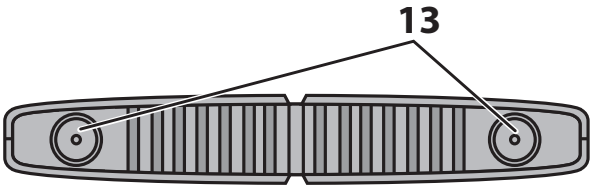
10 Internet LED (Green)

On: The Internet (WAN) port is connected.
Flashing: The Internet port is transmitting data.

11 Internet Port Connect your cable or DSL modem to this port. 10 Mbps and 100 Mbps connections are supported. In bridge/AP mode (router switch off), the Internet port becomes a regular LAN port, for a total of 5 usable LAN ports.

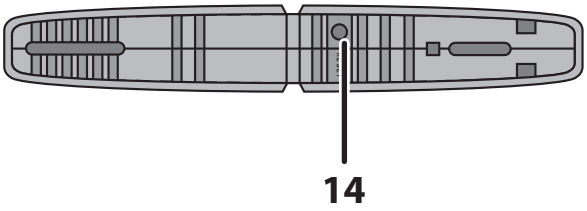
12 DC Connector Connect the included AC adapter.

Top



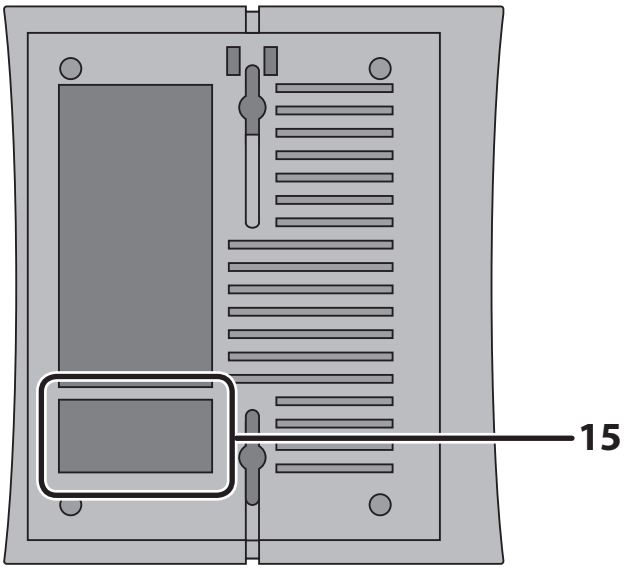
13 Antenna connector Screw on the antenna(s) here.

Bottom



14 Reset Button Hold in this button until the Diag LED comes on to initialize the AirStation's settings. Power must be on for this to work.

Right Side



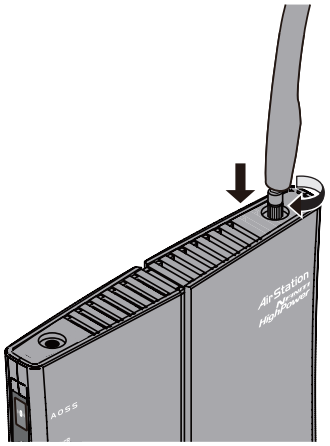
15 Factory Default Settings This sticker shows the AirStation's default SSID, encryption key, and WPS PIN.

Chapter 2
Placing Your AirStation

Note: Illustrations show the WHR-HP-G300N. The WHR-HP-GN is similar.

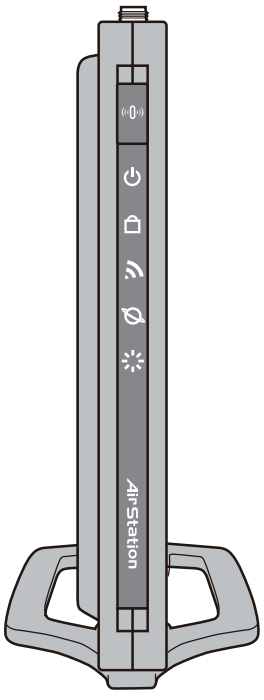
Antenna Placement

The antenna(s) are included in the package. The WHR-HP-G300N has two antennas; the WHR-HP-GN has one. Screw the antenna(s) clockwise to install.



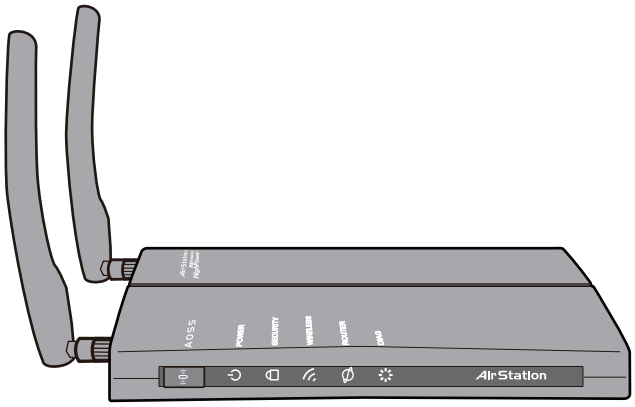
Vertical Placement

To stand the AirStation vertically, attach the base as shown.



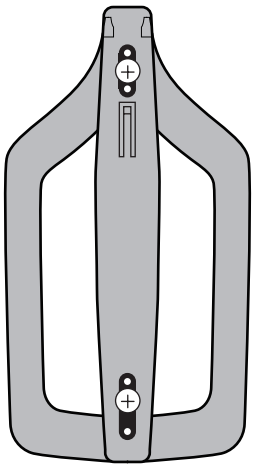
Horizontal Placement

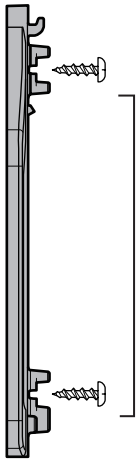
To place the unit horizontally, adjust the antenna(s) as shown.



Wall-Mounting

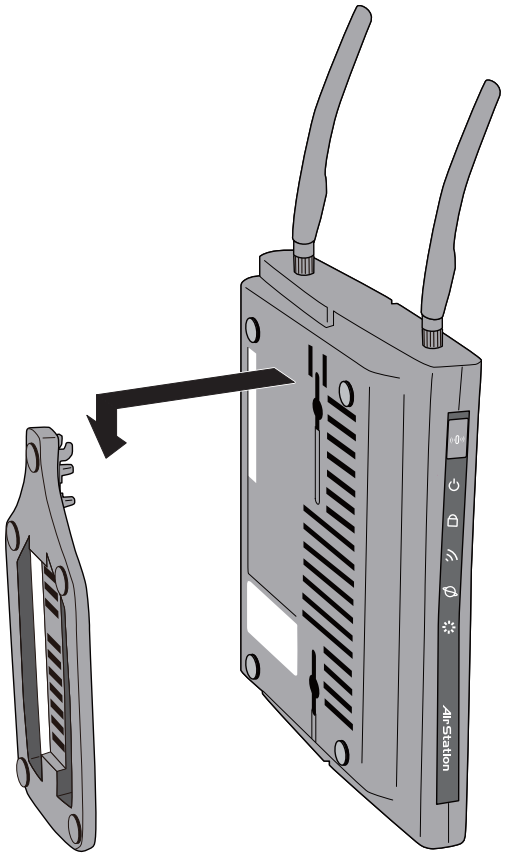
1





To wall-mount, attach the stand with screws as shown.

2



Place the center of the AirStation on the center of the stand and slide downward to lock in place.

Chapter 3
Installation

Automatic Setup

The AirNavigator CD can step you through installing your AirStation. Insert it into your Windows 7, Vista, or Windows XP PC and follow the instructions on the screen. If your computer uses a different operating system, use manual setup instead.

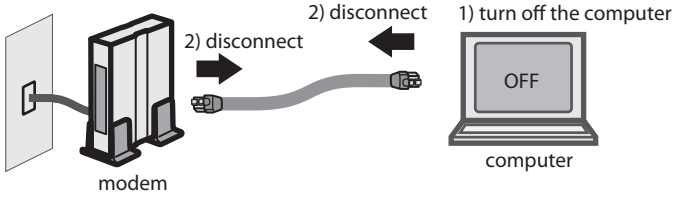
Manual Setup

Using AirStation As A Router or An Access Point

To use the AirStation as a router or an access point, configure as below.

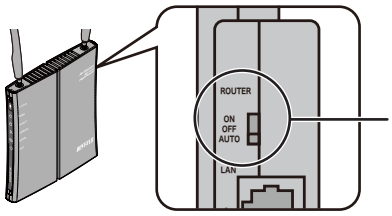
1 Turn off your computer and modem.

2



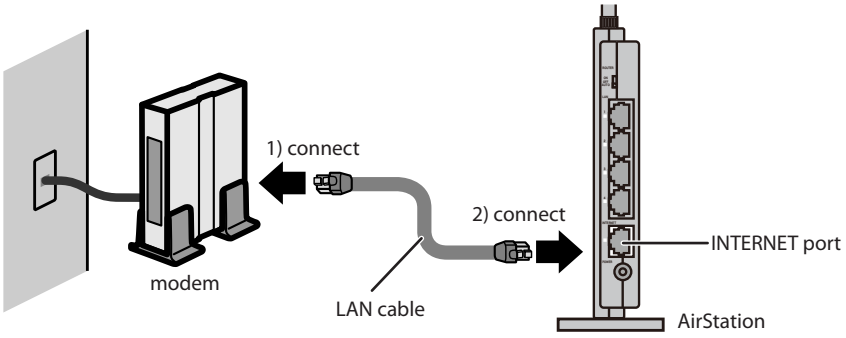
Unplug the LAN cable that connects your computer and modem.

3

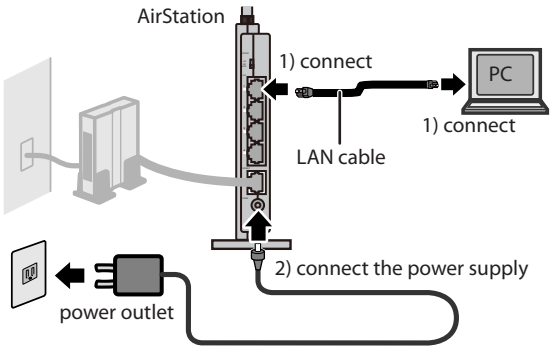


Make sure the mode switch on the back of the AirStation is in the [AUTO] position.

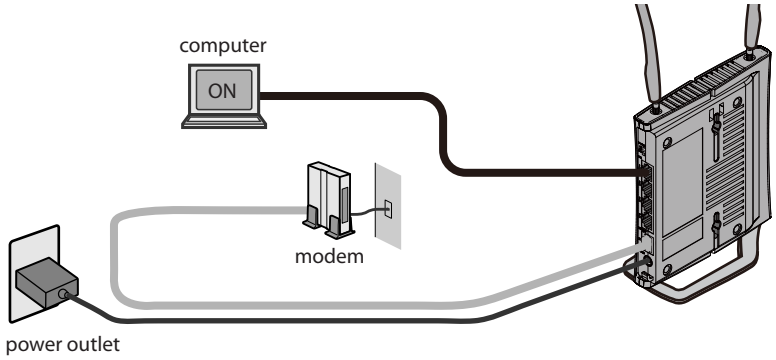
4 Connect one end of the LAN cable to the modem, and connect the other end to the Internet port of the AirStation. Turn on your modem.



5 Connect the AirStation's LAN port to your computer with another LAN cable.
Turn on the AirStation, wait 60 seconds, and then turn on your computer.



6 Confirm that the devices are connected correctly as shown below.



7 After the computer has booted, the LEDs on the AirStation should be in the following condition:

POWER	Green light on
WIRELESS	Green light on or blinking
ROUTER	Green light on or off depending on your network
DIAG	Off
LAN	Green light on or blinking
INTERNET	Green light on or blinking

※ Refer to page 8 and 10 for LED locations and other details.

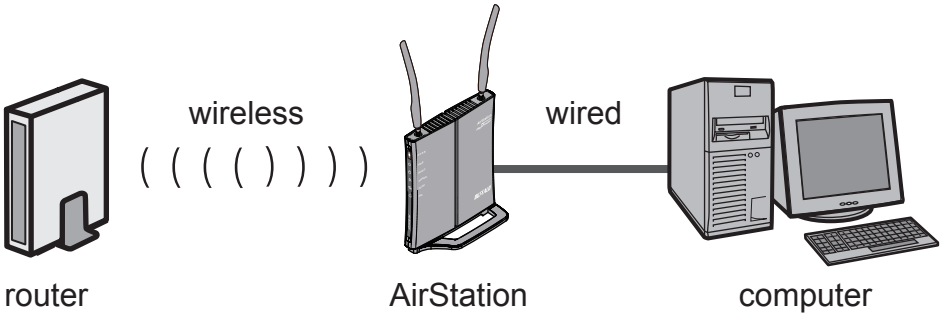
8 Launch a web browser. If the home page is displayed, setup is complete.
If a user name and password screen is displayed, enter [root] (in lower case) for the user name, leave the password blank, and click [OK]. Follow the instructions on the screen to complete setup.

You've completed initial setup of your AirStation. Refer to Chapter 4 for advanced settings.

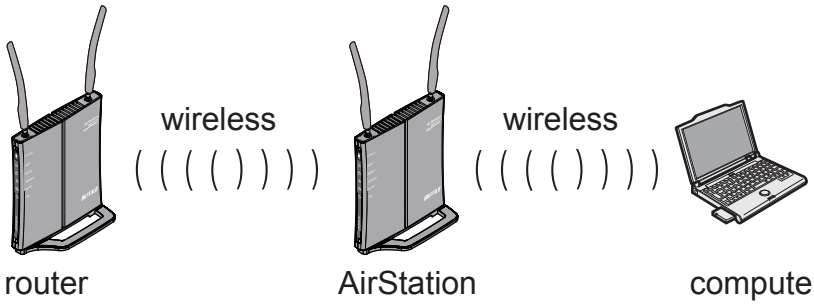
Using AirStation As An Ethernet Converter or A Repeater

To use the AirStation as an Ethernet converter or a repeater, follow the directions below.

Using as an Ethernet Converter:



Using as a repeater:



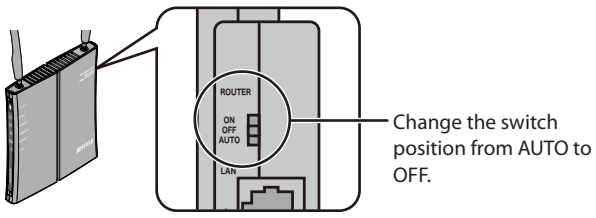
In this section, manual configuration is described. However, you can also use AOSS/WPS to configure it.

1 Set your computer's IP address settings as follows (Appendix C).

IP Address	192.168.11.80
Subnet mask	255.255.255.0
Default gateway	192.168.11.1
Preferred DNS server	192.168.11.1
Alternate DNS server	blank

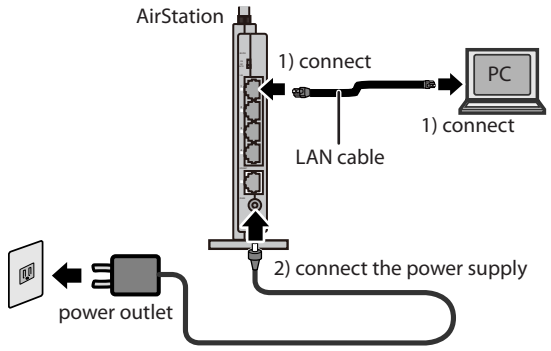
2 Shut down your computer.

3

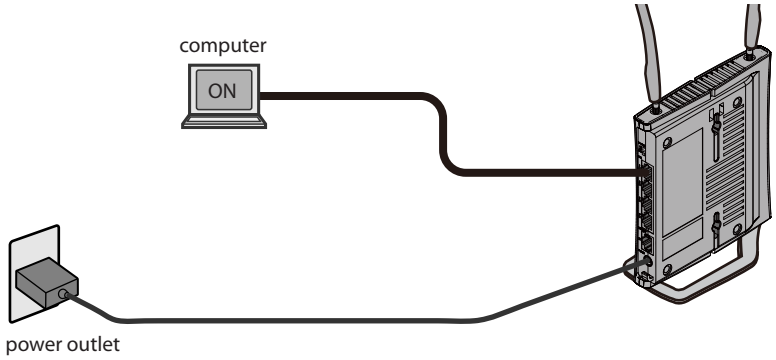


Change the switch position from AUTO to OFF.

4 Connect the AirStation's LAN port to your computer with another LAN cable. Turn on the AirStation, wait 60 seconds, and then turn on your computer.



5 Confirm that the devices are connected correctly as shown below.



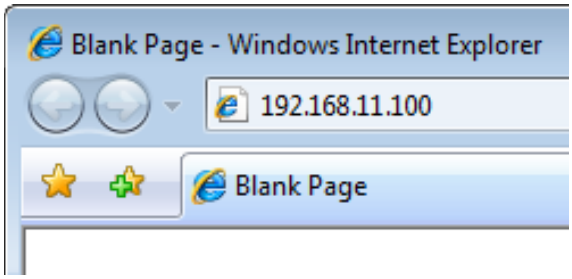
6 After the computer has booted, the LEDs on the AirStation should be in the following condition:

POWER	Green light on
WIRELESS	Green light on or blinking
ROUTER	Off
DIAG	Off
LAN	Green light on or blinking

※ Refer to page 8 and 10 for LED locations and other details.

7 Launch a web browser.

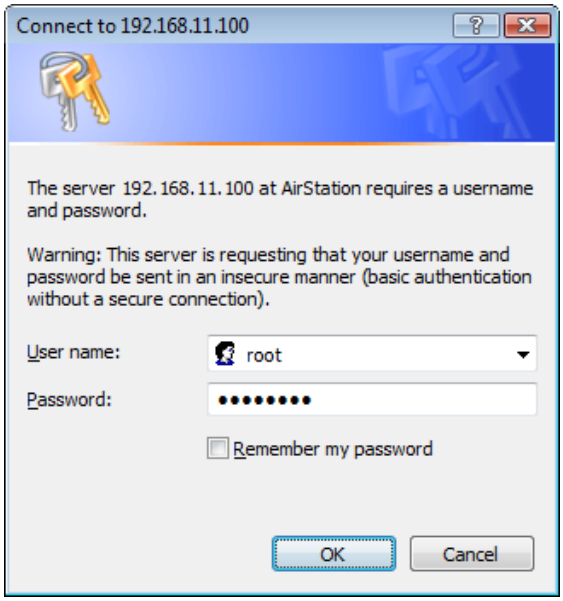
8



Enter the LAN IP address of the AirStation in the address field, then press the [Enter] key.

Notes:
- The default IP address of the AirStation is 192.168.11.100 on access point mode.
- If you have changed the IP address of the AirStation, enter that IP address.

9

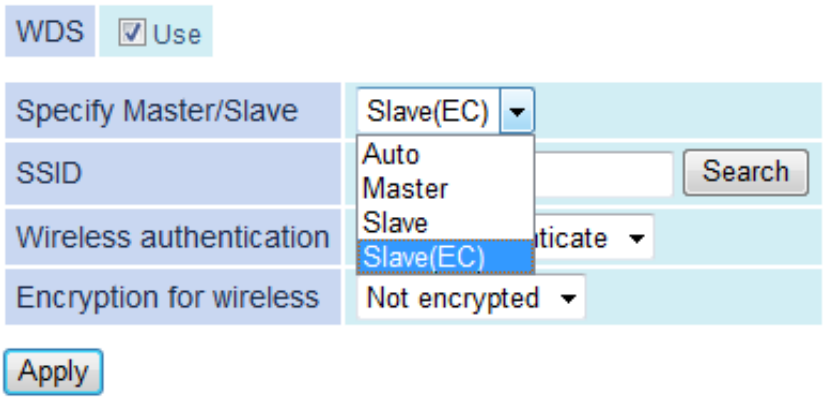


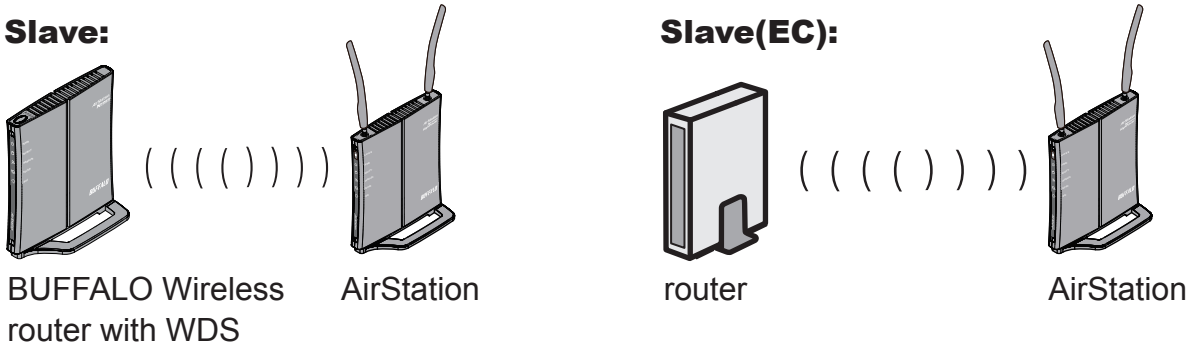
When this screen appears, enter [root] (in lower case) for the user name and the password that you set during initial setup. Click [OK].

Notes:
- By default, the password is blank (not set).
- If you forget your password, hold down the reset button (page 11) to initialize all settings. The password will then be blank. Note that all other settings will also revert to their default values.

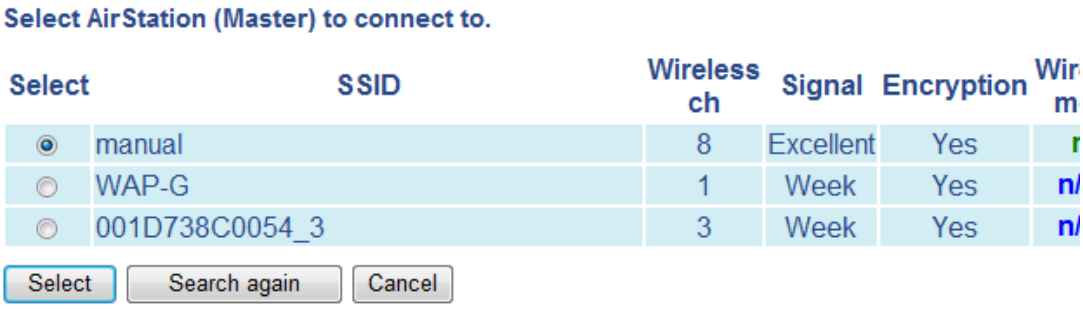
10 Click [Wireless Config] > [WDS].

11 If the device you connect supports WDS such as WHR-G300N, WHR-HP-G300N and WZR-HP-G300NH, select [Slave] from [Specify Master/Slave] menu and click [Search].
If the device you connect doesn't support WDS, select [Slave(EC)] from [Specify Master/Slave] menu and click [Search].

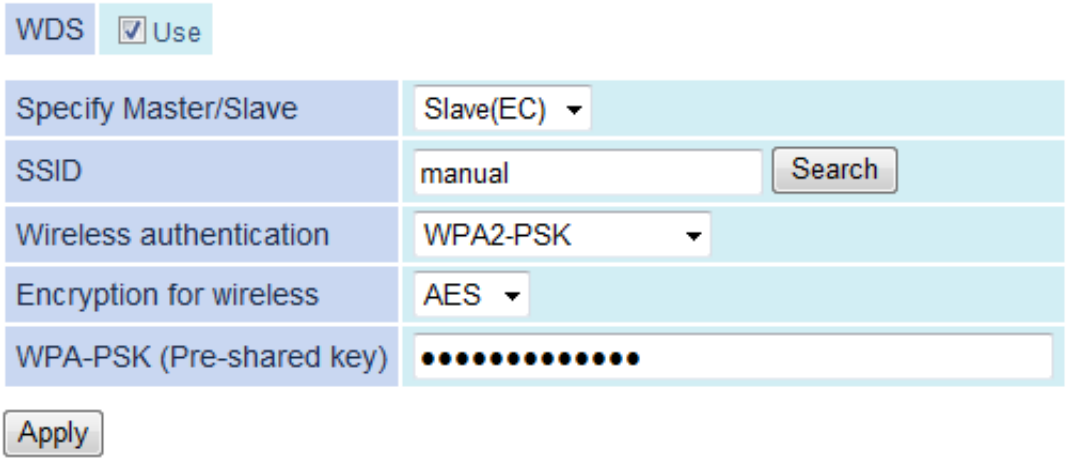




12 Once the list of the access points is displayed, select the access point you are going to connect to, then click [Select].
If the access point you are going to connect to is not displayed, click [Search again].



13 Enter the encryption settings and password ("key") for the access point you are connecting to, then click [Apply].



14 Change your computer's IP address settings back to their former values.

ex) IP Address — Obtain an IP address automatically
DNS server — Obtain DNS server address automatically

Note: If using the AirStation as a repeater, unplug the LAN cable from your computer. You're now connected to the AirStation wirelessly.

15 Launch a web browser. If your home page is displayed, setup is complete.

Firmware Differences

You can choose between two different firmwares for your AirStation. By default, the Professional firmware (DD-WRT) is installed. If you prefer, you may install the User-friendly firmware instead. the two firmwares have slightly different features, as shown in the chart below.

Function	Professional firmware (DD-WRT)	User-friendly firmware
Router switch function	—	✔
Default administrator name	root	root (fixed)
Default administrator password	admin	none
AOSS	✔	✔
WPS	—	✔
WDS	✔	✔

Changing Firmware

To change between the Professional firmware (DD-WRT) and the User-friendly firmware, follow the steps below.

1 Insert the AirNavigator CD into your computer. The setup wizard will automatically launch.

Note: If the Setup Wizard does not launch, open the CD and double-click [ASSetWiz.exe] to launch manually.

2

Click [Change Firmware].

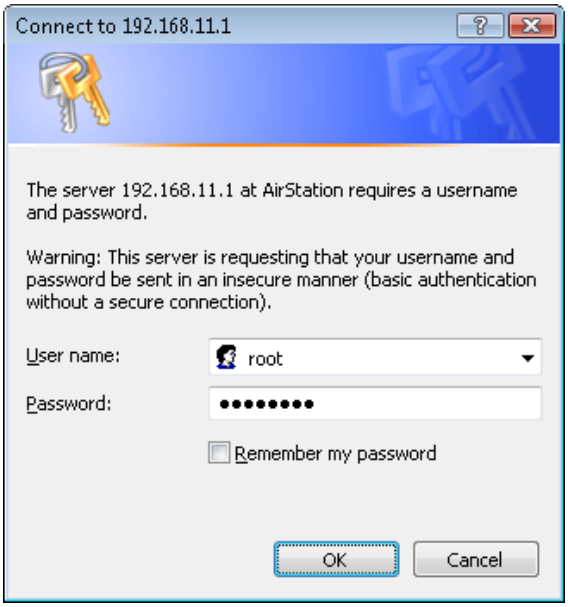
3

The procedure for wiring will be displayed. Step through the wizard to connect your AirStation.

4

When this screen is displayed, click [Change Firmware].

5



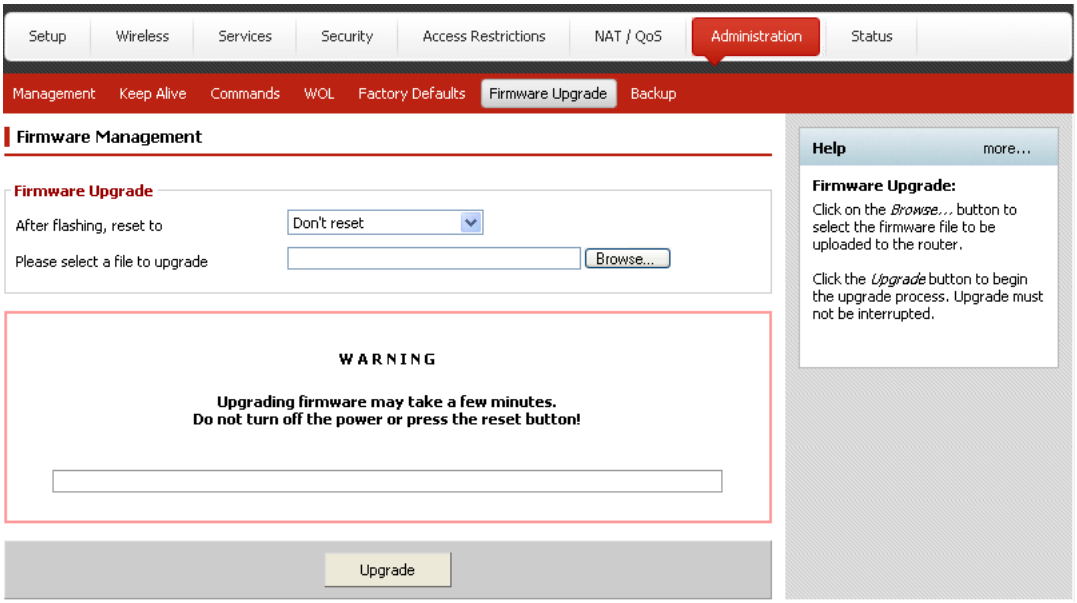
If requested, enter the AirStation's username and password.

Note: By default, the Professional firmware doesn't have a username and a password configured. Set them before you go to the next step.

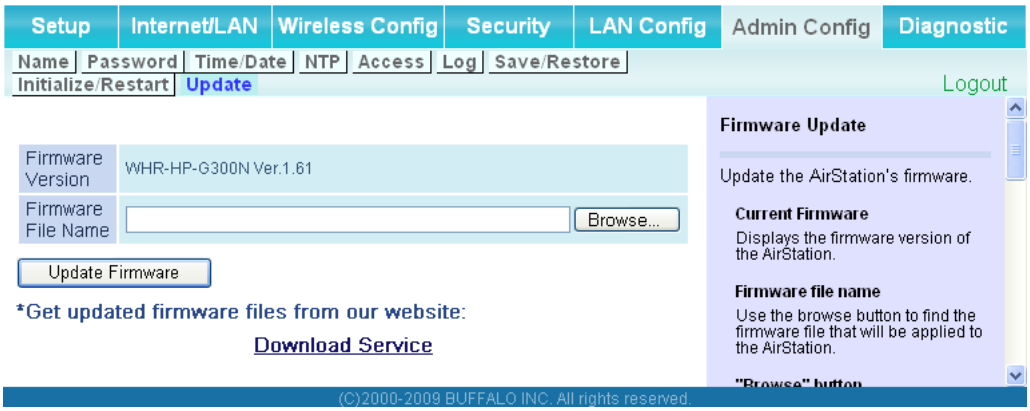
6 When the following screen is displayed, make sure that the firmware file name is displayed, click [Update] or [Update Firmware], and follow the instructions on the screen.

Note: If the firmware name is not displayed on the screen, click [Browse...] and select the desired firmware. Firmware files are in the root directory on the AirNavigator CD.

Professional firmware (DD-WRT) update screen:



User-friendly firmware update screen:



About this User Manual

This user manual is primarily for AirStations with the User-friendly firmware. For more information on the Professional firmware (DD-WRT), refer to ***www.dd-wrt.com/wiki***.

Chapter 4
Configuration

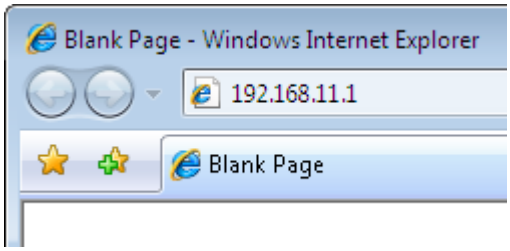
The web-based configuration interface lets you change AirStation settings. Don't change these settings unless you know what you're doing.

Accessing the Web-based Configuration Interface

To configure the AirStation's advanced settings manually, log in to the web-based configuration interface as shown below.

1 Launch a web browser.

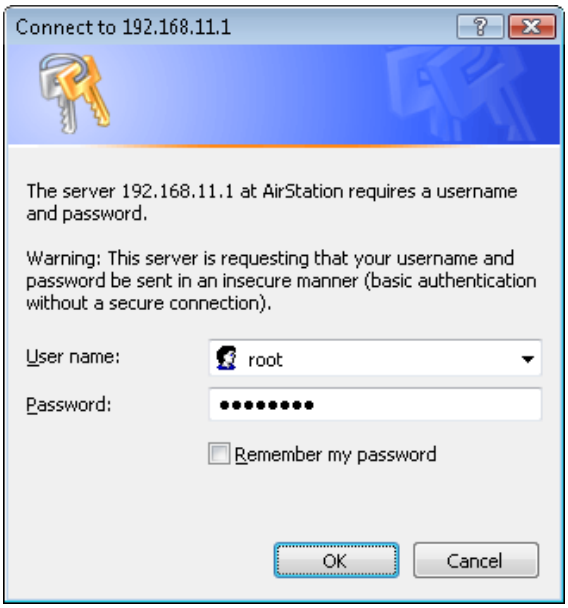
2



Enter the AirStation's LAN-side IP address in the address field, and press the enter key.

Note:
- The AirStation's default LAN-side IP address depends on the position of the mode switch.
  In router mode: 192.168.11.1
  In bridge mode: 192.168.11.100
  If the router switch is set to AUTO and the unit is in bridge mode, then the AirStation's IP address was assigned by an external DHCP server.
- If you changed the IP address of the AirStation, then use the new IP address.

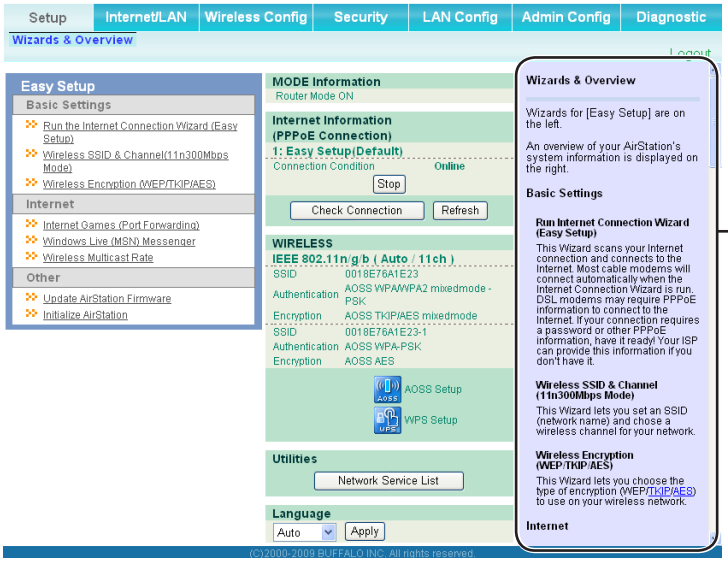
3



When this screen appears, enter [root] (in lower case) for the user name and the password that you set during initial setup. Click [OK].

Note:
- By default, the password is blank (not set).
- If you forget your password, hold down the Reset button (page 11) to initialize all settings. The password will then be blank. Note that all other settings will also revert to their default values.

4



The configuration interface is displayed.

Help is always displayed on the right side of the configuration utility. Refer to the Help screens for more information on each page in the web-based configuration interface.

Note : This example, like others in this manual, shows the User-friendly firmware. The dd-wrt based Professional firmware is somewhat different. For more information on the Professional firmware, visit dd-wrt's website at ***www.dd-wrt.com***.

Configuration Menu (Router Mode)

In router mode, the AirStation's web-based configuration interface has the following menu screens. See the pages listed at right for more information about a menu screen.

Main screen	Descriptions	Page
Internet/LAN		
Internet	Configure Internet side port and settings	Page 34
PPPoE	PPPoE settings (DSL login)	Page 35
DDNS	DNS settings	Page 38
VPN Server	VPN server settings	Page 40
LAN	LAN side port and DHCP server configuration	Page 42
DHCP Lease	DHCP lease settings	Page 44
NAT	Network address translation settings, used to connect LAN side devices to the Internet	Page 45
Route	Configure the IP communication route that the AirStation uses	Page 46
Wireless Config		
WPS	WPS settings and status	Page 47
AOSS	AOSS (AirStation One-touch Secure System) settings and status	Page 48
Basic	Configure basic wireless settings	Page 50
Advanced	Configure advanced wireless settings	Page 53
WMM	Set priorities for Wireless Multimedia Extensions (Wi-Fi Multimedia)	Page 54
MAC Filter	Limit access to specific devices	Page 56
Multicast Control	Configure limits on sending unnecessary multicast packets to the wireless LAN port	Page 57
WDS	Configure communication among AirStation	Page 58
Security		
Firewall	Protect your computer from outside intruders	Page 60
IP Filter	Edit IP filters which relates to the packets passing through the LAN side and the Internet side	Page 62
VPN Pass Through	Configure IPv6 passthrough, PPPoE passthrough, and PPTP passthrough	Page 63

LAN Config		
Port Forwarding	Configure port translation and exceptions for games and other programs	Page 64
DMZ	Configure a destination to transfer communication packets without a LAN side destination.	Page 65
UPnP	Configure UPnP (Universal Plug and Play)	Page 66
QoS	Configure priority for packets that require a certain data flow	Page 67
Admin Config		
Name	Configure the AirStation's name	Page 68
Password	Configure the AirStation's login password for access to configuration utilities	Page 69
Time/Date	Configure the AirStation's internal clock	Page 70
NTP	Configure the AirStation to synchronize with an NTP server to automatically set the AirStation's internal clock	Page 71
Access	Configure access restrictions to the AirStation's configuration utilities	Page 72
Log	Configure a syslog server to manage the AirStation's logs	Page 73
Save/Restore	Save or restore the AirStation's configuration from a configuration file	Page 74
Initialize/Restart	Initialize the AirStation or reboot it	Page 75
Update	Update the AirStation's firmware	Page 76
Diagnostic		
System Info	View current system information for the AirStation	Page 77
Logs	Check the AirStation's logs	Page 79
Packet Info	View all packets transferred by the AirStation	Page 80
Client Monitor	View all devices currently connected to the AirStation	Page 81
Ping	Test the AirStation's connection to other devices on the network	Page 82
Logout		
Click this to log out of the AirStation's web-based configuration interface		

Configuration Menu (Bridge Mode)

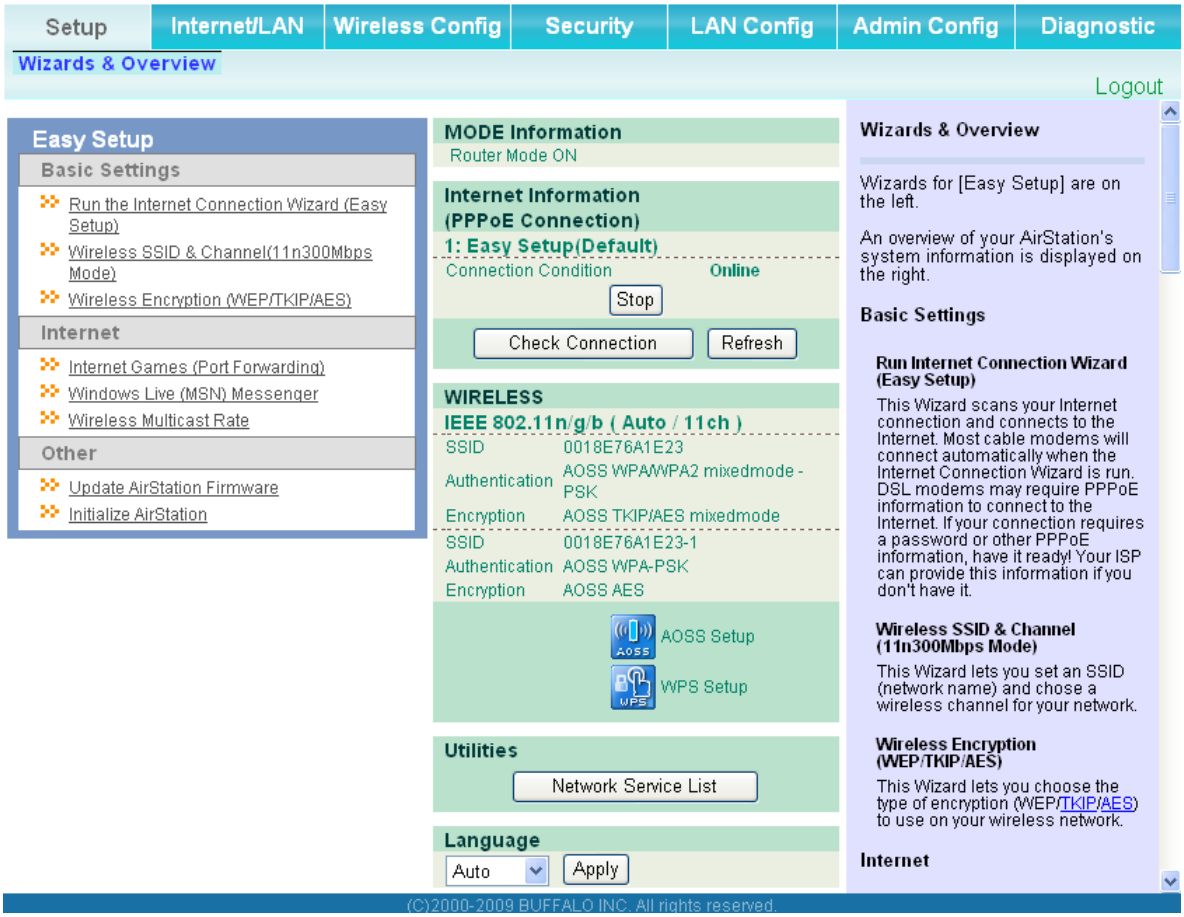
In bridge mode, the AirStation's web-based configuration interface has the following menu screens. See the pages listed at right for more information about a menu screen.

Main screen	Descriptions	Page
LAN Config		
LAN	Configure LAN side ports and devices	Page 42
Route	Configure the IP communication route that the AirStation uses	Page 46
Wireless Config		
WPS	WPS settings and status	Page 47
AOSS	AOSS (AirStation One-touch Secure System) settings and status	Page 48
Basic	Configure basic wireless settings	Page 50
Advanced	Configure advanced wireless settings	Page 53
WMM	Set priorities for Wireless Multimedia Extensions (Wi-Fi Multimedia)	Page 54
MAC Filter	Limit access to specific devices	Page 56
Multicast Control	Configure limits on sending unnecessary multicast packets to the wireless LAN port	Page 57
WDS	Configure communication among AirStation	Page 58
Admin Config		
Name	Configure the AirStation's name	Page 68
Password	Configure the AirStation's login password for access to configuration utilities	Page 69
Time/Date	Configure the AirStation's internal clock	Page 70
NTP	Configure the AirStation to synchronize with an NTP server to automatically set the AirStation's internal clock	Page 71
Access	Configure access restrictions to the AirStation's configuration utilities	Page 72
Log	Configure a syslog server to manage the AirStation's logs	Page 73
Save/Restore	Save or restore the AirStation's configuration from a configuration file	Page 74
Initialize/Restart	Initialize the AirStation or reboot it	Page 75
Update	Update the AirStation's firmware	Page 76
Diagnostic		
System Info	View current system information for the AirStation	Page 77

Logs	Check the AirStation's logs	Page 79
Packet Info	View all packets transferred by the AirStation	Page 80
Client Monitor	View all devices currently connected to the AirStation	Page 81
Ping	Test the AirStation's connection to other devices on the network	Page 82
Logout		
Click this to log out of the AirStation's web-based configuration interface.		

Setup

This is the home page of the configuration interface. You can verify settings and the status of the AirStation here.



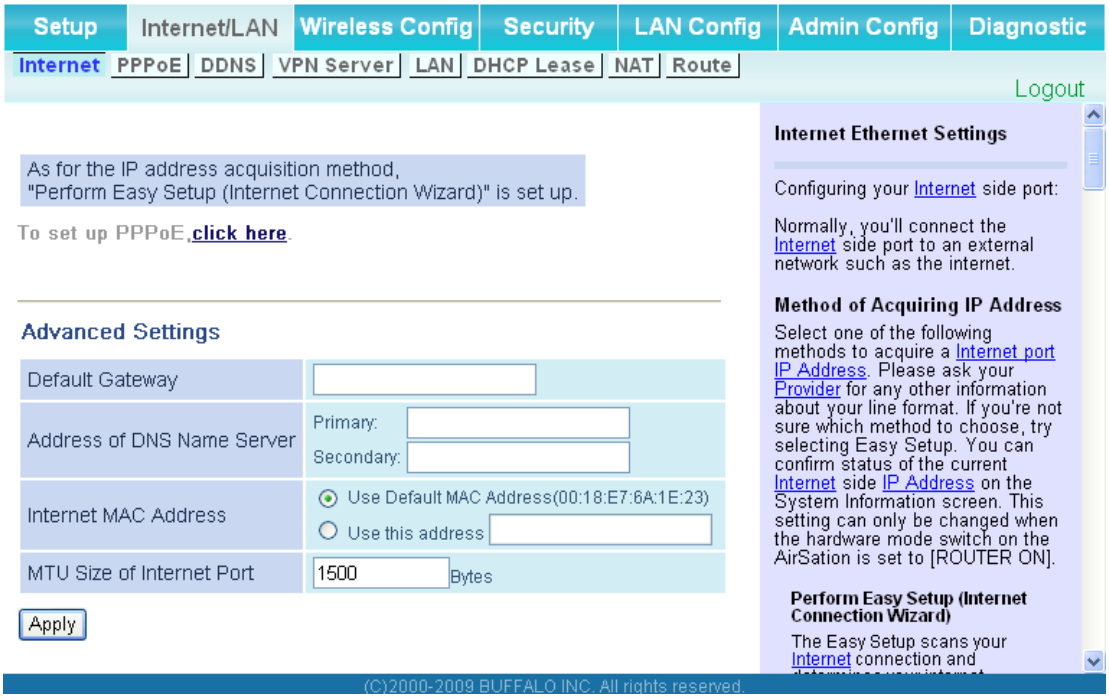
Parameter	Meaning
Internet/LAN	Configure WAN side network settings.
Wireless Config	Configure wireless settings.
Security	Configure security settings.
LAN Config	Open ports for games and applications.
Admin Config	Open the Admin configuration screen.
Diagnostic	Gives information and tools for troubleshooting the network.

Parameter	Meaning
Easy Setup	Automatically configures the AirStation's internet connection.
Internet Information	Displays the current internet connection.
Check Connection	Checks if the AirStation is connected to the Internet properly.
Refresh	Click to refresh the display.
WIRELESS	Displays current wireless settings.
AOSS	Click to display the AOSS configuration screen.
WPS	Click to display the WPS configuration screen.
Network Service List	Shows a list of network services.
Language	Select the language you use.
Logout	Log out of the AirStation's web-based configuration interface. After 5 minutes of inactivity, the AirStation will log off automatically.

Internet/LAN (LAN Config)

Internet (Router Mode only)

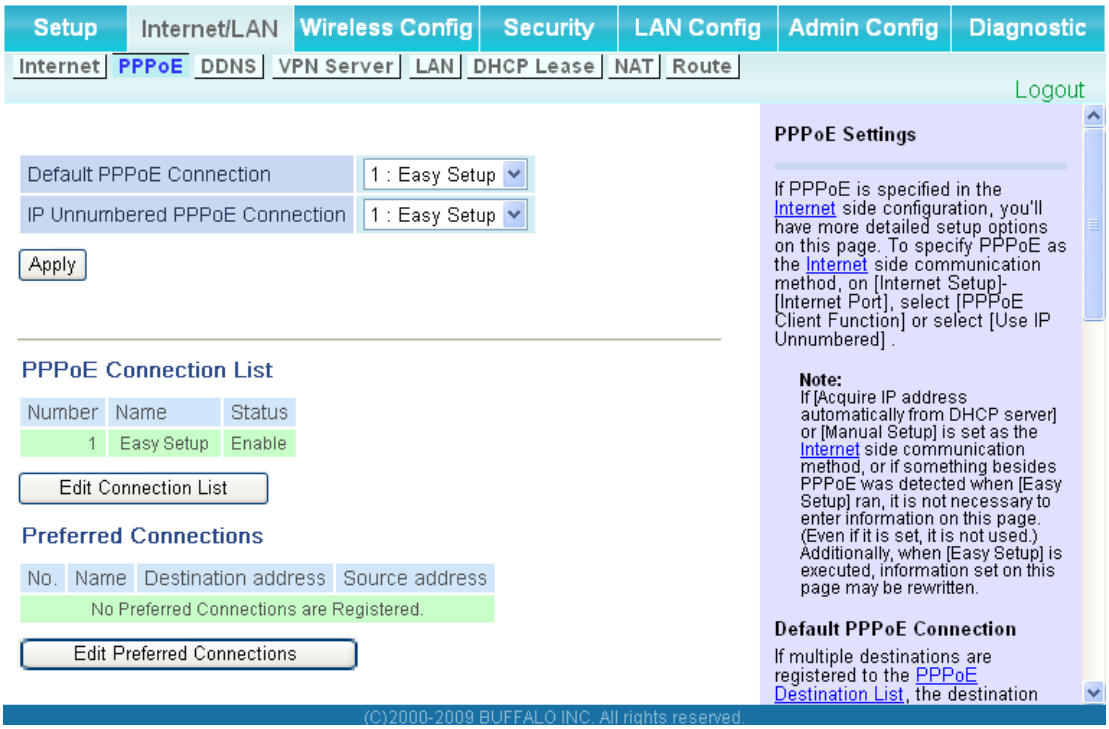
The screen to configure a port of the Internet side.



Parameter	Meaning
Method of Acquiring IP Address	Specifies how the current WAN side IP address was obtained.
Default Gateway	Specify an IP address for the default gateway.
Address of DNS Name Server	Specify an IP address for the DNS server.
Internet MAC Address	Configure the Internet side MAC address. Note: Configuring an improper MAC address may make the AirStation unusable. Change this setting at your own risk.
MTU size of Internet Port	Values between 578 to 1500 bytes may be entered.

PPPoE (Router Mode only)

The screen to configure PPPoE settings.



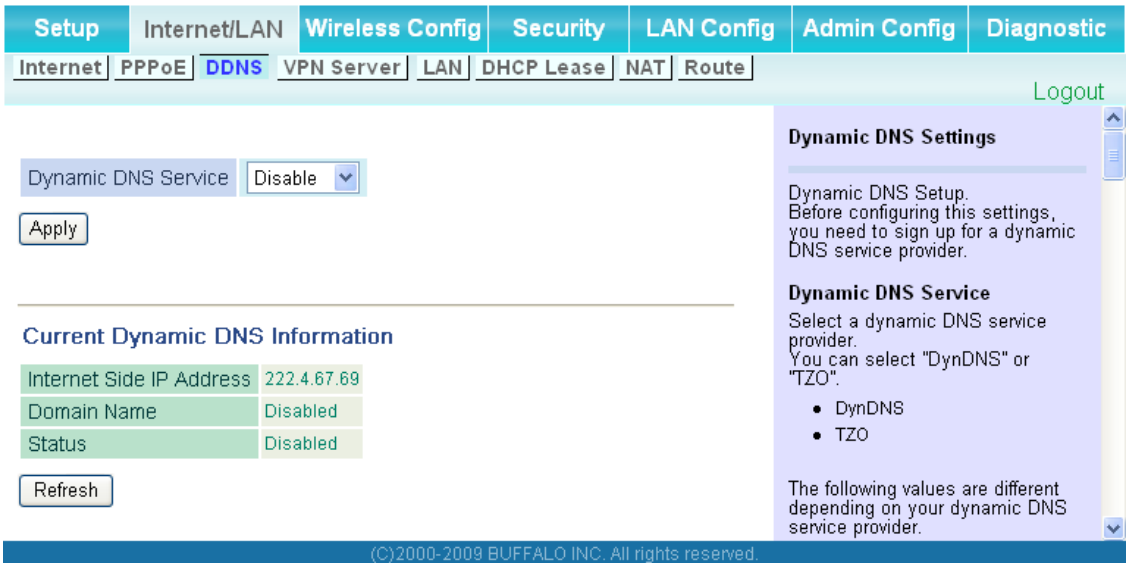
Parameter	Meaning
Default PPPoE Connection	If you have registered multiple connection destinations in PPPoE Connection List, connection destinations selected here have priority. You need to configure the route to which PPPoE is connected to if you don't use the default setting.
IP Unnumbered PPPoE Connection	Select the destination from the PPPoE Connection List which is used when specifying [Use IP Unnumbered] in Method of Acquiring IP Address (page 34).
PPPoE Connection List	Edit PPPoE destination. You can register up to 5 sessions.
[Edit Connection List]	Click this button to display the screen to edit the settings of destination.

Parameter	Meaning
PPPoE Connection No.*-Add	Click [Edit Connection List] to display. **Name of Connection** Enter a name to identify the connection. You may enter up to 32 alphanumerical characters and symbols. **User Name** Enter the user name specified by your provider for PPPoE. You may enter up to 32 alphanumerical characters and symbols. **Password** Enter the password specified by your provider for PPPoE. You may enter up to 32 alphanumerical characters and symbols. **Service Name** Fill in this field only when your provider specifies a Service Name. Leave blank otherwise. You may enter up to 32 alphanumerical characters and symbols. **Connection Type** Specifies the timing for the AirStation to connect to your provider. **Automatic disconnection** Set time to disconnect after communication is stopped when the connection method is set to [Connect on Demand] or [Manual]. You can enter up to 1440 minutes. **Authorization** Configure an authorization method with a provider. **MTU Size** Configure the MTU value between 578 and 1492 bytes. **MRU Size** Configure the MRU (Maximum Receive Unit) value between 578 and 1492 bytes.
Preferred Connections	Displays connections that you've added to the preferred connection list.
[Edit Preferred Connections]	Click this button to display the screen to edit the settings of connection destination route.

Parameter	Meaning
PPPoE Connection No. *-Add	**Keep Alive** If Keep Alive is enabled, the AirStation issues LCP echo requests to maintain the connection with the PPPoE server once a minute. If the server does not respond after 6 minutes, then the line is considered disconnected and the AirStation will terminate the connection. If your PPPoE connection is often disconnected, disable Keep Alive.
Preferred PPPoE Connection -Add	This is displayed when clicking [Edit Preferred Connections]. **Name** The name of destination to connect by PPPoE if [Destination address] and [Source address] of the communication match. Select the destination registered to PPPoE Connection List. **Destination address** Destination address to communicate. When communicating to this destination address, the AirStation will communicate with [Name of Connection]. **Source address** Source address to communicate. When communicating from this source address, the AirStation will communicate with [Name of Connection].

DDNS (Router Mode only)

Configure Dynamic DNS settings.

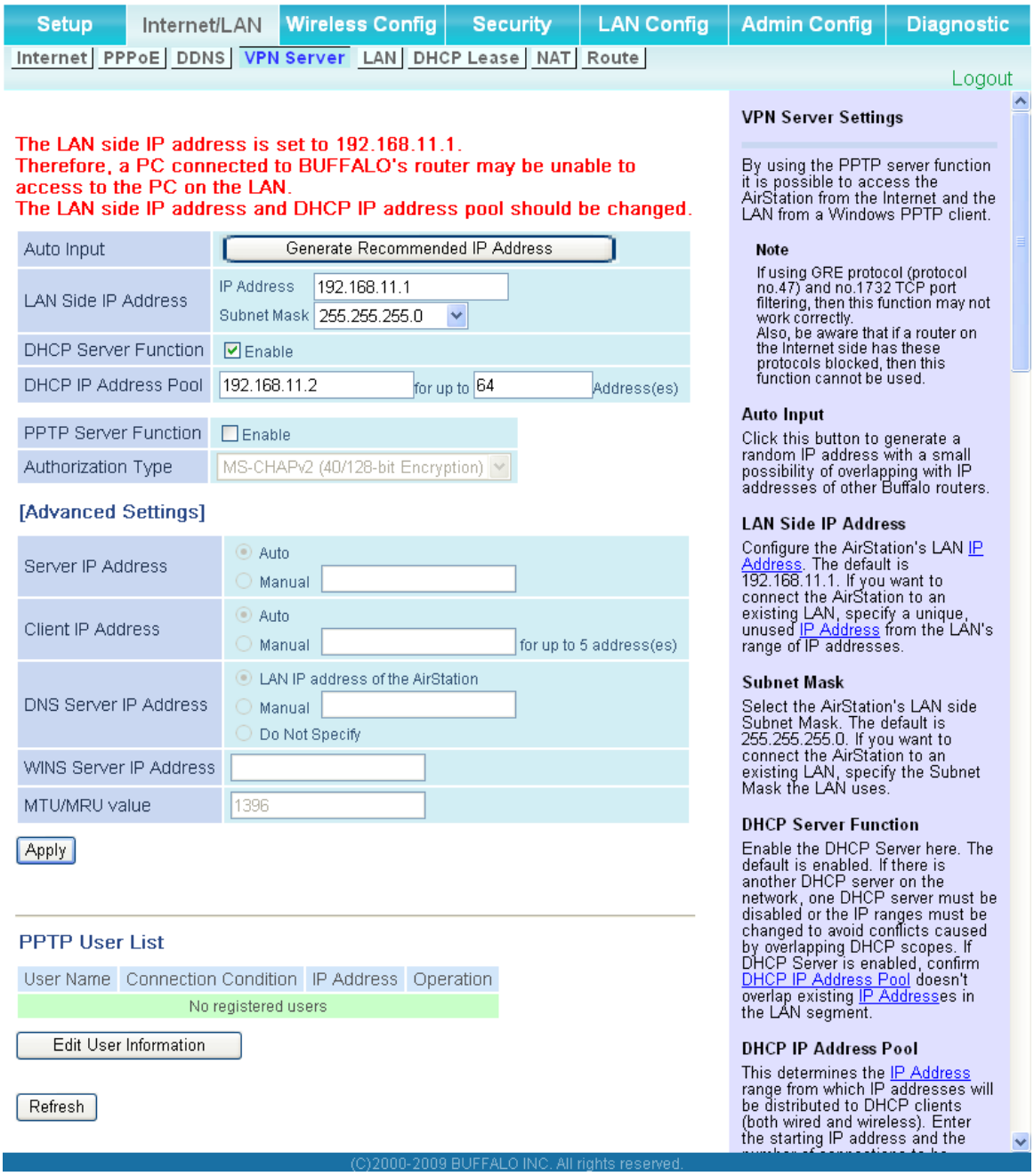


Parameter	Meaning
Dynamic DNS Service	Select a provider (DynDNS or TZO) for Dynamic DNS.
User Name Only when DynDNS is selected	Enter the user name for the Dynamic DNS service. You may enter up to 64 alphanumerical characters and symbols.
Password Only when DynDNS is selected	Enter the password for the Dynamic DNS service. You may enter up to 64 alphanumerical characters and symbols.
Host Name Only when DynDNS is selected	Enter the host name for the Dynamic DNS service. You may enter up to 255 alphanumerical characters, hyphens, and periods.
Email Address Only when selecting TZO	Enter the email address which is registered to the Dynamic DNS service. You may enter up to 64 alphanumerical characters and symbols.
TZO Key Only when selecting TZO	Enter the TZO Key which is registered to the Dynamic DNS service. You may enter up to 64 alphanumerical characters and symbols.
Domain Name Only when selecting TZO	Enter the domain name which is registered to the Dynamic DNS service. You may enter up to 255 alphanumerical characters, hyphens, and periods.

Parameter	Meaning
IP Address Update Period	Specifies the period to notify the dynamic DNS service provider of the current IP address. When DynDNS is selected, set it between 0 and 35 days. When TZO is selected, set it between 0 and 99 days. If 0 (zero) day is set, no periodic update is performed.
Internet Side IP Address	The WAN-side IP address of the AirStation's Internet port. This address is sent to the dynamic DNS service provider.
Domain Name	The domain name assigned by the dynamic DNS Service provider. The AirStation can be accessed from the Internet using this domain name.
Status	Displays the status of dynamic DNS service.

VPN server (Router Mode Only)

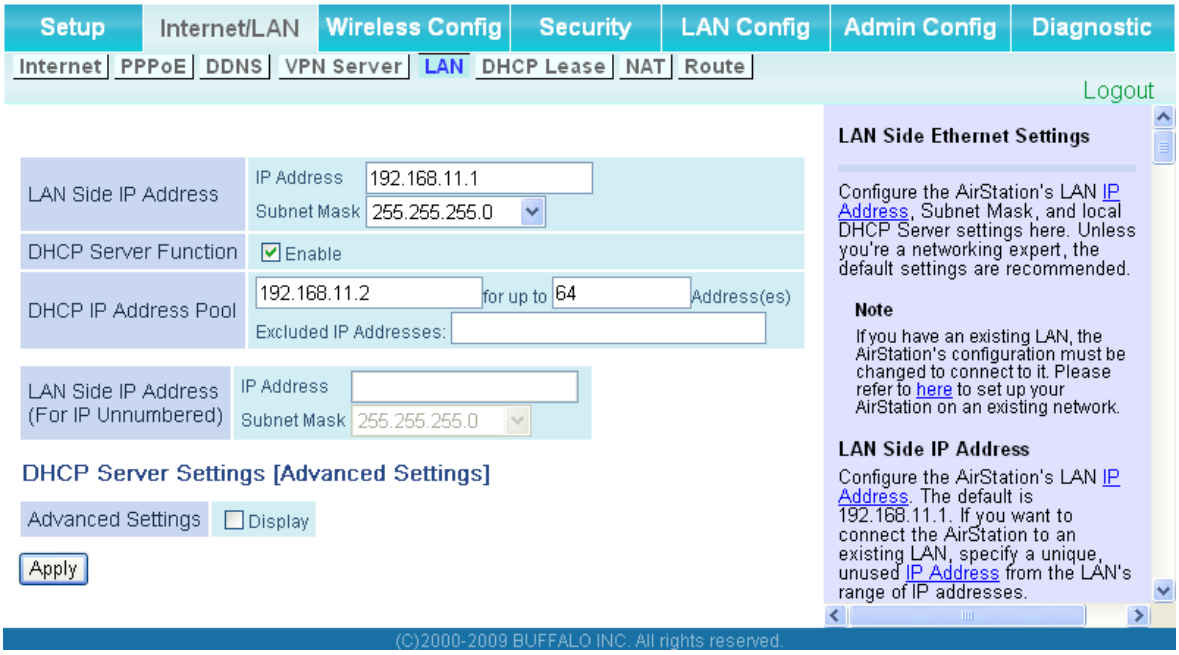
Configure a VPN server.



Parameter	Meaning
Auto Input	Click to generate a random IP address.
LAN Side IP Address	Set a LAN side IP address and subnet mask.
DHCP Server	If enabled, the DHCP server will assign LAN-side IP addresses automatically.
DHCP IP Address Pool	You may choose the range of IP addresses assigned by the DHCP server and select IP addresses to be excluded from that range. Values from 0-253 may be entered.
PPTP Server	Enable to use a PPTP server.
Authorization Type	Select the authentication method for PPTP connection.
Server IP Address	Select the server IP address.
Client IP Address	Select the IP address range.
DNS Server IP Address	Set the DNS server IP address for the DHCP server to issue to clients.
WINS Server IP Address	Set the WINS server IP address for the DHCP server to issue to clients.
[Edit User Information]	Click to edit user information.
User Name	Enter the user name to connect to the PPTP server. You may enter up to 16 alphanumerical characters and symbols.
Password	Enter the password to connect to the PPTP server. You may enter up to 16 alphanumerical characters and symbols.
Method of Acquiring IP Address	Select the method to be used to assign the client's IP address.
PPTP User List	Displays the PPTP connection user information.

LAN

Configure LAN-side IP address settings.

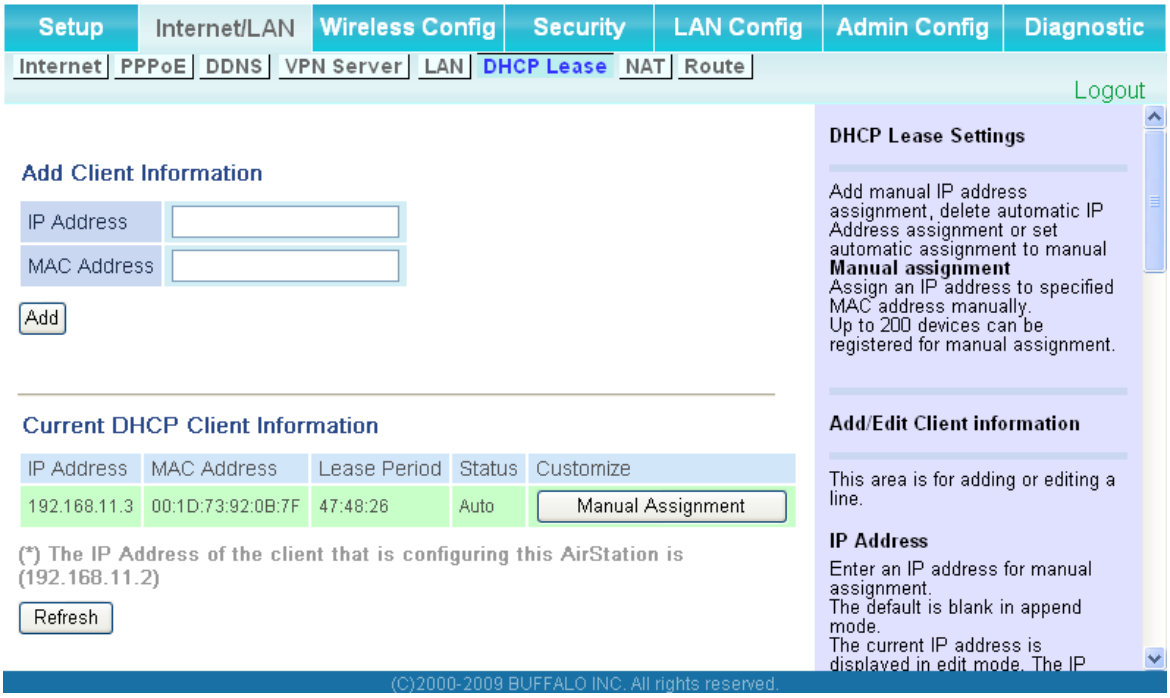


Parameter	Meaning
LAN Side IP Address	Set a LAN side IP address and subnet mask.
DHCP Server Function Router Mode only	Enable or disable the DHCP server, which assigns IP addresses automatically.
DHCP IP Address Pool Router Mode only	Configure the range of IP addresses to be assigned by the DHCP server and IP addresses to be excluded from that range. Values from 0-253 may be entered.
LAN Side IP Address (IP Unnumbered) Router Mode only	Set a LAN side IP address for IP unnumbered. Note: A PC with a normal LAN side IP address and a PC with an LAN side IP address for IP Unnumbered cannot communicate each other.
Advanced Settings Router Mode only	Select Display to display the advanced settings options for the DHCP server.
Lease Period Router Mode only	Set the effective period of an IP address assigned by the DHCP server. Up to 999 hours may be entered.

Parameter	Meaning
Default Gateway Router Mode only	Set the default gateway IP address for the DHCP server to issue to clients.
DNS Servers Router Mode only	Set the DNS server IP address for the DHCP server to issue to clients.
WINS Server Router Mode only	Set the WINS server IP address for the DHCP server to issue to clients.
Domain Name Router Mode only	Set the domain name for the DHCP server to issue to clients. You may enter up to 127 alphanumerical characters, hyphens, and periods.
Default Gateway Bridge Mode only	Set the default gateway IP address.
DNS Server Address Bridge Mode only	Set the DNS server IP address.

DHCP Lease (Router Mode only)

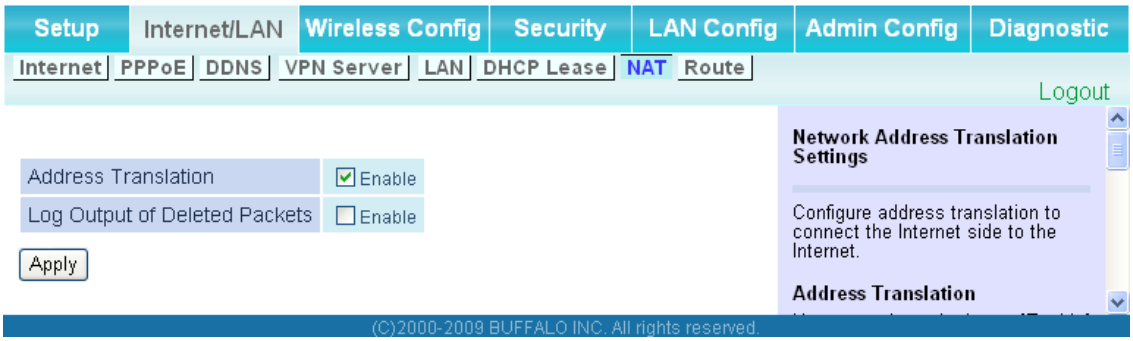
Configure DHCP leases.



Parameter	Meaning
IP Address	Enter an IP address to lease manually. The IP address should be from the same subnet as the DHCP scope, but not be within the range that DHCP is assigning to other devices.
MAC Address	Enter the MAC address which identifies the client.
Current DHCP Client Information	Displays information for current leases. An IP address which is leased automatically can be changed to be leased manually by clicking [Manual Assignment].

NAT (Router Mode only)

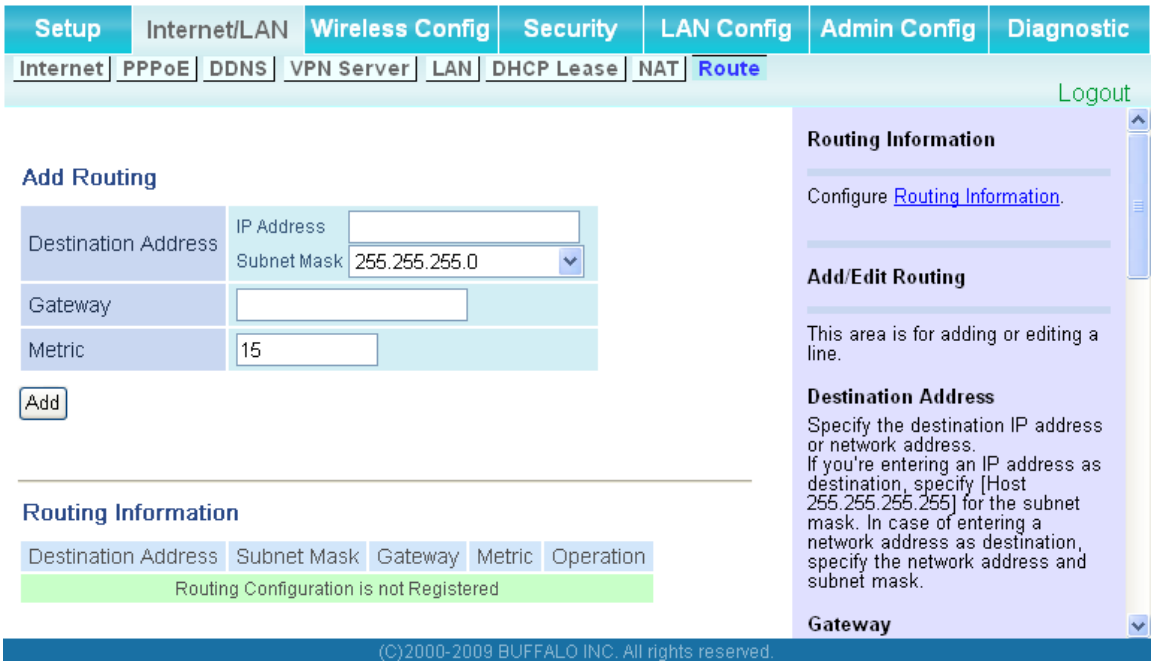
NAT (network address translation) allows your private LAN side network devices to communicate with the Internet.



Parameter	Meaning
Address Translation	Enable to use Network Address Translation.
Log Output of Deleted Packets	Enable to log deleted packets (such as errors) from address translation.

Route

Configure the AirStation's IP communication routes.

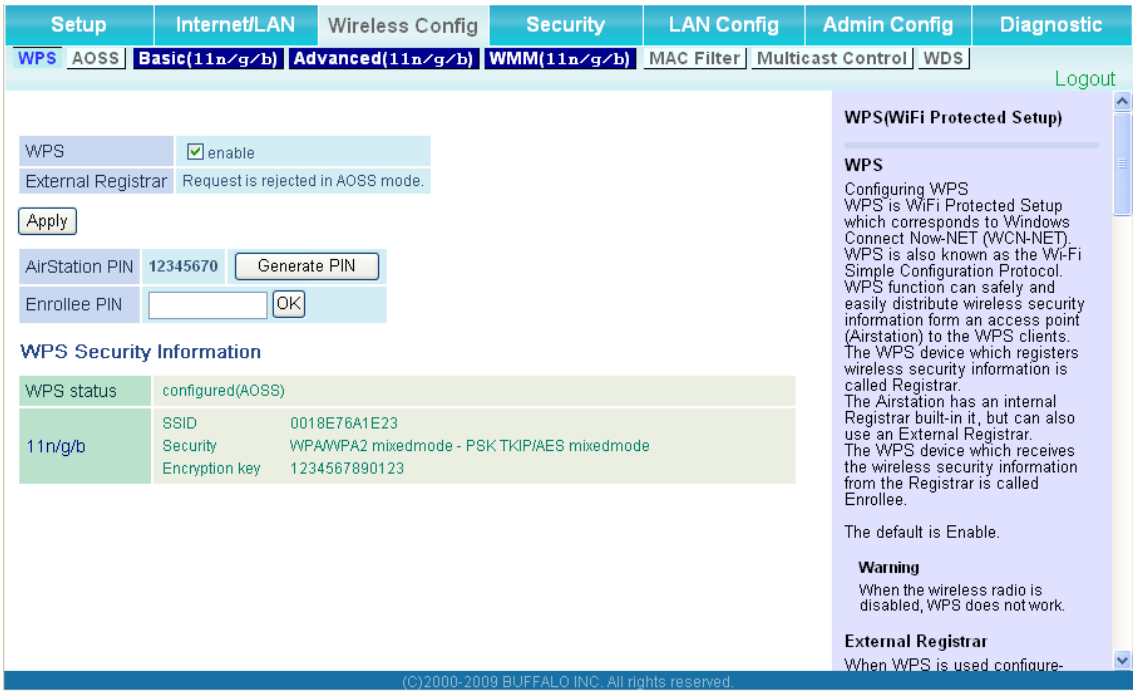


Parameter	Meaning
Destination Address	Adds a destination IP address and subnet mask to a routing table.
Gateway	Adds a gateway address to a routing table.
Metric	The metric is the maximum number of router hops a packet may take on the way to its destination address. Values between 1 and 15 may be entered. The default value is 15.
Routing Information	Manual entries will appear here after being added.

Wireless Config

WPS

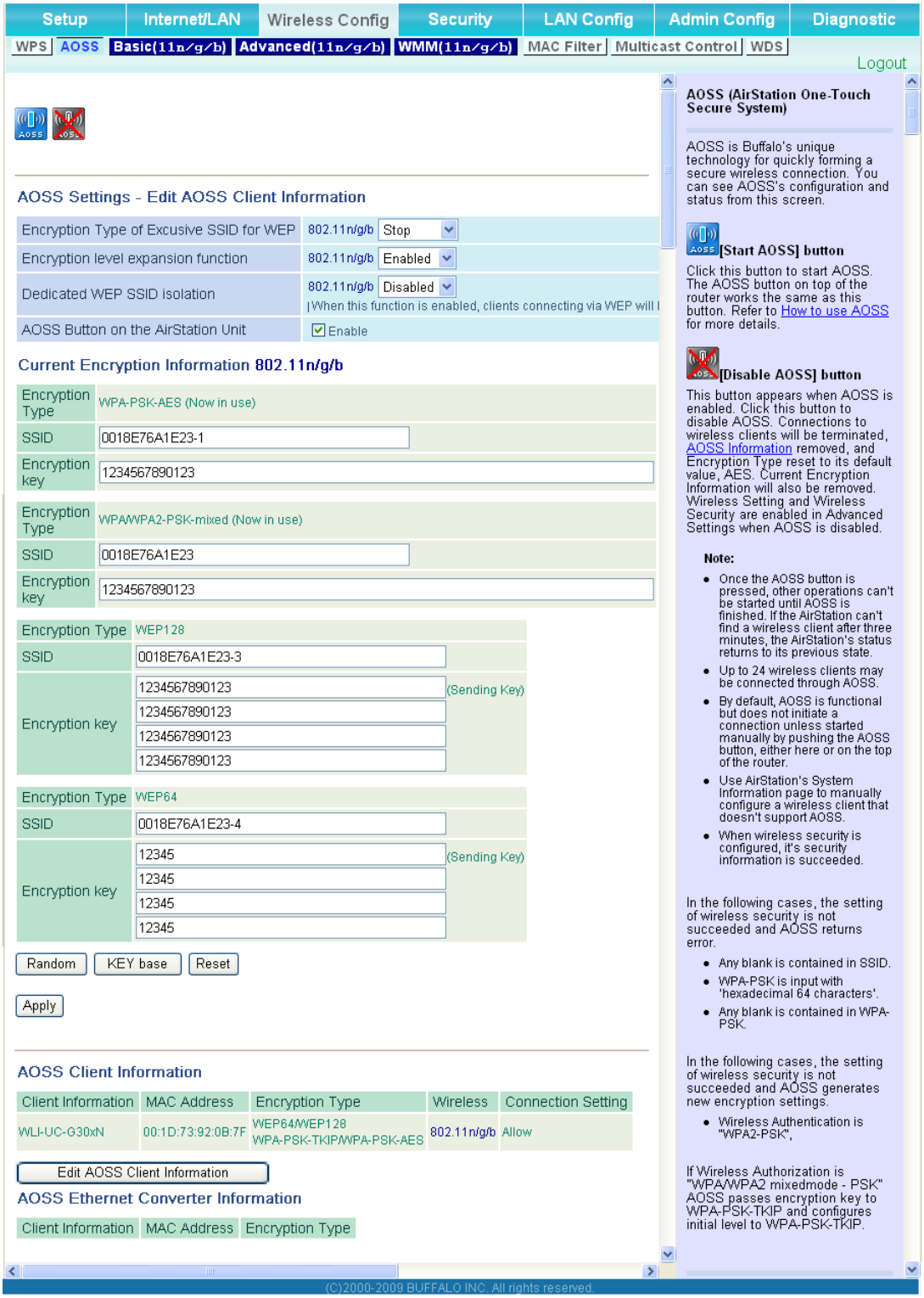
Configure WPS settings.



Parameter	Meaning
WPS	Enable to use WPS automatic configuration.
External Registrar	Enable to accept external configure requests from other WPS devices. Note: External configure requests will not be accepted if AOSS is in use.
AirStation PIN	Displays the PIN code of the AirStation. Clicking [Generate PIN] will generate a new PIN code. This code can be entered into other wireless devices that support WPS.
Enrollee PIN	Enter the PIN code for the other wireless device and click [OK].
WPS status	Displays [configured] if all available wireless bands are configured. Displays [unconfigured] if at least one wireless band is unconfigured.

AOSS

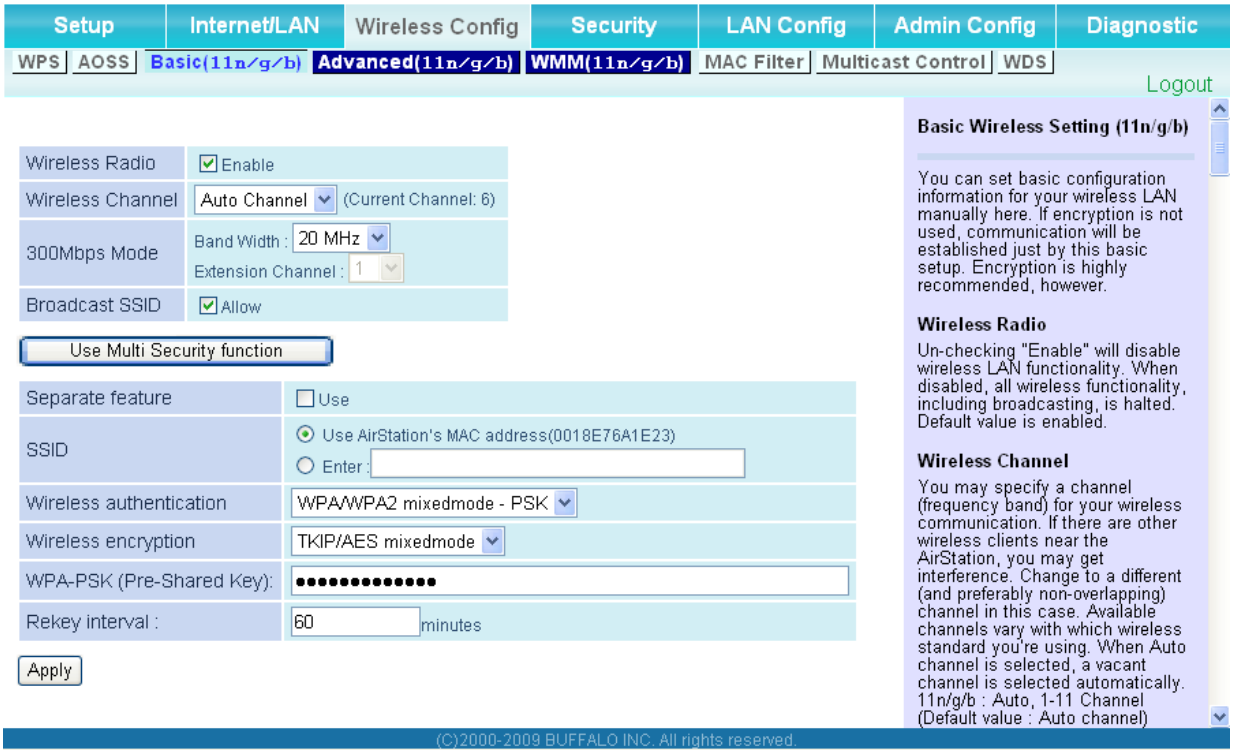
Configure and use AirStation One-touch Secure System (AOSS).



Parameter	Meaning
	Initiates AOSS automatic wireless configuration. Click this, then press or click the AOSS button on your AOSS-compatible wireless client. Repeat for additional AOSS clients.
	Click this button to disconnect all AOSS connections. Note: If AOSS connections are disconnected, the SSID and encryption keys will be restored to their most recent settings before using AOSS.
Encryption Type of Exclusive SSID for WEP	You may allow a separate SSID specifically for WEP connections. If [disabled] is selected, then clients will not be able to connect with WEP.
Encryption level expansion function	Expands security method from TKIP to WPA/WPA2-PSK-mixed mode.
Dedicated WEP SSID isolation	Set a separate SSID and network segment specifically for WEP connections. Devices connected with WEP will not be able to communicate with devices connected using AES/TKIP. All connected devices will be able to communicate with the internet.
AOSS Button on the AirStation Unit	Normally, pressing the physical AOSS button on the AirStation initiates AOSS. If this box is unchecked, it will not, and the button on this page will be the only way to initiate AOSS.
Current Encryption Information AOSS Connection only	Displays the encryption type, SSID, and encryption key that AOSS has configured.
[Random]	Click to enter random values for SSID, encryption key, and other settings.
[KEY base]	Click to return the SSID, encryption key, and other wireless settings to the values on the case sticker.
[Reset]	Click to return the SSID, encryption key, and other wireless settings to their previous values.
AOSS Client Information AOSS Connection only	Displays basic information for AOSS clients connected to the AirStation.
AOSS Ethernet Converter Information AOSS Connection only	Displays basic information for Ethernet converters connected to the AirStation via AOSS.

Basic

Configure basic wireless settings.



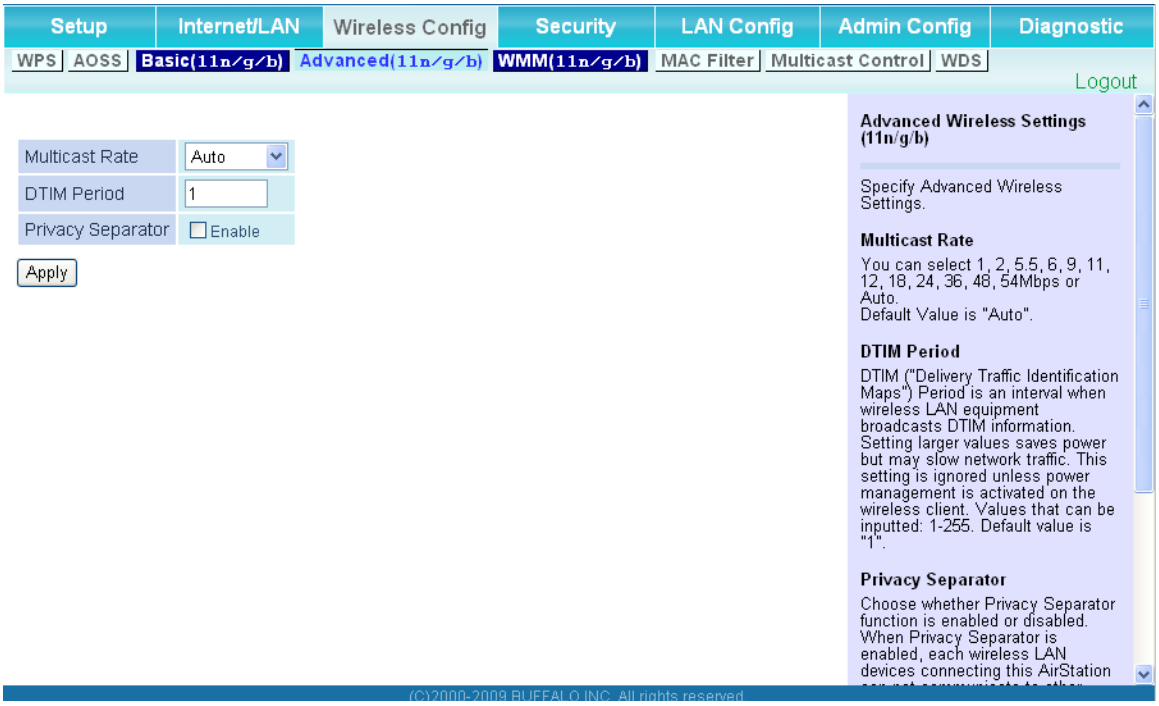
Parameter	Meaning
Wireless Radio	Determines whether or not to allow wireless communication. If this is unchecked, then no wireless connections will be allowed.
Wireless Channel	Sets a channel (a range of frequencies) used for wireless connections. Channels 1-11 are available. If Auto Channel selected, the AirStation will automatically use the best available channel.
300 Mbps Mode (WHR-HP-G300N) 150 Mbps Mode (WHR-HP-GN)	300/150 Mbps mode uses twice the normal frequency range, 40 MHz instead of 20 MHz. In uncongested areas this can increase performance. To use 300/150 Mbps mode, set the Bandwidth to 40 MHz and choose an Extension Channel. Note: If using Auto Channel for the wireless channel, then the Extension Channel is set automatically.

Parameter	Meaning
Broadcast SSID	If [Allow] is checked, then the AirStation will respond to SSID searches from wireless devices by broadcasting its SSID. If [Allow] is unchecked, then the AirStation ignore SSID searches from wireless devices.
[Use Multi Security function] [Do not use Multi Security function]	Clicking [Use Multi Security function] will enable Multi Security, allowing the use of multiple SSIDs, each with different wireless security settings. Clicking [Do not use Multi Security function] will disable the Multi Security function. The AirStation will then allow one SSID and one type of wireless security. Note: When using Multi Security, you need to enable at least one of the following SSID1, SSID2, or SSID3.
SSID1	Multi Security SSID1 can use WPA-PSK-TKIP or WPA/WPA2-Mixed for wireless security.
SSID2	Multi Security SSID2 can use WPA-PSK-AES for wireless security.
SSID3	Multi Security SSID3 can use WEP for wireless security.
Separate feature	When [Use] is checked, wireless devices connected to the AirStation can communicate only with the Internet side, not with each other.
SSID	SSIDs may contain 1-32 alphanumeric characters.
Wireless authentication	Choose an authentication method for wireless connections.

Parameter	Meaning
Wireless encryption	Select a type of data encryption for wireless communication from the following options: **No encryption** Data is transmitted without encryption. Avoid this option since any communication may be intercepted. [No encryption] can be selected only when [No authentication] is selected for wireless authentication. **WEP** WEP is a common encryption method supported by most devices. It uses an encryption key. WEP can only be selected when [No authentication] is selected for wireless authentication. **TKIP** TKIP is an encryption method which is more secure than WEP, but slower. Use an pre-shared-key to communicate with a wireless device. TKIP can be selected only when WPA-PSK or WPA2-PSK is selected for wireless authentication. **AES** AES is more secure than TKIP, and faster. Use a pre-shared-key to communicate with a wireless device. AES can be selected only when WPA-PSK or WPA2-PSK is selected for wireless authentication. **TKIP/AES mixed mode** TKIP/AES mixed mode allows both TKIP and AES authentication. TKIP/AES mixed mode can be selected only when WPA/WPA2 mixed mode - PSK is selected for wireless authentication.
WPA-PSK (Pre-Shared Key)	There are two different ways to enter pre-shared keys. Character keys may contain between 8 and 63 case-sensitive alphanumeric characters. Hexadecimal keys contain exactly 64 characters. Only 0 - 9 and a - f (not case-sensitive) should be used in hexadecimal keys.
Rekey interval	The rekey interval determines how often an encryption key is updated. Values from 0 to 1440 minutes may be entered.
Setup WEP encryption key	There are two different ways to enter WEP encryption keys. Character keys may contain either 5 or 13 case-sensitive alphanumeric characters. Hexadecimal keys may contain either 10 or 26 digits. Only 0 - 9 and a - f (not case-sensitive) should be used in hexadecimal keys.

Advanced

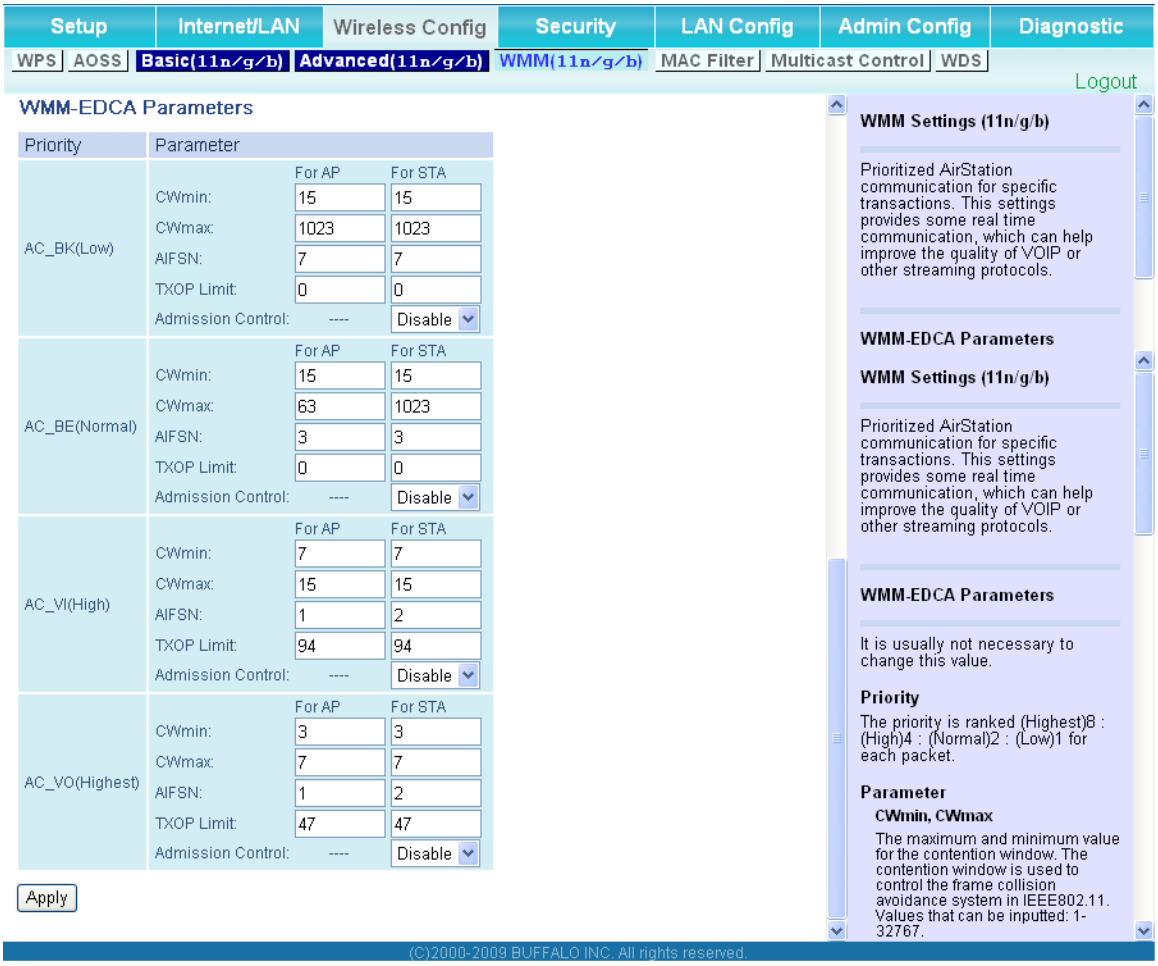
Don't change advanced wireless settings unless you know what you're doing.



Parameter	Meaning
Multicast Rate	Set the communication speed of multi-cast packets.
DTIM Period	Set the interval (1 -255) for the beacon to respond to a wireless device. This setting is only effective when power management is enabled on the wireless device.
Privacy Separator	If enabled, the Privacy Separator blocks communication between wireless devices connected to the AirStation. Wireless devices will be able to connect to the Internet but not with each other. Devices that are connected to the AirStation with wired connections will still be able to connect to wireless devices normally.

WMM

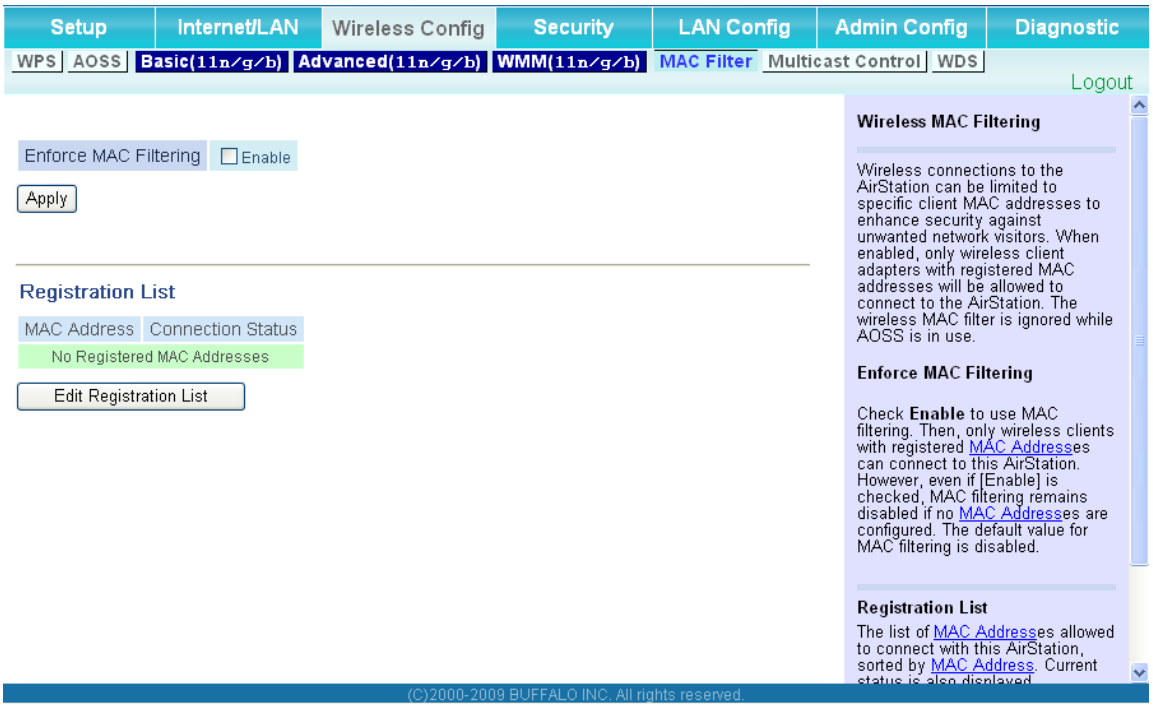
Configure QoS priorities here.



Parameter	Meaning
WMM-EDCA Parameters	You don't usually need to change these settings. Using the default settings is recommended. **Priority** The following priorities may be applied to individual transmission packets: (Highest) 8, (High) 4, (Normal) 2, and (Low) 1. From the queue, these packets are processed in order of priority. **CWmin, CWmax** The maximum and minimum value of the contention window. The contention window is used in the frame collision avoidance structure performed in IEEE802.11, and generally the smaller the value in the window, the higher the probability that the queue obtains the right to send. **AIFSN** The interval to send frames. The unit of the AIFSN is a slot, just as the window defined by CWmin and CWmax is. The smaller the interval of sending frames, the faster the algorithm can restart. As a result, the priority of the queue is higher. **TXOP Limit** The period of time that the queue can use after obtaining the right to send. The unit is 32 ms. The longer this time, the more frames can be sent per right to send. However, the que may interfere with other packet transmissions. If TXOP Limit is set to 0 (zero), only one frame can be sent per right to send. **Admission Control** Restricts new frames from interfering with a previous queue. New packets are prioritized lower until a queue of them is collected. As the new queue accumulates more packets, its priority increases.

MAC Filter

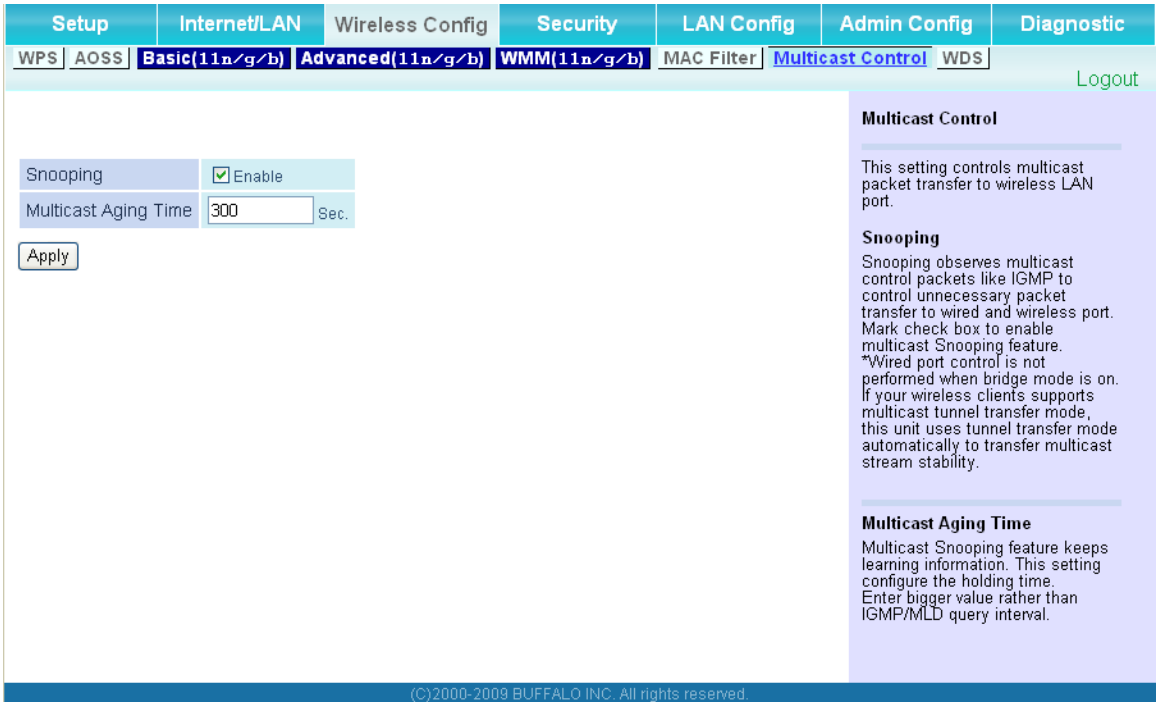
This screen lets you restrict wireless access to wireless devices with specific MAC addresses.



Parameter	Meaning
Enforce MAC Filtering	Enable to restrict wireless connections to devices with registered MAC addresses.
Registration List	Displays the MAC addresses of registered devices which are permitted to connect wirelessly.
[Edit Registration List]	Click this button to add a MAC address of a wireless device to the list of permitted devices.
MAC Addresses to be Registered	Enter a MAC address of a wireless device you permit to connect to the AirStation. Click [Register] to add that MAC address to the list.
List of all clients that are associated with this AirStation	Display the list of all MAC addresses of wireless devices connected to the AirStation.

Multicast Control

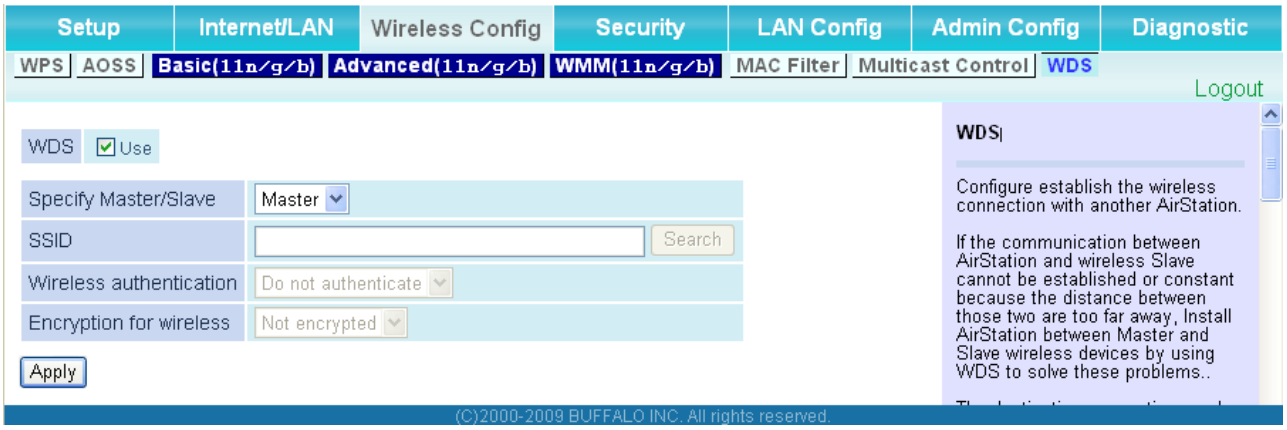
Restrict unnecessary multicast packets from wireless LAN ports.



Parameter	Meaning
Snooping	If enabled, snooping supervises multicast administrative packets such as IGMP and restricts unnecessary multicast transfers to wired or wireless ports.
Multicast Aging Time	Set the time to hold the data from multicast snooping in the range of 1 to 3600 (seconds). Enter a value larger than the interval of a IGMP/MLD query.

WDS

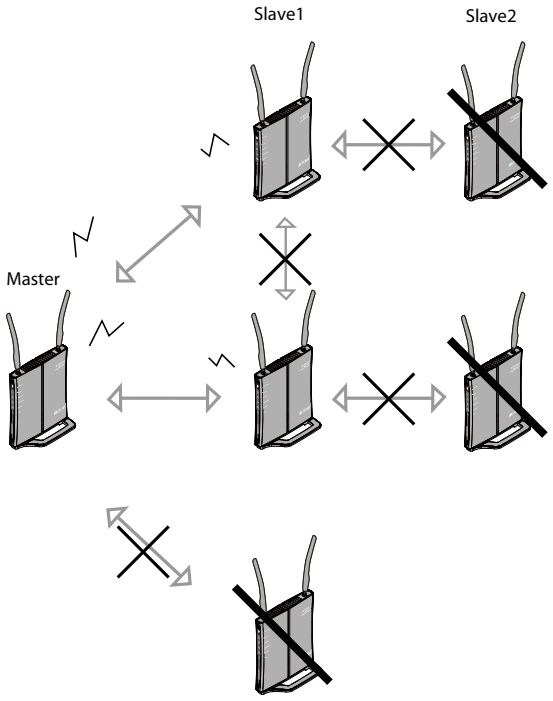
WDS bridging allows communication between AirStations.



Parameter	Meaning
WDS	Check to use WDS bridging.
Specify Master/Slave	Define this AirStation's role in a WDS bridge. **Master** This AirStation will the master in a WDS bridge. It will have the Internet connection, and other AirStations in the bridge will be connected through this AirStation. **Slave** Set AirStation as a slave. This can be connected with the AirStation which is set as a master by using WDS feature only if the Master AirStation supports WDS. **Slave (EC)** Set AirStation as a slave. This uses Ethernet Converter to connect with the AirStation which is set as a master, so it can be connected even though Master AirStation does not support WDS. **Auto** Automatically switches between Master and Slave modes depending on the surrounding network. If an AirStation works as a router, it will automatically be set as a master. If the Airstation works as a bridge and a DHCP server exists in the network, it will automatically be set as a master . If the AirStation works as a bridge and no DHCP server is available, it will automatically be set as a slave.

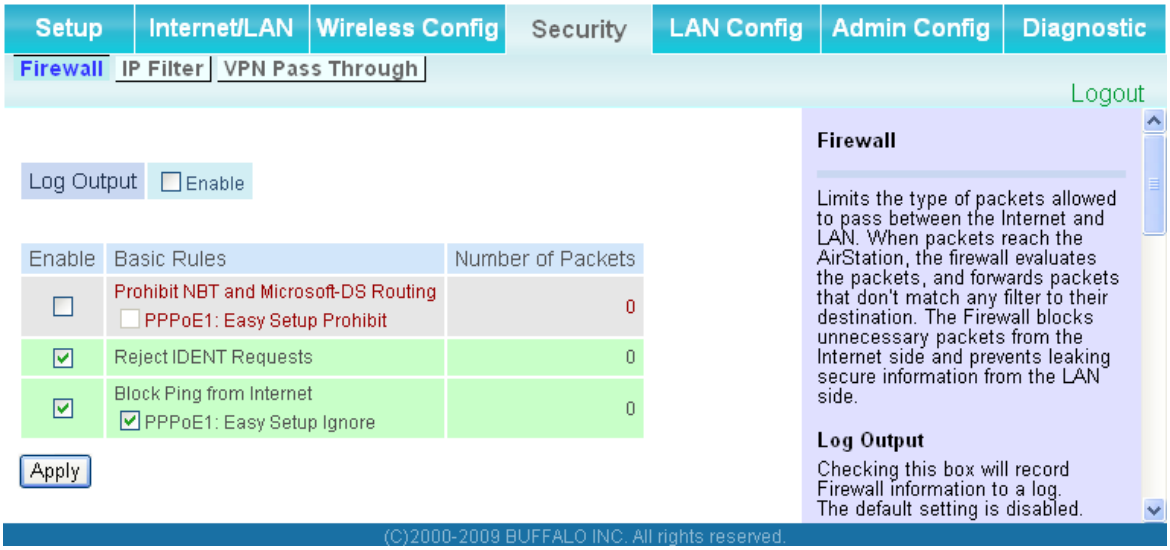
Parameter	Meaning
SSID	Configure the Master Airstation's SSID.
[Search]	Click to search for other AirStations' SSIDs.
Wireless authentication	Configure authentication method for the master AirStation
Encryption for wireless	Choose encryption type for the master AirStation.
WPA-PSK (Pre Shared Key)	Set the master AirStation's Encryption key.

Notes: A master AirStation can communicate with two slaves only.
A slave AirStation cannot communicate with any AirStation other than its master.



Security (Router Mode only)

Firewall (Router Mode only)

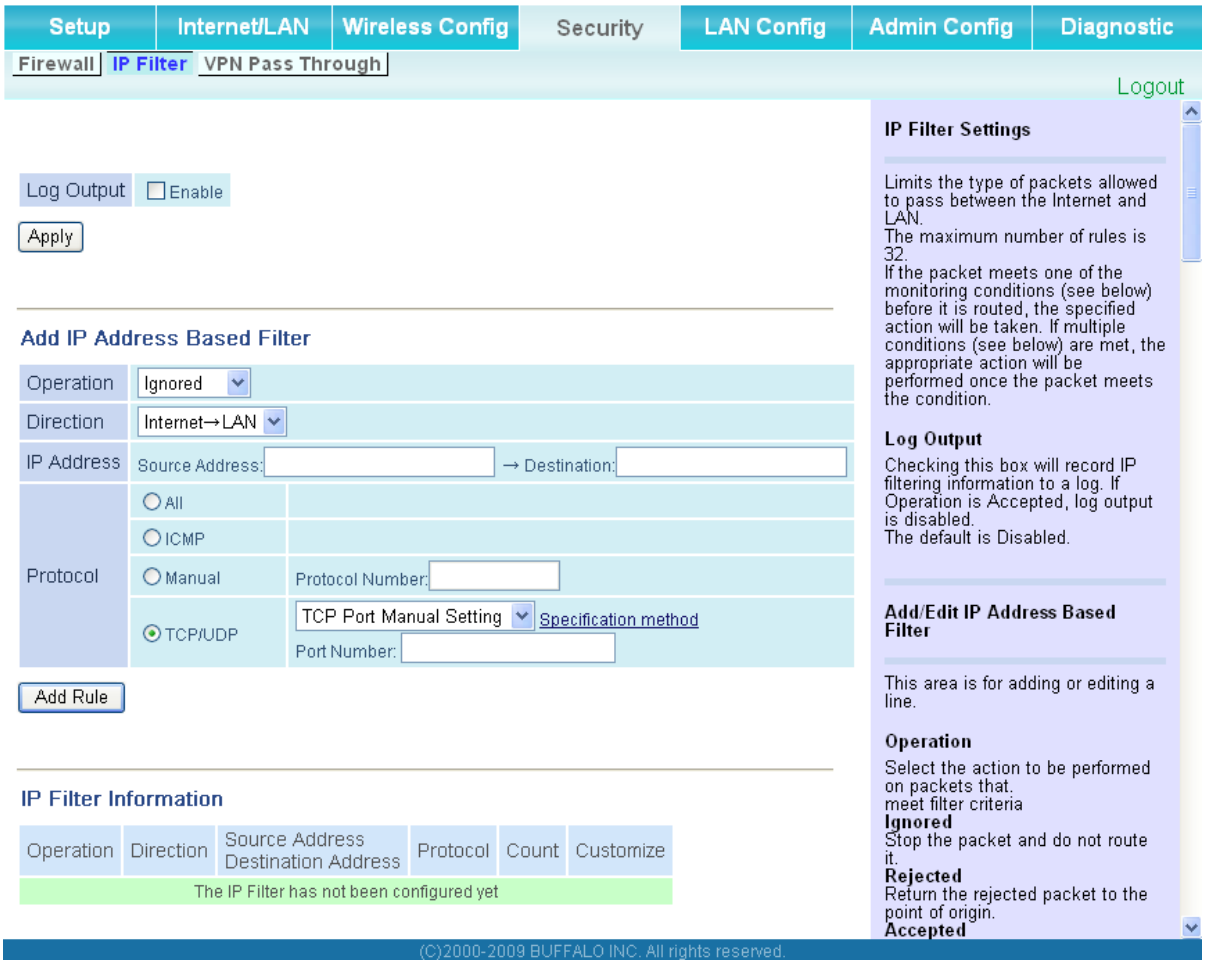


Parameter	Meaning
Log Output	Enable to output a log of firewall activity.
Basic Rules	Enable to use any of the quick filters. Preconfigured quick filters include: **Prohibit NBT and Microsoft-DS Routing** When enabled, this prevents Microsoft networking from communicating between the LAN side and the WAN side. You can configure this with PPPoE if you select [Use PPPoE Client] or [Use IP Unnumbered] in Method of Acquiring IP address, or if Easy Setup identified a PPPoE connection during setup.

Parameter	Meaning
	Reject IDENT Requests Enabling this option will answer IDENT requests from the Internet side with corresponding rejection packets. Enable this option if you experience slow transfer speeds for network applications such as email, ftp, or browsing. If you have configured transfer of IDENT requests to the LAN side in the address translation settings (DMZ or TCP port:113), that setting has higher priority, and overrides this setting. **Block Ping from Internet** If this is enabled, the AirStation will not respond to pings from the Internet side. You can configure this with PPPoE if you select [Use PPPoE Client] or [Use IP Unnumbered] in Method of Acquiring IP address (page 34), or if Easy Setup identified a PPPoE connection during setup.

IP Filter (Router Mode only)

Create and edit IP filters.



Parameter	Meaning
Log Output	If enabled, IP filter activity is saved to a log.
Operation	Specify how to process target packets.
Direction	Specify the transmission direction of target packets.
IP Address	Specify the sender's IP address and receiver's IP address of the target packets.
Protocol	Select a protocol for target transmission packet.
IP Filter Information	Display the list of IP filters which have been registered.

VPN Pass Through (Router Mode only)

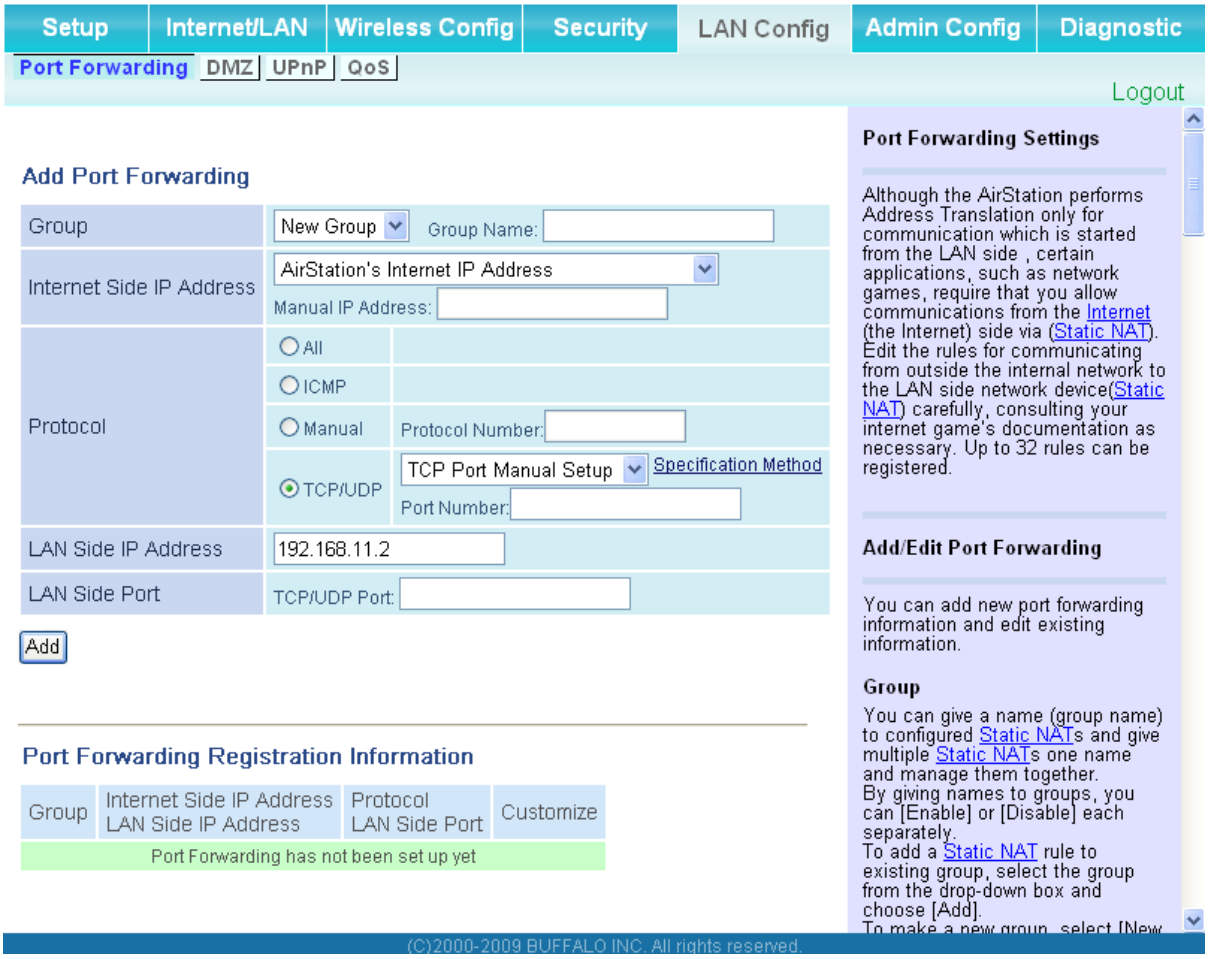
Configure IPv6 pass through, PPPoE pass through, and PPTP pass through.

Parameter	Meaning
IPv6 Pass Through	Enable to use IPv6 Pass Through for address translation.
PPPoE Pass Through	Enable to use PPPoE bridge. Using PPPoE bridge lets you automatically obtain an IP address from your provider using the PPPoE protocol from your computer connected to the LAN side because all PPPoE packets can pass through between the Internet and LAN.
PPTP Pass Through	Enable to use PPTP Pass Through for address translation.

LAN Config (Router Mode only)

Port Forwarding (Router Mode only)

Configure port translation.



Parameter	Meaning
Group	Specify a group name for a new rule to belong to. Select [New Group] and enter the new group name in the Group Name field to create a new group. A group name can include up to 16 alphanumeric letters.
Internet Side IP Address	Enter the Internet side IP address (before translation) for the port translation table entry.
Protocol	Select the Internet side protocol (before translation) for the port translation table entry.

Parameter	Meaning
LAN Side IP Address	Enter the LAN side IP address (after translation) for the port translation table entry.
LAN Side Port	Select the LAN side (after translation) port number (1 - 65535) for the port translation table entry.
Port Forwarding Registration Information	Shows current entries in the port translation table.

DMZ (Router Mode only)

Configure a destination to transfer communication packets without a LAN side destination.

Parameter	Meaning
IP Address of DMZ	Enter the IP address of the destination to which packets which are not routed by a port translation table are forwarded. Note: RIP protocol packets (UDP port number 520) will not be forwarded.

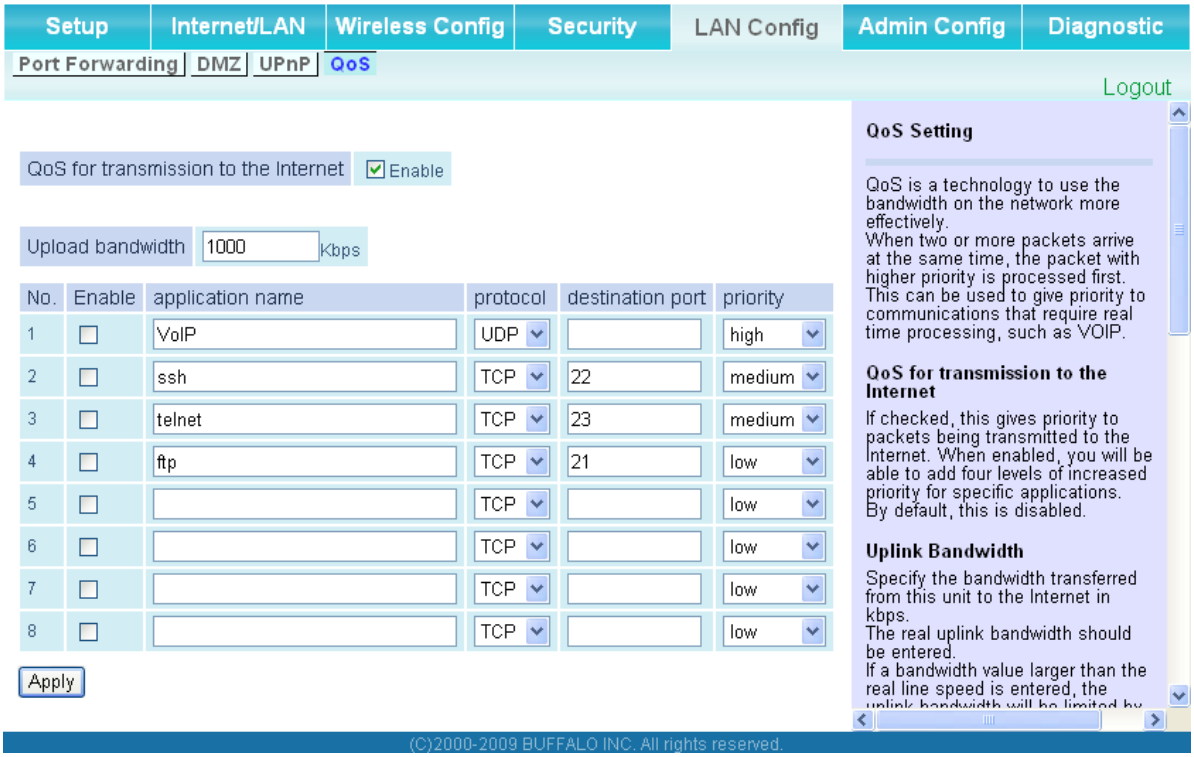
UPnP (Router Mode only)

Configure Universal Plug and Play.

Parameter	Meaning
UPnP	Enable or disable Universal Plug and Play (UPnP) functionality.

QoS (Router Mode only)

Configure the priority of packets sent to the Internet.



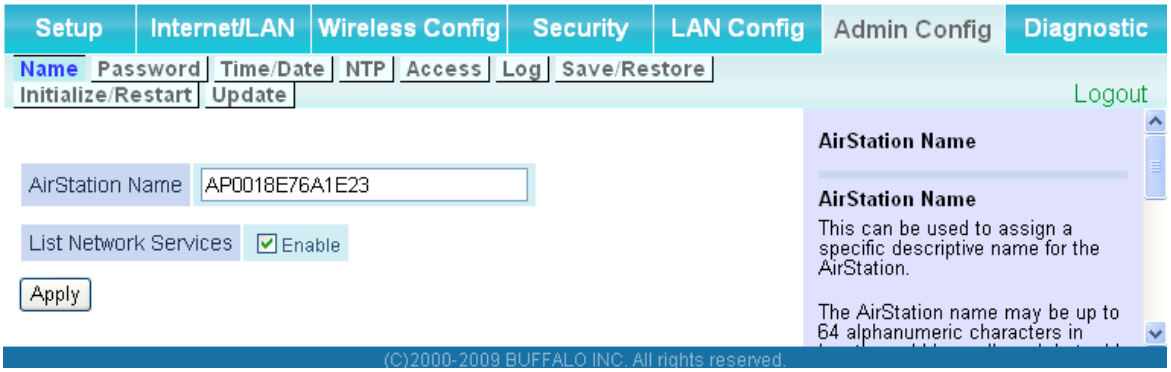
Parameter	Meaning
QoS for transmission to the Internet	Enable to give priority to specific types of Internet traffic.
Upload bandwidth	Specify the upstream bandwidth in kbps from the AirStation to the internet side. Set the actual value for the upstream bandwidth.
Enable	Check to enable desired entries, then click [apply].
application name	Enter an application name. Names may use up to 32 alpha numerical characters, double or single tick marks ("'), quotation marks (“), and semicolons (;).
protocol	Select either TCP or UDP.

Parameter	Meaning
destination port	Specify a destination port with the value of 1 - 65535. If this field is empty, a random port is selected.
priority	Select high, medium or low. If packets do not qualify for classification as a type on the list, then their priority is treated as a level between medium and low.

Admin Config

Name

Configure the AirStation's name.



Parameter	Meaning
AirStation Name	Enter a name for the AirStation. Names may include up to 64 alphanumeric characters and hyphens (-).
List Network Services	Enable display the computers and devices on your network with their supported services.

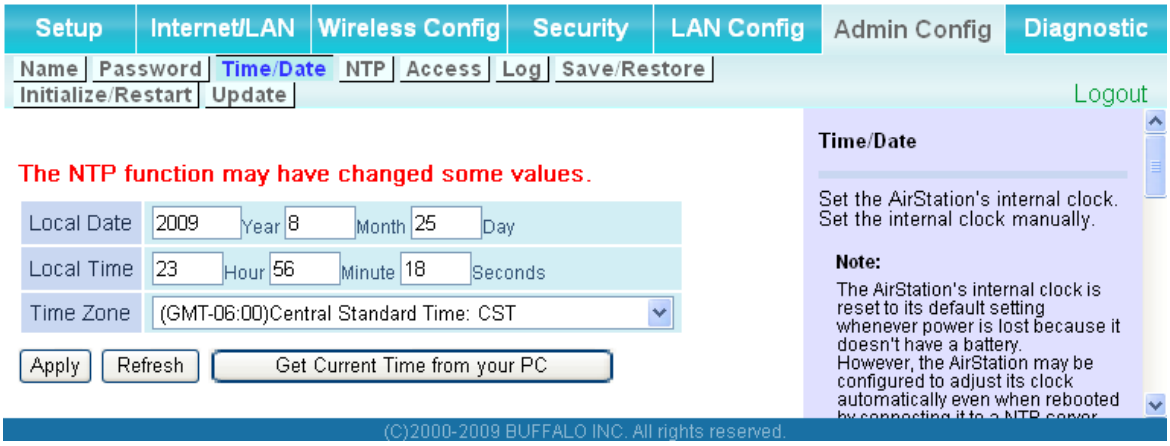
Password

Configure the login password for the AirStation's configuration utility.

Parameter	Meaning
Administrator Name	[root] is the configuration utility's user name for login. This name is fixed.
Administrator Password	Enter a password for logging in to the AirStation's configuration utility. The password may contain up to 8 alphanumeric characters and underscores (_).

Time/Date

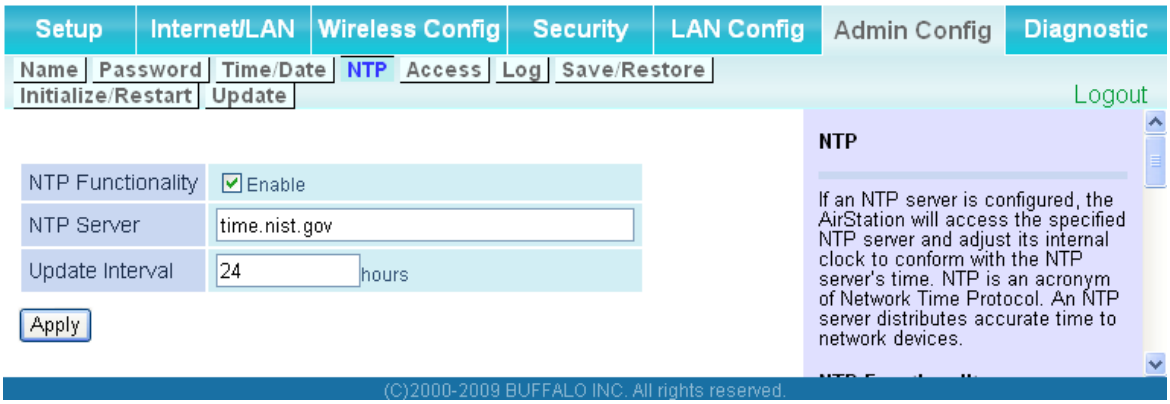
Configure the AirStation's internal clock.



Parameter	Meaning
Local Date	You may manually set the date of the AirStation's internal clock.
Local Time	You may manually set the time of the AirStation's internal clock.
Time Zone	Specify the time zone (offset of Greenwich Mean Time) of the AirStation's internal clock.

NTP

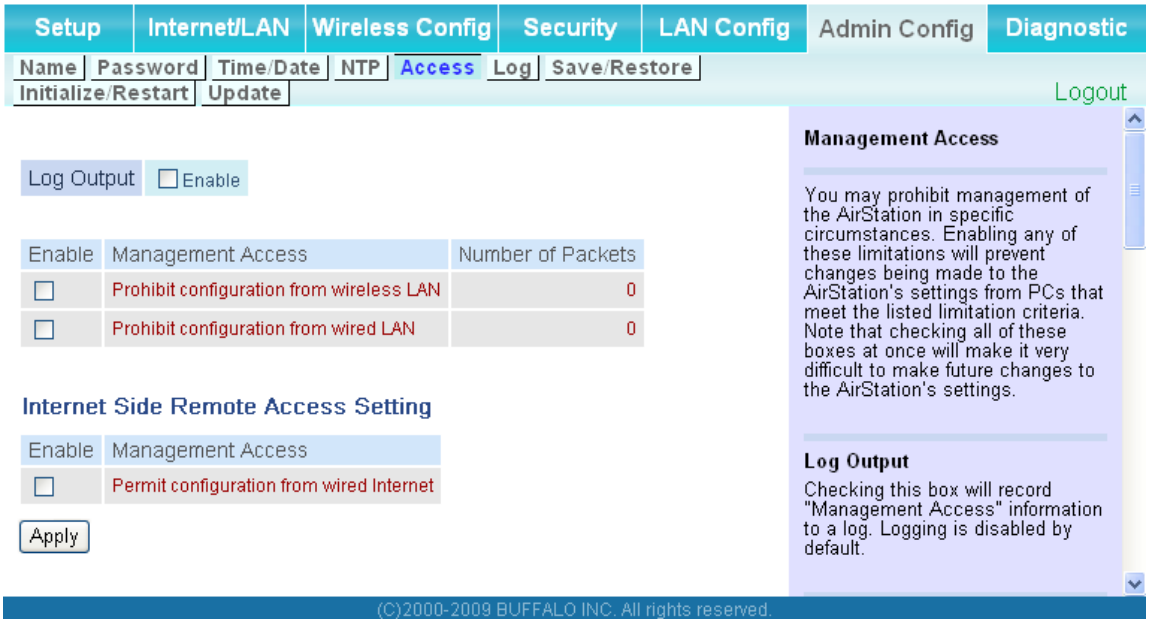
Configure the AirStation's internal clock to automatically synchronize with an NTP server.



Parameter	Meaning
NTP Functionality	Enable to use an NTP server to automatically set the AirStation's internal clock.
NTP Server	Enter the name of the NTP server as a host name, host name with domain name, or IP address. Up to 255 alphanumeric characters, hyphens (-), and underscores (_) may be used.
Update Interval	How often should the AirStation submit a time request to the NTP server? Intervals of 1 - 24 hours may be set.

Access

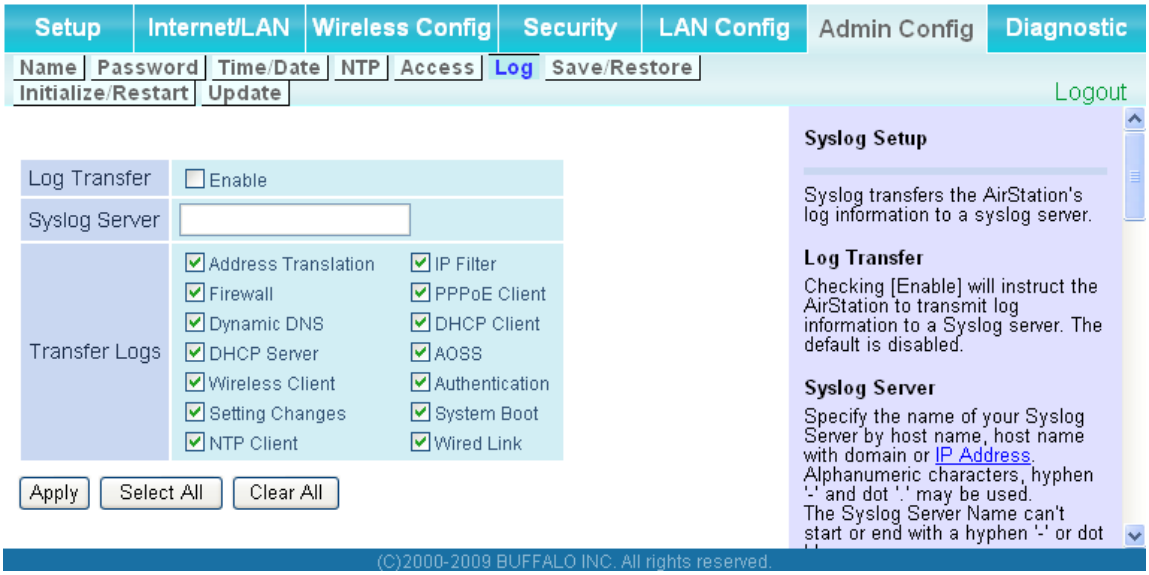
You may restrict access to the AirStation's settings screens.



Parameter	Meaning
Log Output	Enabling outputs a log of changes to access settings.
Prohibit configuration from wireless LAN	If enabled, prevents access to settings screens from wirelessly connected devices (only wired devices may configure).
Prohibit configuration from wired LAN	If enabled, prevents access to settings screens from wired devices (only wirelessly connected devices may configure).
Permit configuration from wired Internet	If enabled, allows access to settings screens from network devices on the Internet side.
Permitted IP address	Displayed only if Internet side configuration is enabled. Enter the IP address of the device that is permitted to configure the AirStation remotely from the Internet side.
Permitted Port	Displayed only if Internet side configuration is enabled. Set a port number (1 - 65535) if configuring the AirStation from the Internet side.

Log

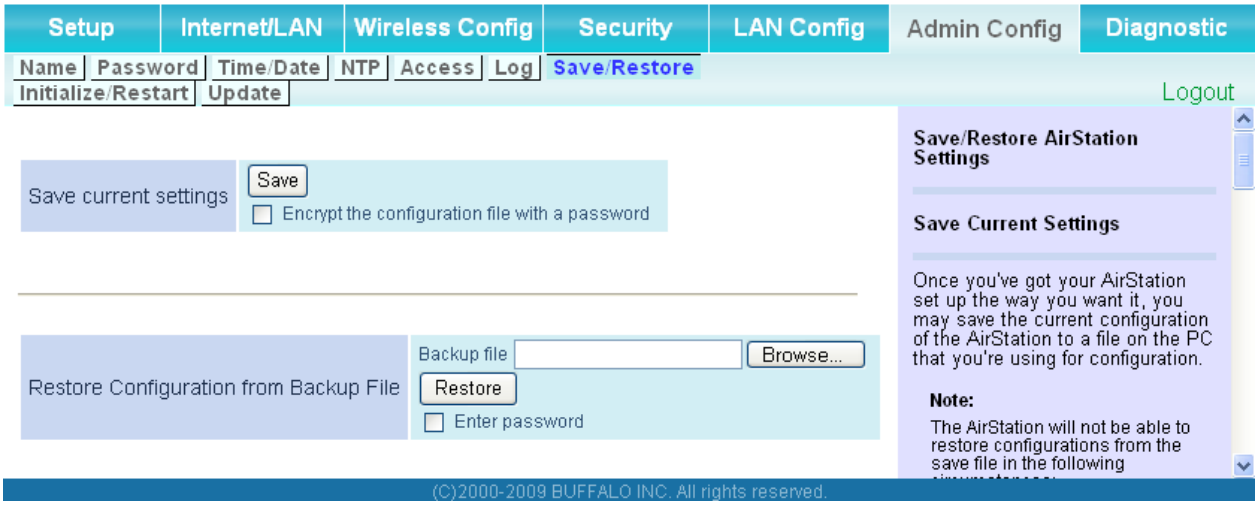
You may use a syslog server to manage the AirStation's logs.



Parameter	Meaning
Log Transfer	Enable to send logs to a syslog server.
Syslog Server	Identify the syslog server by host name, host name with domain name, or IP address. You may enter up to 255 alphanumeric characters, hyphens (-), and underscores (_).
Transfer Logs	Choose which logs will be transferred to the syslog server.

Save/Restore

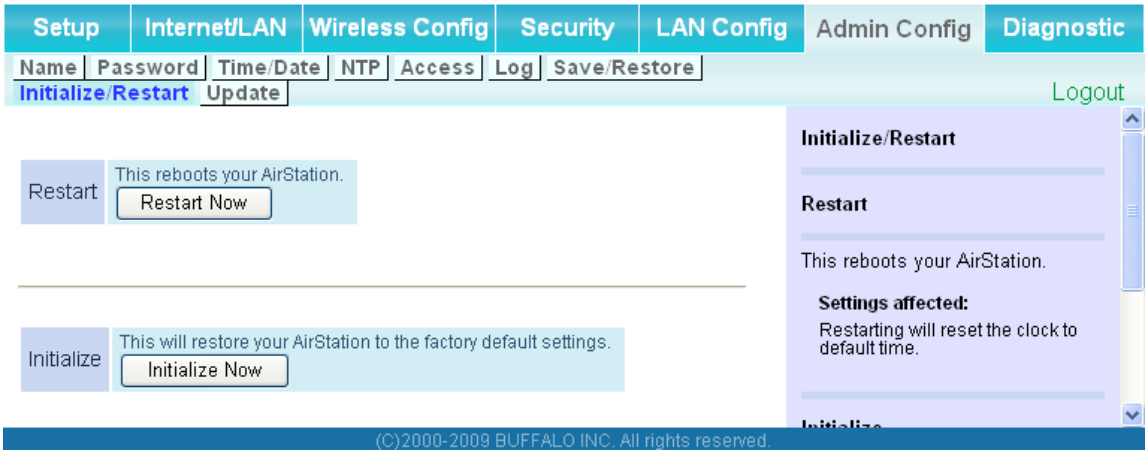
You may save your AirStation's settings as a file and restore settings from that file later.



Parameter	Meaning
Save current settings	Clicking [Save] will save the current configuration of the AirStation to a file. If the [Encrypt the configuration file with a password] option is checked, then the configuration file will be password protected with the current Administrator Password.
Restore Configuration from Backup File	Restore the configuration of the AirStation from a saved configuration file by clicking the [Browse...] button, navigating to the configuration file, and then clicking Restore. If the configuration file was password protected, then put a check next to [To restore from the file you need the password], enter the password, and click [Open].

Initialize/Restart

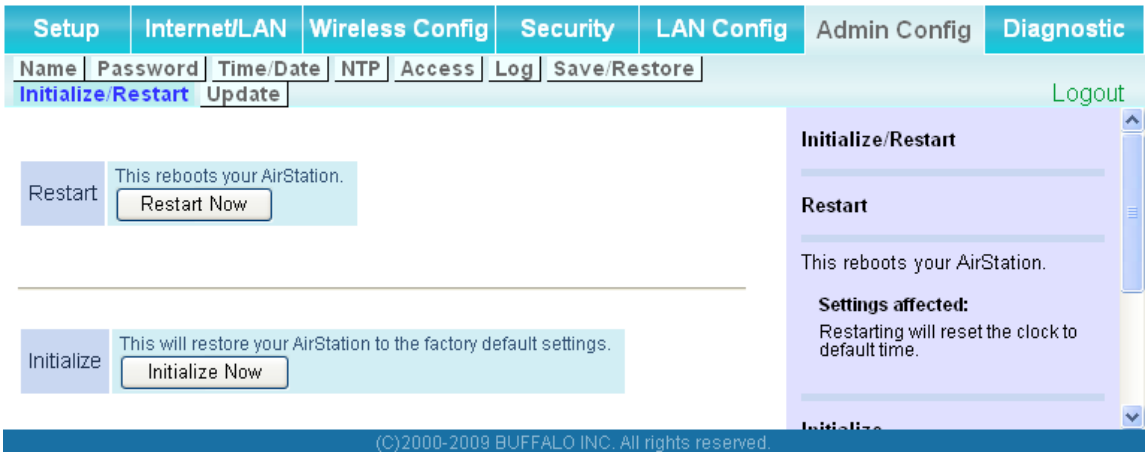
Reboot or initialize the AirStation.



Parameter	Meaning
Restart	Click [Restart Now] to restart the AirStation.
Initialize	Click [Initialize Now] to initialize and restart the AirStation.

Update

Update the AirStation's firmware.

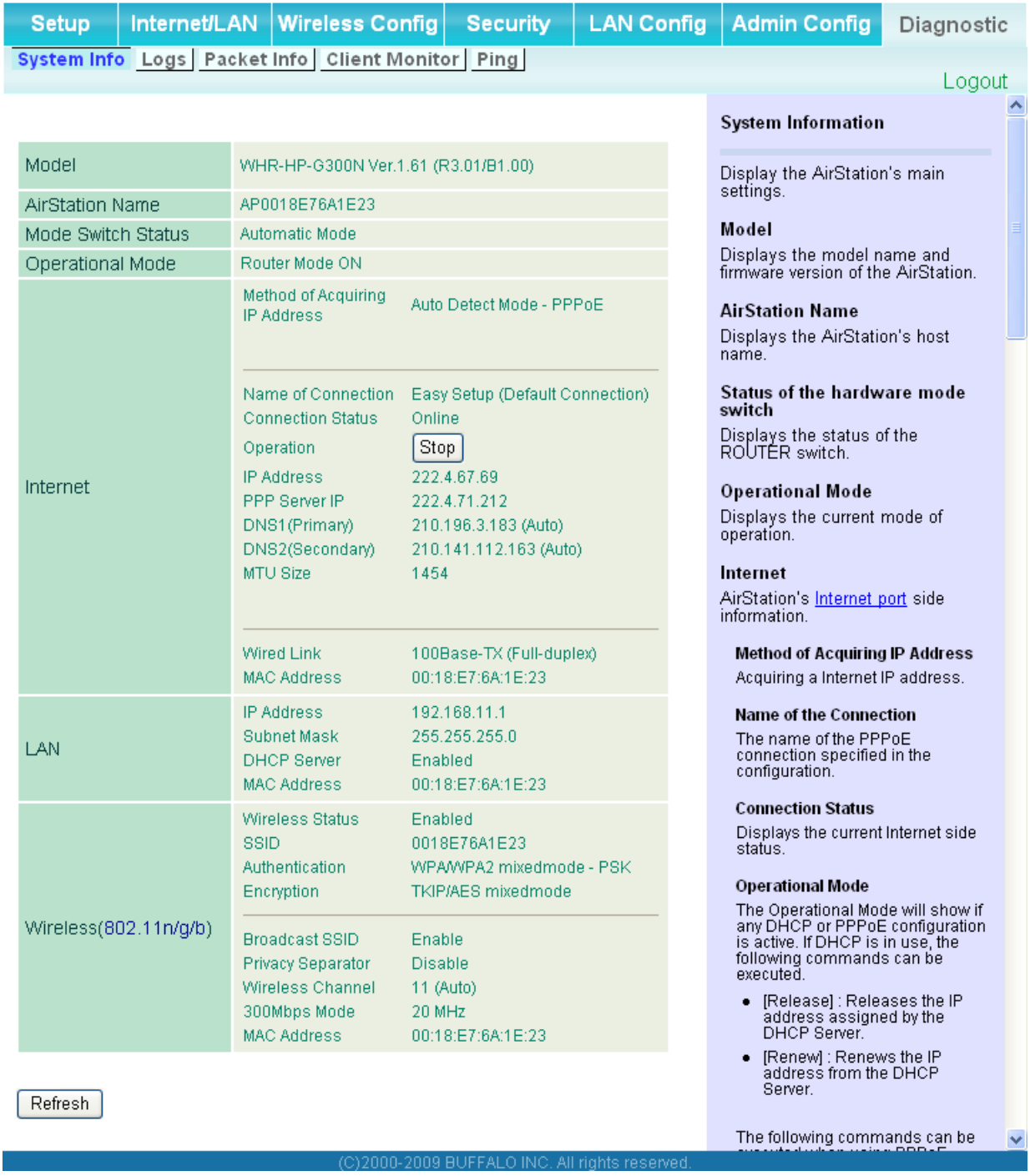


Parameter	Meaning
Firmware Version	Displays the current firmware version of the AirStation.
Firmware File Name	Click [Browse...] and navigate to a firmware update file. Click [Update Firmware].

Diagnostic

System Info

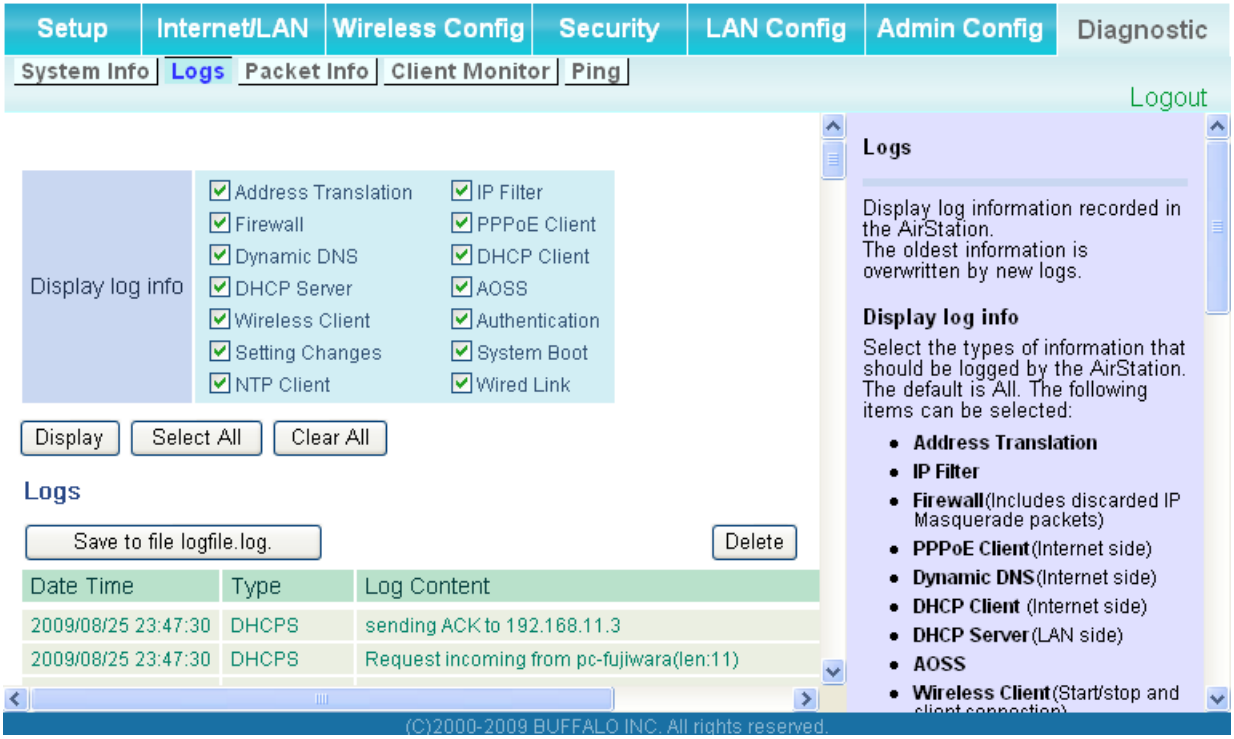
This screen displays the AirStation's system information.



Parameter	Meaning
Model	Displays the product name of the AirStation and the firmware version.
AirStation Name	Displays the AirStation's Name.
Mode Switch Status	Displays the status of the mode switch on the back of the AirStation.
Operational Mode	Displays the current operational mode of the AirStation.
Internet	Displays the information about the Internet port.
LAN	Displays the information about the LAN port.
Wireless	Displays the wireless status.

Logs

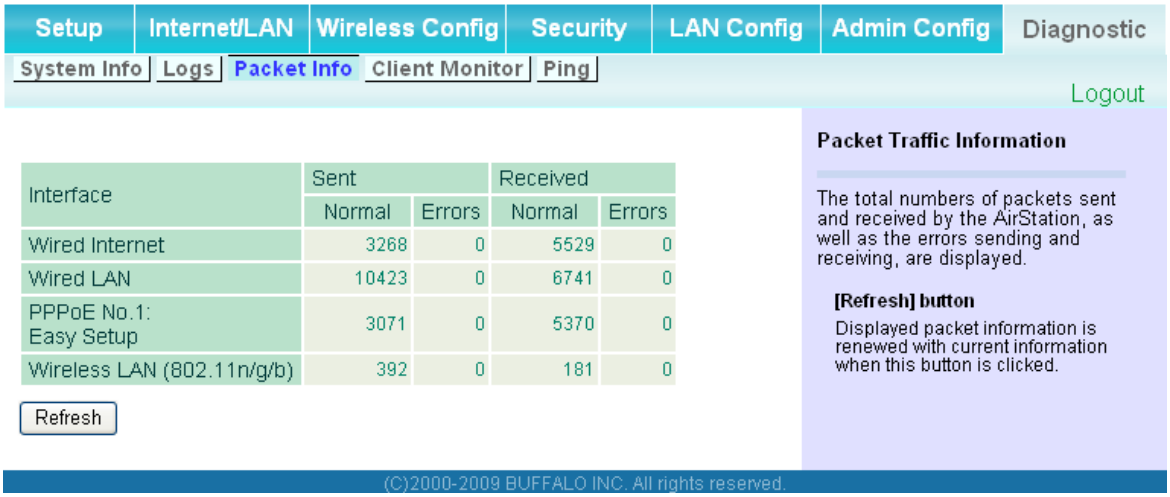
Check the AirStation's logs.



Parameter	Meaning
Display log info	Choose the types of log information to display.
Save to file	Saves selected logs to the file logfile.log.

Packet Info

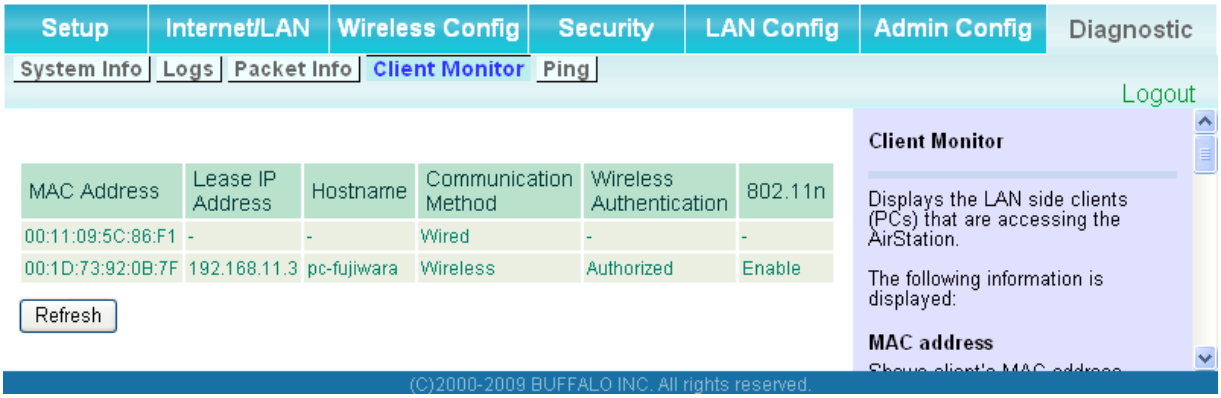
Verify transferred packets.



Parameter	Meaning
Sent	Displays the number of packets sent to the Internet side of Ethernet, the LAN side of the Ethernet, and the LAN side of the wireless connection.
Received	Displays the number of packet received from the Internet side of Ethernet, the LAN side of the Ethernet, and the LAN side of the wireless connection.

Client Monitor

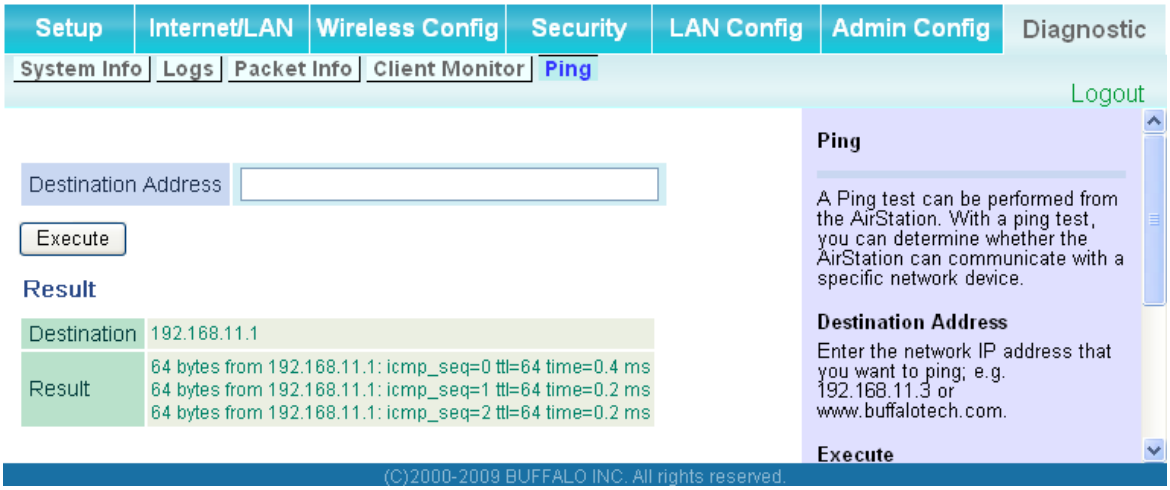
This screen list connected devices.



Parameter	Meaning
Client Monitor	Displays information (MAC address, lease IP address, host name, communication method, wireless authentication and 802.11n) for devices that are connected to the AirStation.

Ping

A Ping test checks whether the AirStation can communicate with a specific network device.



Parameter	Meaning
Destination Address	Enter an IP address or a host name for the target device and click [Execute]. The AirStation will attempt to communicate with that device and the result will be displayed in the [Result] field.

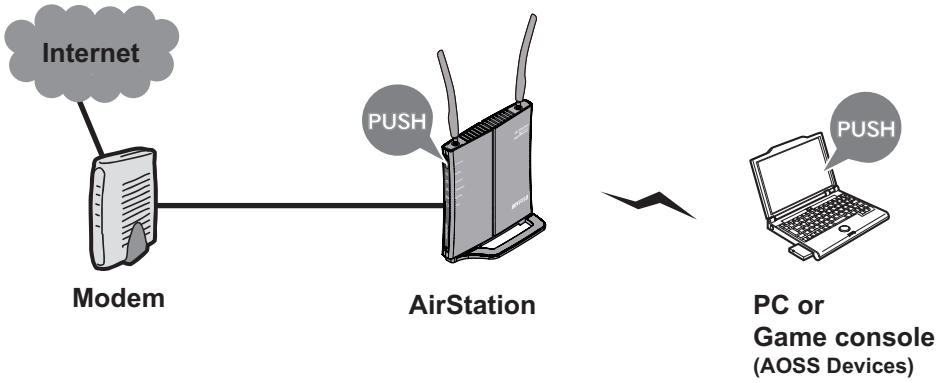
Note : Examples in this manual show the "User-friendly" firmware. The dd-wrt based Professional firmware is somewhat different. For more information on the Professional firmware, visit dd-wrt's website at ***www.dd-wrt.com***.

Chapter 5
Connect to a Wireless Network

Automatic Secure Setup (AOSS/WPS)

AOSS and WPS are systems which enable you to automatically configure wireless LAN settings. Just pressing the buttons will connect wireless devices and complete security settings. Easily connect to any wireless devices, computers, or game machines which support AOSS or WPS.

AOSS (AirStation One-Touch Secure System) was developed by Buffalo Technology. WPS was created by the Wi-Fi Alliance.



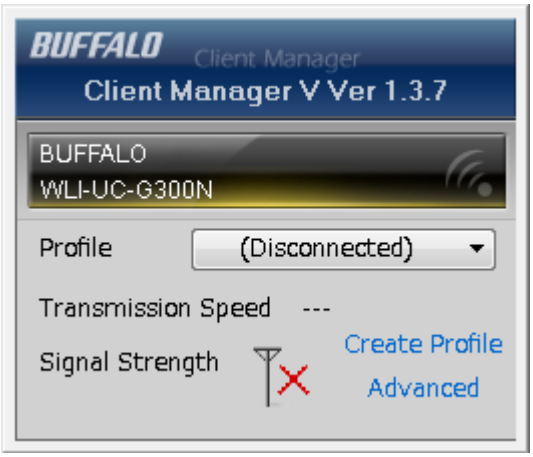
- Before using AOSS or WPS to connect to a Buffalo wireless client, install Client Manager software from the included AirNavigator CD. Consult your wireless client's documentation for more information.
- Buffalo's Client Manager software can be used with the wireless LAN devices built into your computer. However, it is not guaranteed to work with all wireless LAN devices available. Some wireless clients may require manual setup.

Windows 7/Vista (Client Manager V)

If you are using Windows 7 or Windows Vista, use the included Client Manager V software to connect wirelessly with AOSS/WPS.

1 Click the icon in the system tray.

2



Click [Create Profile].

3 When the message "A Program needs your permission to continue" appears, click [Yes] or [Continue].

4

Click the [WPS AOSS] button.

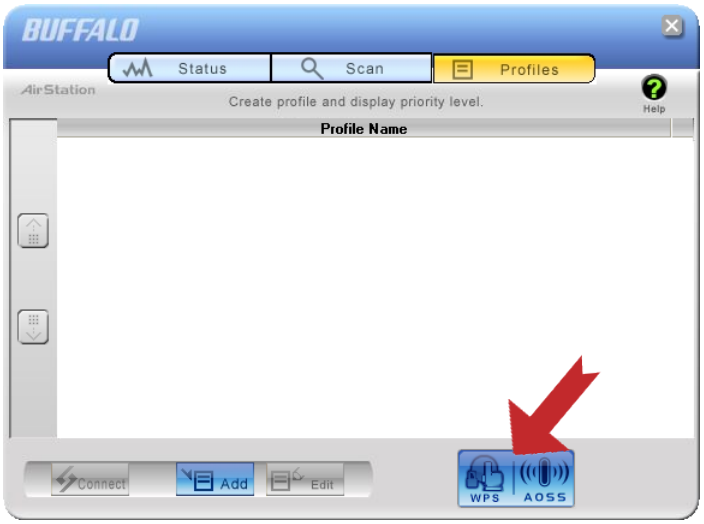
Follow any instructions displayed on the screen. When the Security LED on the front of the AirStation stops flashing and is lit steadily, the connection is complete.

Windows XP (Client Manager 3)

If you are using Windows XP, use Client Manager 3 to connect wirelessly with AOSS/WPS.

1 Right click on the icon in the system tray, and select [Profile].

2



Click the [WPS AOSS] button.

Follow any instructions displayed on the screen. When the Security LED on the front of the AirStation stops flashing and is lit steadily, the connection is complete.

Other Devices (e.g. Game Console)

If you are using a game machine which supports AOSS or WPS, refer to that device's manual to initiate AOSS/WPS. When instructed, hold down the AOSS button on the AirStation for 1 second.

When the Security LED stops blinking and is lit steadily, the connection is complete.

Manual Setup

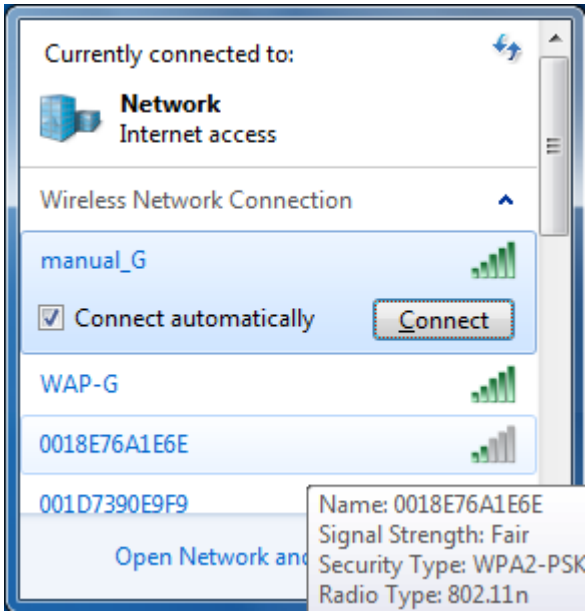
You can also connect to the AirStation without installing Client Manager V or Client Manager 3 by using the utility built-in to Windows. The procedure varies depending on which version of Windows you are using.

Windows 7 (WLAN AutoConfig)

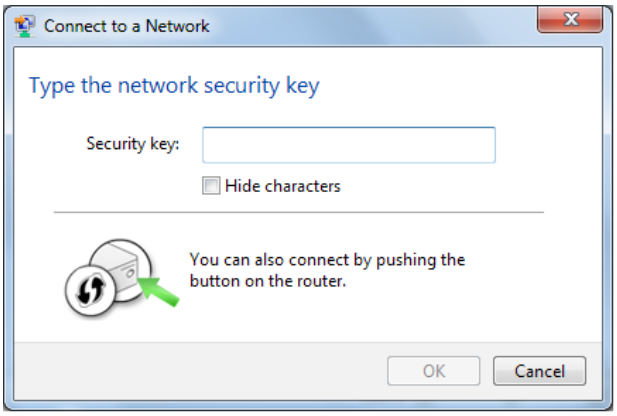
With Windows 7, use WLAN AutoConfig to connect to the AirStation.

1 Click on the network icon  in the system tray.

2



Select the target AirStation's name and click [Connect]. If you will be connecting to this device in the future, checking [Connect automatically] is recommended.

3 

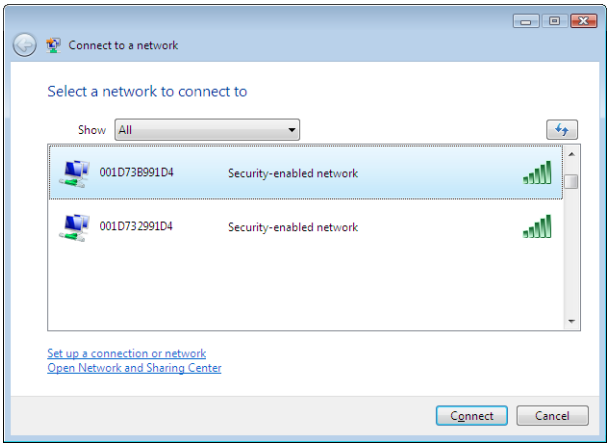
Enter the encryption key and click [OK].

Windows Vista (WLAN AutoConfig)

With Windows Vista, use WLAN AutoConfig to connect to the AirStation.

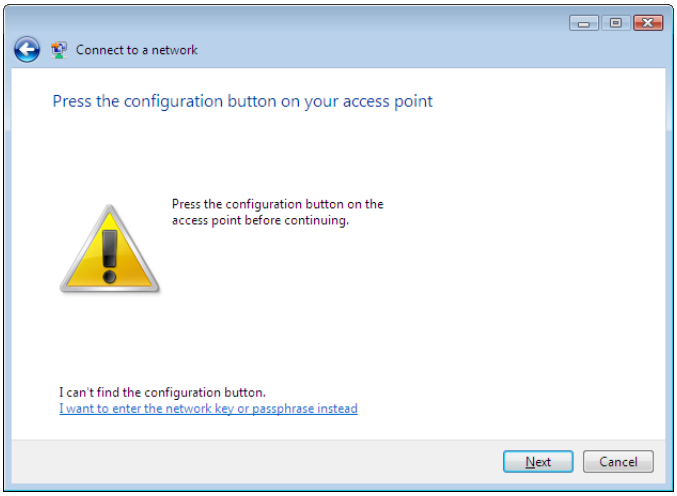
1 Right click on the wireless network icon  in the system tray.

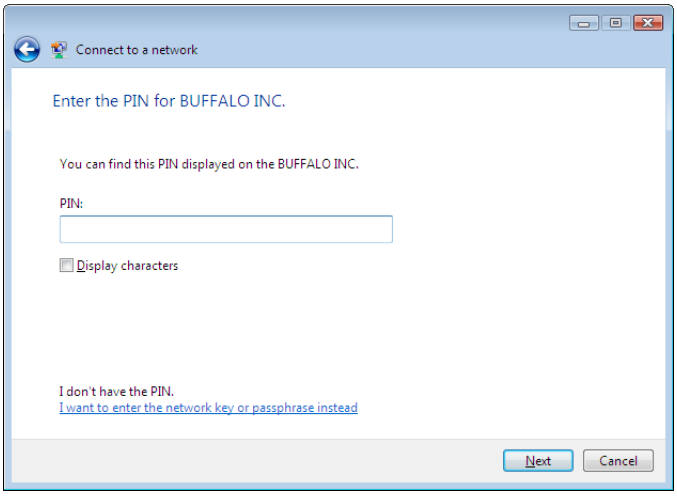
2 Click [Connect to a network].

3 

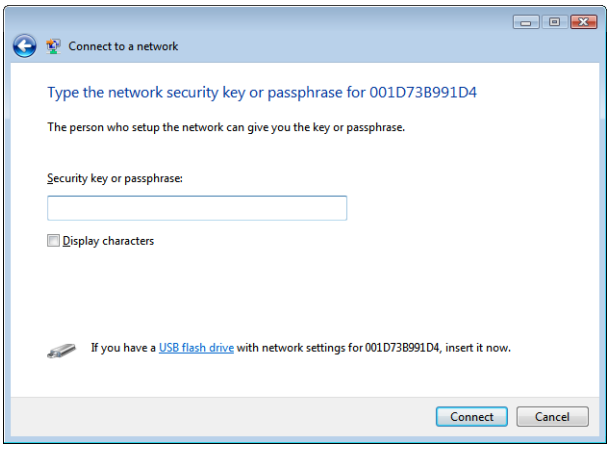
When the screen at left is displayed, select the network to connect to and click [Connect].

If the screen below is displayed, click [I want to enter the network key or passphrase instead]. Otherwise, go to step 4.





4



Enter the encryption key and click [Connect].

Step through the wizard to finish configuration. If the Set Network Location screen is displayed, select [Home], [Work], or [Public location] depending where you're using the AirStation.

Windows XP (Wireless Zero Configuration)

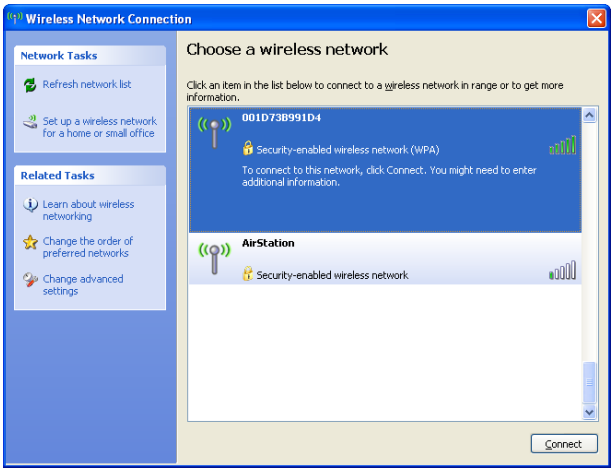
Windows XP includes a built-in utility to connect to your AirStation.

Note: If Client Manager 3 is installed on your computer, Wireless Zero Configuration is disabled. Uninstall Client Manager 3 to use Wireless Zero Configuration, or just use Client Manager 3 to connect to the AirStation.

1 Right click on the wireless network icon  displayed in the system tray.

2 Click [View Available Wireless Networks].

3



Select the network to connect to and click [Connect].

4

Enter the encryption key (twice) and click [Connect].

Follow the instructions displayed on the screen to finish configuration.

Chapter 6
Troubleshooting

Cannot connect to the Internet over wired connection.

- Make sure that your AirStation is plugged in!
- Check that the status LEDs of your AirStation are lit as below:

Power	Green light on
Wireless	Green light on or flashing
Router	Green light may be on or off depending on your network
Diag	off
LAN	Green light on or flashing
Internet	Green light on or flashing

- Make sure that your computer is set to [obtain an IP address automatically] (see appendix C).
- Restart your AirStation.

Cannot access the web-based configuration utility.

- See chapter 4 for instructions to open the AirStation's configuration utility.
- Enter the correct user name and password to login to the configuration screen. The factory defaults are [root] (in lower case) for the user name and a blank password (enter nothing). If you changed the password, enter the new password that you set.
- Verify that your web browser is not set to use proxies.
- Make sure that your computer is configured to [Obtain an IP Address Automatically] (see appendix C).
- Restart your AirStation.

Cannot connect to the network wirelessly.

- Configure your wireless client with the same SSID, encryption type, and encryption key as set on the AirStation.
  The factory defaults are:

SSID -	The AirStation's MAC address (printed on the label)
Encryption Type -	WPA/WPA2 mixed mode - PSK (Connect with either WPA-PSK TKIP or WPA2-PSK AES).
Encryption Key -	Printed on the label of the AirStation.

- Place your AirStation and wireless devices 2 - 10 feet apart.
- Restart your AirStation.

You forgot AirStation's SSID, Encryption Key, or Password.

Hold down the Reset button on the base of your AirStation for 3 seconds to initialize its settings. All settings, including your password, SSID, and encryption key will be initialized to their defaults. The factory defaults are:

SSID -	The AirStation's MAC address (printed on the label)
Encryption Type -	WPA/WPA2 mixed mode - PSK (Connect with either WPA-PSK TKIP or WPA2-PSK AES).
Encryption Key -	Printed on the label of the AirStation.

The link speed is slower than 300/150 Mbps (Maximum link speed is only 130/65Mbps).

By default, the AirStation's 300/150 Mbps mode is not enabled. You may enable it with the following procedure:

1. Open the configuration utility (chapter 4).
2. Click [Wireless SSID & Channel (11n 300(150)Mbps Mode)] in Easy Setup.
3. Change the value in [300(150) Mbps Mode] - [Band Width] to 40 MHz and click [Apply].

If you still cannot connect at 300/150 Mbps, check the settings of your wireless client device.

Other Tips

Issue:

I reset my wireless router to factory settings and forgot how to log in to the configuration utility.

Answer:

Open your browser and enter 192.168.11.1 as the browser address and hit Enter. You will be prompted to log in. Enter the user name as root and the password box is left empty (no password). Click [OK] to complete the login and the option to reset your password will be available on the first page.

Issue:

How do I forward ports on my wireless router for my gaming console?

Answer:

Log in to the router's configuration utility. From the home page, go to the Internet Game/ Port Mapping section. Enter the port that needs to be forwarded, and the IP address of the gaming console.

Issue:

How do I enable or modify security encryption settings on the wireless router?

Answer:

Log in to the configuration utility with your browser. Go to the Wireless Config tab and then select the Security tab. Buffalo recommends WPA for wireless encryption. The passphrase/key should be at least 8 characters in length.

Issue:

How do I change my wireless router's broadcasted network name (SSID)?

Answer:

Log in to the configuration utility. Go to the Wireless Config tab and then select the Basic tab if necessary. Find the settings area for SSID. Select the [Use] radio button and enter the name you wish to use for your network in the text field provided. Click [Apply] to save the settings. Once the wireless router has rebooted, you will need to manually select the new network name for all wireless devices and enter your encryption key if necessary.

Issue:

What can I do if my wireless connection drops randomly or seems slow?

Answer:

There are many environmental factors that may cause this. First, ensure the issue is not range related by moving the wireless router and the client device closer together. If the the connection drops continue, continue, then range is probably not the issue.
Other 2.4 GHz devices such as microwaves, other wireless networks, and 2.4 GHz wireless phones may impact performance. Try a different wireless channel for your wireless router. Log in to the wireless router with your browser. Click on the Wireless Config tab and then the Basic tab. Wireless channels from 1 - 11 may be selected. Try the Auto-Channel option if available. Otherwise, manually select an alternate channel and click [Apply].

Issue:

Though I am able to successfully make a connection with my wireless router, I am unable to access the Internet with my web browser.

Answer:

First, power off the Cable or DSL modem, the wireless router, and your computer. Move the router's mode switch to the ON position. Verify that the modem is connected to the wireless router with an Ethernet cable to the WAN port. Power on the modem and wait one minute. Power on the wireless router and wait another minute. Power on the computer. Open a browser on the computer and navigate to a familiar website to verify whether the Internet connection is functioning normally.
If after these steps, an Internet connection is still unavailable, power off the Cable or DSL modem and computer again and directly connect your computer to the Cable or DSL modem with a cable between the computer and the port on the modem. Power on the modem and wait one minute. Power on the computer and again check for an Internet connection.
If an Internet connection IS NOT available with a direct connection to the computer, please call the Internet Service Provider who installed the modem.
If an Internet connection IS available with a direct connection to the computer, please call our customer support.

Issue:

Where can I download the latest drivers, firmware and instructions for my Buffalo wireless products?

Answer:

The latest drivers and firmware are available online at
www.buffalotech.com

Appendix A
Specifications

WHR-HP-G300N

Wireless LAN Interface	
Standard Compliance	IEEE802.11b / IEEE802.11g / IEEE802.11n
Transmission Method	Direct Sequence Spread Spectrum (DSSS), OFDM, MIMO
Frequency Range	2,412 - 2,462 MHz (Channels 1 - 11)
Transmission Rate	802.11b/g: 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2, 1 Mbps 802.11n: 20 MHz Channel (LongGI) 130/117/104/78/52/39/26/13 Mbps (mcs15-8) (2 stream) 65/58.5/52/39/26/19.5/13/6.5 Mbps (mcs7-0) (1 stream) 40 MHz Channel (LongGI) 270.0/243.0/216.0/162.0/108.0/81.0/54.0/27.0 Mbps (mcs15-8) (2 streem) 135/121.5/108.0/81.0/54.0/40.5/27.0/13.5 Mbps(mcs7-0) (1 streem) (ShortGI) 300.0 Mbps (mcs15) (2 streem) 150.0 Mbps (mcs7) (1 streem)
Access Mode	Infrastructure Mode
Security	AOSS, WPA2-PSK (TKIP/AES), WPA/WPA2 mixed PSK, WPA-PSK (TKIP/AES), 128/64bit WEP, Mac Address Filter
Wired LAN Interface	
Standard Compliance	IEEE802.3u (100BASE-TX), IEEE802.3 (10BASE-T)
Transmission Rate	10 / 100 Mbps
Transmission Encoding	100BASE-TX 4B5B/MLT-3, 10BASE-T Manchester Cording
Access Method	CSMA/CD
Speed and Flow Control	10/100, Auto Sensing, Auto MDIX
Number of LAN Ports	4
LAN Port Connector	RJ-45
Other	
Power Supply	External AC 100-240 V Universal, 50/60 Hz
Power Consumption	Approx. 5.7 W (Max)
Dimensions	142 mm x 124 mm x 25 mm (5.6 x 4.9 x 1.0 in.)
Weight	230 g (7.4 oz.) not included base
Operating Environment	0-40 °C (32-104 °F) , 20-80 % (non-condensing)

WHR-HP-GN

Wireless LAN Interface	
Standard Compliance	IEEE802.11b / IEEE802.11g / IEEE802.11n specification
Transmission Method	Direct Sequence Spread Spectrum (DSSS), OFDM, SISO
Frequency Range	2,412 - 2,462 MHz (Channels 1 - 11)
Transmission Rate	802.11b/g: 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2, 1 Mbps 802.11n: 20 MHz Channel (LongGI) 65/58.5/52/39/26/19.5/13/6.5 Mbps (mcs7-0) (1 streem) 40 MHz Channel (LongGI) 135.0/121.5/108.0/81.0/54.0/40.5/27.0/13.5 Mbps (mcs7-0) (1 streem) (ShortGI) 150.0 Mbps (mcs7) (1 streem)
Access Mode	Infrastructure Mode
Security	AOSS, WPA2-PSK (TKIP/AES), WPA/WPA2 mixed PSK, WPA-PSK (TKIP/AES), 128/64bit WEP, Mac Address Filter
Wired LAN Interface	
Standard Compliance	IEEE802.3u (100BASE-TX), IEEE802.3 (10BASE-T)
Transmission Rate	10 / 100 Mbps
Transmission Encoding	100BASE-TX 4B5B/MLT-3, 10BASE-T Manchester Cording
Access Method	CSMA/CD
Speed and Flow Control	10/100, Auto Sensing, Auto MDIX
Number of LAN Ports	4
LAN Port Connector	RJ-45
Other	
Power Supply	External AC 100-240 V Universal, 50/60 Hz
Power Consumption	Approx. 5.5 W (Max)
Dimensions	142 mm x 124 mm x 25 mm (5.6 x 4.9 x 1.0 in.)
Weight	210 g (6.8 oz.) not including base
Operating Environment	0 - 40° C (32 - 104° F) , 20 - 80% (non-condensing)

Appendix B
Default Configuration Settings

Feature	Parameter	Default Setting
Internet (Router Mode only)	Method of Acquiring IP Address	Easy Setup (Internet Connection Wizard)
	Default Gateway	none
	Address of DNS Name Server	none
	Internet MAC Address	Use Default MAC Address
	MTU Size of Internet Port	1500 Bytes
PPPoE (Router Mode only)	Default PPPoE Connection	No Active Session
	IP Unnumbered PPPoE Connection	No Active Session
	PPPoE Connection List	none
	Preferred Connections	none
DDNS (Router Mode only)	Dynamic DNS Service	Disabled
	Current Dynamic DNS Information	none
VPN Server (Router Mode only)	LAN Side IP Address	192.168.11.1(255.255.255.0)
	DHCP Server Function	Enabled
	DHCP IP Address Pool	192.168.11.2 for up to 64 Address(es)
	PPTP Server Function	Disabled
	Authorization Type	MS-CHAPv2 (40/128-bit Encryption)
	Server IP Address	Auto
	Client IP Address	Auto
	DNS Server IP Address	LAN IP address of the AirStation
	WINS Server IP Address	None
	PPTP User List	None
LAN	LAN Side IP Address	Router Mode: 192.168.11.1 (255.255.255.0) Bridge Mode (Router Switch off): 192.168.11.100 (255.255.255.0) Bridge Mode (Router Switch set to Auto): Obtain automatically from DHCP Server

Feature	Parameter	Default Setting
	DHCP Server Function (Router Mode only)	Enabled
	DHCP IP Address Pool (Router Mode only)	192.168.11.2 - 192.168.11.65
	LAN Side IP Address (IP Unnumbered) (Router Mode only)	none
	Lease Period (Router Mode only)	48 Hours
	Default Gateway (Router Mode only)	AirStation's IP Address
	DNS Servers (Router Mode only)	AirStation's IP Address
	WINZ Server (Router Mode only)	Do Not Specify
	Domain Name (Router Mode only)	Assigned Domain Name
	Default Gateway (Bridge Mode only)	none
	DNS Server Address (Bridge Mode only)	none
DHCP Lease (Router Mode only)	Current DHCP Client Information	none
NAT (Router Mode only)	Address Translation	Enabled
	Log Output of Deleted Packets	Disabled
Route	Routing Information	none
WPS	WPS	Enabled
	External Registrar	Enabled
	AirStation PIN	An 8-digit random value (Printed on the label of the AirStation)
	WPS Security Information	WPS status: configured SSID: AirStation's MAC Address Security: WPA/WPA2 mixedmode - PSK TKIP/AES mixedmode Encryption key: A 13-digit random value

Feature	Parameter	Default Setting		
AOSS	Encryption level expansion	Enabled		
	Dedicated WEP SSID isolation	Disabled		
	AOSS Button on the AirStation Unit	Enabled		
Basic	Wireless Radio	Enabled		
	Wireless Channel	Auto Channel		
	300(150)Mbps Mode	Band Width: 20 MHz Extension Channel: -		
	Broadcast SSID	Allow		
	Separate feature	not used		
	SSID	Configure AirStation's MAC address		
	Wireless authentication	WPA/WPA2 mixedmode-PSK		
	Wireless encryption	TKIP/AES mixedmode		
	WPA-PSK (Pre-Shared Key)	A 13-digit random value (Printed on the label of the AirStation)		
	Rekey interval	60 minutes		
Advanced	Multicast Rate	Auto		
	DTIM Period	1		
	Privacy Separator	Disable		
WMM	WMM-EDCA Parameters (Priority AC_BK (Low))		For AP	For STA
		CWmin	15	15
		CWmax	1023	1023
		AIFSN	7	7
		TXOP Limit	0	0
		Admission Control	-----	Disable
	WMM-EDCA Parameters (Priority AC_BE (Normal))		For AP	For STA
		CWmin	15	15
		CWmax	63	1023
		AIFSN	3	3
		TXOP Limit	0	0
		Admission Control	-----	Disable

Feature	Parameter	Default Setting		
	WMM-EDCA Parameters (Priority AC_VI (High))		For AP	For STA
		CWmin	7	7
		CWmax	15	15
		AIFSN	1	2
		TXOP Limit	94	94
		Admission Control	-----	Disable
	WMM-EDCA Parameters (Priority AC_VO (Highest))		For AP	For STA
		CWmin	3	3
		CWmax	7	7
		AIFSN	1	2
		TXOP Limit	47	47
		Admission Control	-----	Disable
MAC Filter	Enforce MAC Filter	Disabled		
	Registration List	none		
Multicast Control	Snooping	Enabled		
	Multicast Aging Time	300 Sec.		
WDS	WDS	Use		
	Specify Master/Slave	Master		
Firewall (Router Mode only)	Log Output	Disabled		
	Basic Rules	Prohibit NBT and Microsoft-DS Routing Reject IDENT Requests Block Ping from Internet		Disabled Disabled Disabled
IP Filter (Router Mode only)	Log Output	Disabled		
	IP Filter Information	none		
VPN Pass Through (Router Mode only)	IPv6 Pass Through	Disabled		
	PPPoE Pass Through	Disabled		
	PPTP Pass Through	Enabled		
Port Forwarding (Router Mode only)	Port Forwarding Registration Information	none		
DMZ (Router Mode only)	IP Address of DMZ	none		
UPnP (Router Mode only)	UPnP	Enabled		

Feature	Parameter	Default Setting
QoS (Router Mode only)	QoS for transmission to the Internet	Disabled
Name	AirStation Name	AP + AirStation's MAC Address
	List Network Services	Enabled
Password	Administrator Name	root (fixed)
	Administrator Password	none
Time/Date	Local Date	2010 Year 1 Month 1 Day
	Local Time	0 Hour 0 Minute 0 Seconds
	Time Zone	(GMT−06:00) Central Standard Time: CST or (GMT+00:00) Greenwich Mean Time,London
NTP	NTP Functionality	Enabled
	NTP Server	time.nist.gov
	Update Interval	24 hours
Access	Log Output	Disabled
	Access Limits	Prohibit configuration from wireless LAN Disabled Prohibit configuration from wired LAN Enabled Permit configuration from WAN Enabled
Log	Log Transfer	Disabled
	Syslog Server	none
	Transfer Logs	Router Mode: Address Translation, IP Filter, Firewall, PPPoE Client, Dynamic DNS, DHCP Client, DHCP Server, AOSS, Wireless Client, Authentication, Setting Changes, System Boot, NTP Client, and Wired Link Bridge Mode: IP Filter, DHCP Client, AOSS, Wireless Client, Authentication, Setting Changes, System Boot, NTP Client, and Wired Link

Appendix C
TCP/IP Settings in Windows

Windows 7

To configure TCP/IP in Windows 7, follow the procedure below.

1 Click [Start] > [Control Panel] > [Network and Internet].

2 Double click [Network and Sharing Center].

3 Click [Change Adapter Settings] on the left side menu.

4 Right click on [Local Area Connection], then click [Properties].

5 If the message "Windows needs your permission to continue" appears, click [Continue].

6 Select [Internet Protocol Version 4 (TCP/IPv4)] then click [Properties].

7 To have DHCP set your IP address settings automatically, check [Obtain an IP address automatically] and [Obtain DNS server address automatically].

To set your IP address settings manually, enter values for each setting. Example:

If the AirStation's IP address is 192.168.11.1,

IP address	192.168.11.80
Subnet mask	255.255.255.0
Default gateway	192.168.11.1
Preferred DNS server	192.168.11.1
Alternate DNS server	blank

8 Click [OK].

Windows Vista

To configure TCP/IP in Windows Vista, follow the procedure below.

1 Click [Start] > [Settings] > [Control Panel].

2 Double click [Network and Sharing Center].

3 Click [Manage network connections] on the left side menu.

4 Right click on [Local Area Connection], then click [Properties].

5 When the message "Windows needs your permission to continue" appears, click [Continue].

6 Select [Internet Protocol Version 4 (TCP/IPv4)], then click [Properties].

7 To have DHCP set your IP address settings automatically, check [Obtain an IP address automatically] and [Obtain DNS server address automatically].

To set your IP address settings manually, enter values for each setting. Example:

If the AirStation's IP address is 192.168.11.1,

IP address	192.168.11.80
Subnet mask	255.255.255.0
Default gateway	192.168.11.1
Preferred DNS server	192.168.11.1
Alternate DNS server	blank

8 Click [Close].

Windows XP

To configure TCP/IP in Windows XP, follow the procedure below.

1 Click [Start] > [Settings] > [Control Panel].

2 Double click [Network].

3 Right click on [Local Area Connection], then click [Properties].

4 Select [Internet Protocol (TCP/IP)], then click [Properties].

5 To have DHCP set your IP address settings automatically, check [Obtain an IP address automatically] and [Obtain DNS server address automatically].

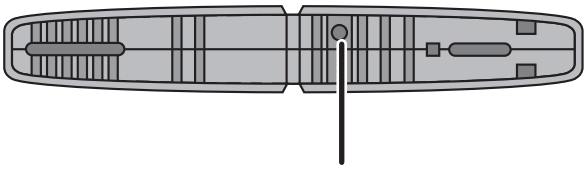
To set your IP address settings manually, enter values for each setting. Example:

If the AirStation's IP address is 192.168.11.1,

IP address	192.168.11.80
Subnet mask	255.255.255.0
Default gateway	192.168.11.1
Preferred DNS server	192.168.11.1
Alternate DNS server	blank

6 Click [Close].

Appendix D
Restoring the Default Configuration



Hold down this button for 3 seconds. The AirStation will be initialized.

Appendix E
Regulatory Compliance

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:

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

FCC ID:

WHR-HP-G300N: FDI-09101621-0
WHR-HP-GN : FDI-09101567-0

Important Note - FCC Radiation Exposure Statement:

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

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

European Union Notice:

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 conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN60950-1:
  2006 Safety of Information Technology Equipment
- EN 50385: 2002
  Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public
- EN 300 328 V1.7.1 (2006-10)
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- EN 301 489-1 V1.8.1 (2008-04)
  Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- EN 301 489-17 V1.3.2 (2008-04)
  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France 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 authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE 0560 ⓘ

Česky[Czech]
Buffalo Technology Inc. tímto prohlašuje, že tento AirStation WHR-HP-GN/G300N je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.

Dansk[Danish]
Undertegnede Buffalo Technology Inc. erklærer herved, at følgende udstyr AirStation WHR-HP-GN/G300N overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.

Deutsch[German]
Hiermit erklärt Buffalo Technology Inc. dass sich das Gerät AirStation WHR-HP-GN/G300N in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.

Eesti[Estonian]
Käesolevaga kinnitab Buffalo Technology Inc. seadme AirStation WHR-HP-GN/G300N vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

English
Hereby, Buffalo Technology Inc. declares that this AirStation WHR-HP-GN/G300N is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Español[Spanish]
Por medio de la presente Buffalo Technology Inc. declara que el AirStation WHR-HP-GN/G300N cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

Ελληνική[Greek]
ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Buffalo Technology Inc. ΔΗΛΩΝΕΙ ΟΤΙ AirStation WHR-HP-GN/G300N ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Français[French]
Par la présente Buffalo Technology Inc. déclare que l'appareil AirStation WHR-HP-GN/G300N est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Italiano[Italian]
Con la presente Buffalo Technology Inc. dichiara che questo AirStation WHR-HP-GN/G300N è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Latviski[Latvian]
Ar šo Buffalo Technology Inc. deklarē, ka AirStation WHR-HP-GN/G300N atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

Lietuvių[Lithuanian]
Šiuo Buffalo Technology Inc. deklaruoja, kad šis AirStation WHR-HP-GN/G300N atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands[Dutch]
Hierbij verklaart Buffalo Technology Inc. dat het toestel AirStation WHR-HP-GN/G300N in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Malti[Maltese]
Hawnhekk, Buffalo Technology Inc. , jiddikjara li dan AirStation WHR-HP-GN/G300N jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.

Magyar[Hungarian]
Alulírott, Buffalo Technology Inc. nyilatkozom, hogy a AirStation WHR-HP-GN/G300N megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.

Polski[Polish]
Niniejszym, Buffalo Technology Inc. , deklaruję, że AirStation WHR-HP-GN/G300N spełnia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.

Português[Portuguese]
Buffalo Technology Inc. declara que este AirStation WHR-HP-GN/G300N está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

Slovensko[Slovenian]
Buffalo Technology Inc. izjavlja, da je ta AirStation WHR-HP-GN/G300N v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.

Slovensky[Slovak]
Buffalo Technology Inc. týmto vyhlasuje, že AirStation WHR-HP-GN/G300N spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.

Suomi[Finnish]
Buffalo Technology Inc. vakuuttaa täten että AirStation WHR-HP-GN/G300N tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Svensk[Swedish]
Härmed intygar Buffalo Technology Inc. att denna AirStation WHR-HP-GN/G300N står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Industry Canada statement

This device complies with RSS-210 of the Industry Canada 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:
Radiation Exposure Statement:
This equipment complies with IC 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 device has been designed to operate with an antenna having a maximum gain of 2 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Industry Canada ID:

WHR-HP-G300N: 6102A-025
WHR-HP-GN: 6102A-024

For Taiwan 警語

第十二條：

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條：

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

CONDICIONES (Mexico)

PRIMERA
-El certificado provisional tiene vigencia de un año a partir de esta fecha y prodrá ser renovado hasta en dos ocasiones por el mismo período, para lo cual, previo a la fecha de vencimiento del Certificado deberá solicitar por escrito a esta Comisión su renovación. El Ceritificado definitivo tiene vigencia indefinida.

SEGUNDA
-El Certificado de Homologación, podrá ser cancelado a petición del solicitante a cuando la Comisión Federal de Telecomunicaciones así lo determine con fundamento en el Artículo 149 del Reglamento de Telecomunicaciones, o bien de acuerdo a lo señalado en el Capítulo Segundo de la Ley Federal de Procedimiento Administrativo.

TERCERA
-Los equipos amparados por este Certificado de Homologación deberán tener indicado en alguna parte visible, firmemente adherido, el númerode Certificado de Homologación correspondiente, así como la marca y modelo con la que se expide este Certificado.

CUARTA
-La Comisión Federal de Telecomunicación podrá requerir en cualquier momento a la empresa presentación de información ténica adicional, así como las muestras del equipo para realizar pruebas de comportamiento y verificar las caraterísticas del mismo.

QUINTA
-Cualquier modificación estructural o de configuración ténica deberá someterse a consideración de la Comisión, para que ésta determine si procede el otorgamiento de una ampliación del Certificado de Homologación o si requiere de un nuevo Certificado.

SEXTA
-El equipo que ampara el presente certificado deberá operar conforme a las regulaciones ténicas, reglas,reglamentos y otras disposiciones administrativas vigente o que llegara a emitir o adoptar la Comisión Federal de Telecomunicaciones y/o la Secretaría de Comunicaciones y Transportes.

SEPTIMA
-El equipo de radiocomunicación que ampara el presente certificado deberá operar de conformidad con el Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones y el Cuadro Nacional de Atribución de Frequencias México vigente.

OCTAVA
-Las antenas de las estaciones terrenas deberán cumplir con el patrón de radiación Recomendado por la Unión Internacional de Telecomunicaciones, Sector de Radio Frequencia UIT-R, en el casdo de sistemas de microondas las antenas de los mismos deberán cumplir con las recomendaciones del UIT-R, conforme a su banda de operación.

NOVENA
-La homologación de este equipo no implica la autorización para prestar servicios públicos de telecomunicaciones ni para establecer aplicaciones que obstruyan o invadan cualquier via general de comunicación.

DECIMA

- El inclumplimiento de las condiciones estipuladas en este Certificado será motivo de sanción con base a lo dispuesto en la Ley de Vías General de Comunicación, Ley Fedreal de Telecomunicación y en el Reglamento de Telecomunicaciones.

Appendix F
Environmental Information

- 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.

Appendix G
GPL Information

Source code for Buffalo products that use GPL code is available at *http://opensource.buffalo.jp/* .

Appendix H
Warranty

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

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

Appendix I
Contact Information

North America

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*

Europe

Buffalo Technology provides technical support in English, German, French, Italian, and Spanish.

UK	0845 3511005
Austria	08101 0251552
Belgium	0787 99917
Denmark	70150919
Finland	010802812
France	0811 650220
Germany	01801 003757
Ireland	1890 719901
Italy	848 782113
Netherlands	09000401256
Norway	81000050
Spain	9018 10750
Sweden	0771404105
Switzerland	0848 560374

For all other regions please contact +353 61 704617

www.buffalo-technology.com/contact

Asia Pacific

Australia	TEL: 1300 761 310
	e-mail: buffalo_support@uniden.com.au
China	TEL: 86-800-820-8262
	e-mail: support@buffalo-china.com
Hong Kong	TEL: 852-2345-0005
	e-mail: support@hornington.com
India	TEL: 1-8004256210
	e-mail: csbuffalo@accelfrontline.in
Indonesia	TEL: 021-6231-2893
Malaysia	TEL: 03-5032-0138
	e-mail: buffalo@ecsm.com.my
Philippines	TEL: 2-688-3999
	e-mail: digisupport@msi-ecs.com.ph
Republic of Korea	TEL: 02-2057-2095
	e-mail: support@buffalotech.co.kr
Singapore	TEL: 65-6297-2085
	e-mail: buffalo@blumm.com
Taiwan	TEL: 0800-660-886
	e-mail: support@buffalo-tech.com.tw
Thailand	TEL: 02-716-6669
Other Areas	Please contact the shop or distributor where you purchased the unit, referring to the attached warranty card issued by the distributor.