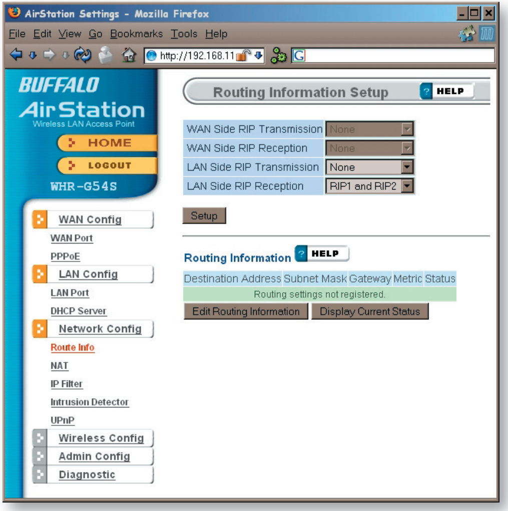


Routing Information Setup

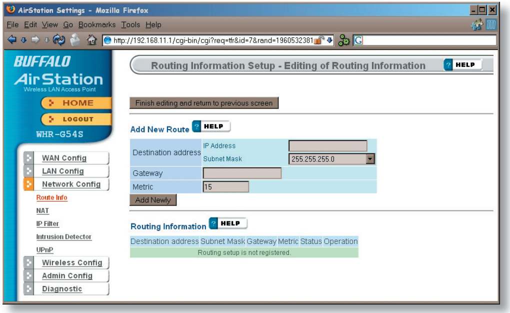
WAN Side RIP Transmission	None
WAN Side RIP Reception	None
LAN Side RIP Transmission	None
LAN Side RIP Reception	RIP1 and RIP2

Routing Information

Destination Address	Subnet Mask	Gateway	Metric	Status
Routing settings not registered.				

By default, the AirStation receives RIP (Route Information Protocol) information only from your local network, and doesn't broadcast RIP at all. For large, complicated network configurations, you may wish to modify this behavior. Click *Apply* when you have your desired configuration.

Lower on the page, routing information is displayed. Click *Edit Routing Information* to add a new route manually.


AirStation Settings - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.11.1/cgi-bin/cgi?req=tfr&id=7&rand=1960532381
BUFFALO
AirStation
Wireless LAN Access Point
HOME
LOGOUT
WHR-G54S
WAN Config
LAN Config
Network Config
Route Info
NAT
IP Filter
Intrusion Detector
UPnP
Wireless Config
Admin Config
Diagnostic
HELP
Finish editing and return to previous screen
Add Newly

Routing Information Setup - Editing of Routing Information

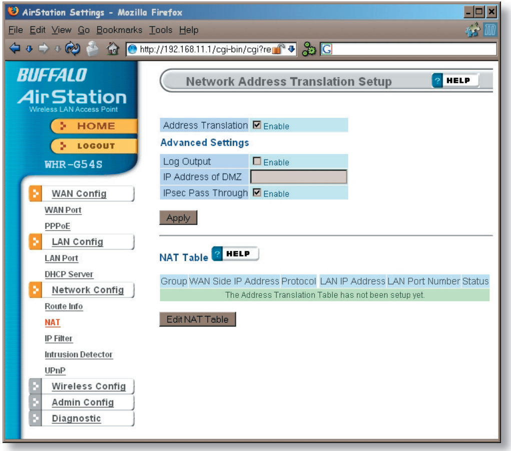
Add New Route

Destination address	IP Address	
	Subnet Mask	255.255.255.0
Gateway		
Metric	15	

Routing Information

Destination address	Subnet Mask	Gateway	Metric	Status	Operation
Routing setup is not registered.					

To configure a route manually, enter its *Destination Address* and *Gateway*. Enter a maximum number of hops allowable in *Metric* and click *Add*.



Network Address Translation Setup

Address Translation	☑ Enable

Advanced Settings

Log Output	□ Enable
IP Address of DMZ	
IPsec Pass Through	☑ Enable

Apply

NAT Table

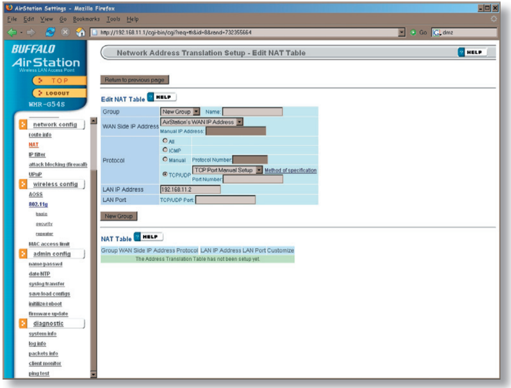
Group	WAN Side IP Address	Protocol	LAN IP Address	LAN Port Number	Status
The Address Translation Table has not been setup yet.					

Edit NAT Table

You may disable Network Address Translation and IPsec passthrough by unchecking the appropriate *Enable* boxes. If you have a DMZ, enter its IP address in the *IP Address of DMZ* box. Incoming packets containing no recognizable destination port information will be redirected to the DMZ's IP address.

Click *Apply* when done.

To set a NAT table entry manually, click *Edit NAT Table*.



http://192.168.11.1/cgi-bin/cgi?req=tfr&id=8&rand=732355664

Network Address Translation Setup - Edit NAT Table

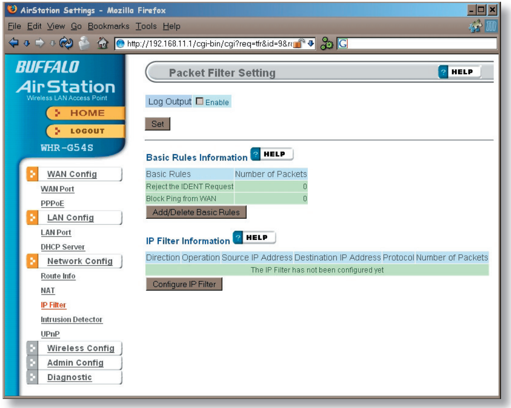
Edit NAT Table

Group	New Group Name:
WAN Side IP Address	AirStation's WAN IP Address Manual IP Address:
Protocol	○ All ○ ICMP ○ Manual Protocol Number: ● TCP/UDP TCP Port Manual Setup Method of specification Port Number:
LAN IP Address	192.168.11.2
LAN Port	TCP/UDP Port:

NAT Table

Group	WAN Side IP Address	Protocol	LAN IP Address	LAN Port	Customize
The Address Translation Table has not been setup yet.					

From this page you may manually add entries into the Address Translation Table. Click *Add New Group* when each is complete.



Packet Filter Setting

Log Output □ Enable

Basic Rules Information

Basic Rules	Number of Packets
Reject the IDENT Request	0
Block Ping from WAN	0

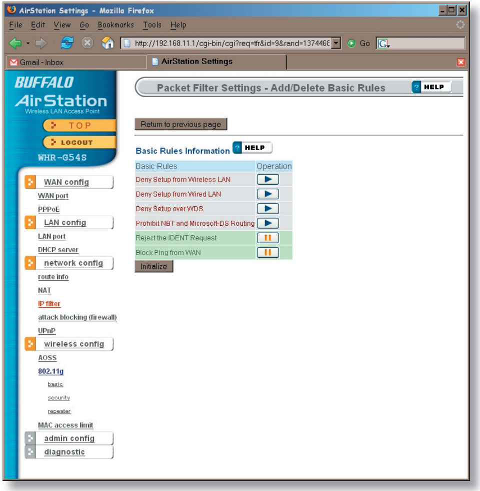
IP Filter Information

Direction	Operation	Source IP Address	Destination IP Address	Protocol	Number of Packets
The IP Filter has not been configured yet					

Your AirStation comes pre-configured with basic rules. You may choose which of these to use by clicking on *Add/Delete Basic Rules* and turning to page 36.

To make a custom rule, click on *Configure IP Filter* (page 37).

IP Filter (Add/Delete Basic Rules)

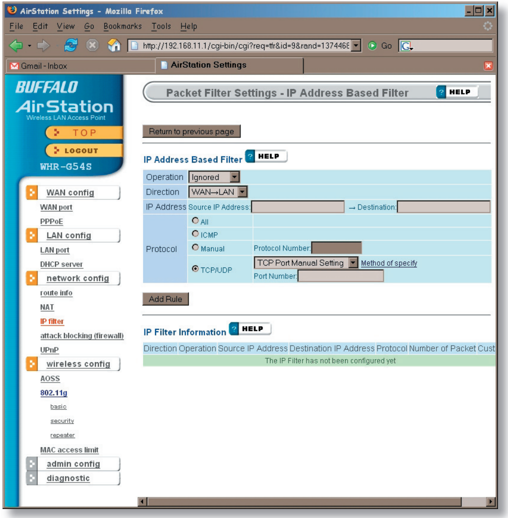


Packet Filter Settings - Add/Delete Basic Rules

Basic Rules Information

Basic Rules	Operation
Deny Setup from Wireless LAN	▶
Deny Setup from Wired LAN	▶
Deny Setup over WDS	▶
Prohibit NBT and Microsoft-DS Routing	▶
Reject the IDENT Request	❚❚
Block Ping from WAN	❚❚

Get here by clicking on *Add/Delete Basic Rules* (see page 35). You may choose which of AirStation's preconfigured basic rules are enabled or disabled. Active rules are displayed with a green background, and disabled rules are shown in red. Choose the rules you want to use by clicking under *Operation*. When your choices are complete, click on *Initialize*.



Packet Filter Settings - IP Address Based Filter

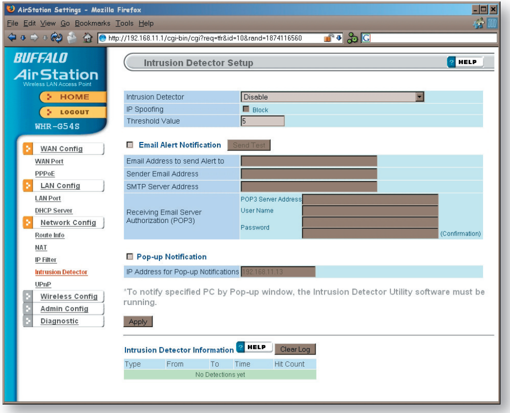
IP Address Based Filter

Operation	Ignored	
Direction	WAN→LAN	
IP Address	Source IP Address:	→ Destination:
Protocol	○ All	
	○ ICMP	
	○ Manual	Protocol Number:
	● TCP/UDP	TCP Port Manual Setting Method of specify Port Number:

IP Filter Information

Direction	Operation	Source IP Address	Destination IP Address	Protocol	Number of Packet	Cust
The IP Filter has not been configured yet						

Clicking on *Configure IP Filter* from the IP filter page (page 35) will bring you to this page, where you can make your own rules. Click *Add Rule* when you have each rule configured the way you want it.



http://192.168.11.1/cgi-bin/cgi?req=tfr&id=10&rand=1874116560

Intrusion Detector Setup

Intrusion Detector	Disable
IP Spoofing	□ Block
Threshold Value	5

□ Email Alert Notification

Email Address to send Alert to		
Sender Email Address		
SMTP Server Address		
Receiving Email Server Authorization (POP3)	POP3 Server Address	
	User Name	
	Password	
		(Confirmation)

□ Pop-up Notification

IP Address for Pop-up Notifications	192.168.11.13

*To notify specified PC by Pop-up window, the Intrusion Detector Utility software must be running.

Intrusion Detector Information

Type	From	To	Time	Hit Count
No Detections yet				

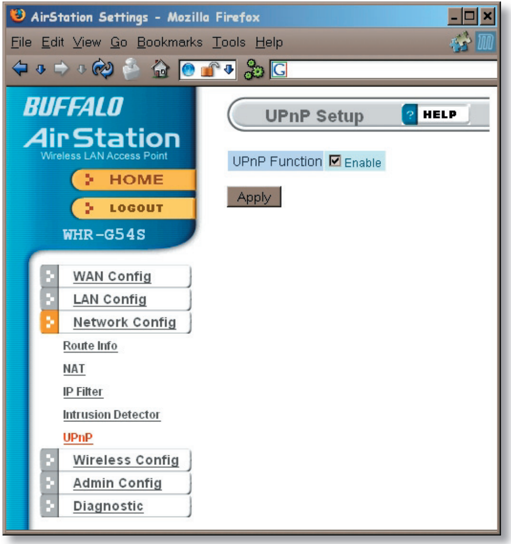
To enable intrusion detector, choose *Enable* or *Enable (Apply packet filter rules)* from the Intrusion Detector drop-down box. If packet filter rules are applied, packets will be filtered with packet filter rules before Intrusion Detector is applied.

Blocking IP spoofing blocks packets from devices using an IP address that is not their own.

In the *Threshold Value* box, enter the number of times an event has to occur before you receive notification.

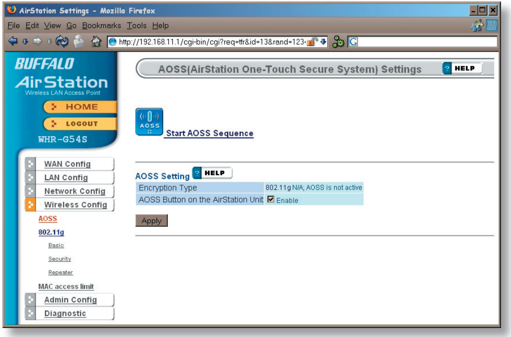
To configure your email alerts, enter your email address and mail server information. You may make up a sender email address, such as “alert@router.com”. Alert emails will appear to come from this address.

Intrusion detector also blocks unauthorized access attempts and suspicious traffic from WAN-side devices (the internet).



UPnP Function ☑ Enable

You may disable Universal Plug and Play functionality by unchecking *Enable* here. Note that Windows (MSN) Messenger will not function correctly with UPnP disabled.



AOSS(AirStation One-Touch Secure System) Settings

Start AOSS Sequence

AOSS Setting

Encryption Type	802.11g N/A; AOSS is not active
AOSS Button on the AirStation Unit	☑ Enable

Clicking *Start AOSS Sequence* has the same function as pushing the AOSS button on the router: it initiates the AOSS process.

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

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

Consult your client device's documentation for the location of its AOSS button.