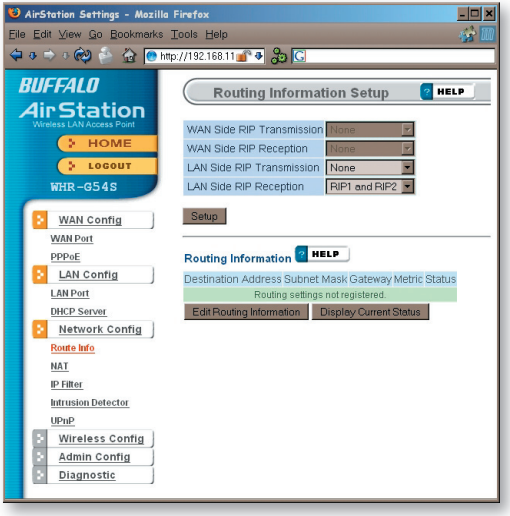
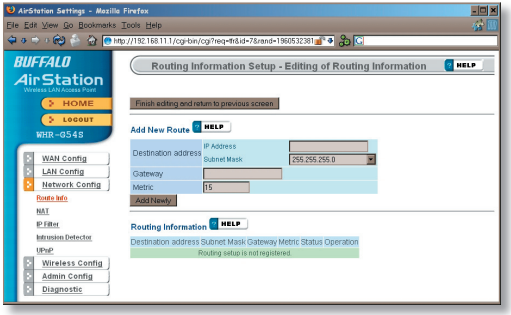
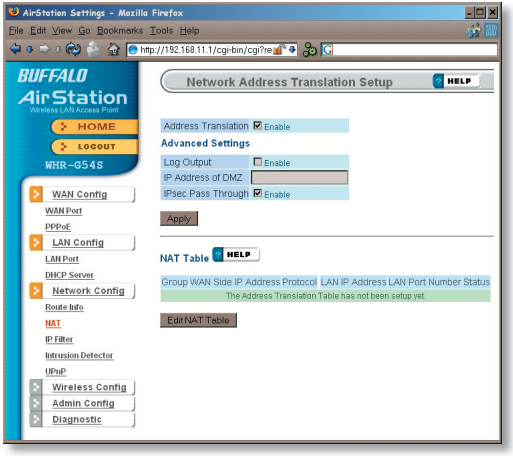


By default, the AirStation receives RIP (Route Information Protocol) information only from your local network, and doesn't broadcast RIP at all. For large, complicated network configurations, you may wish to modify this behavior. Click *Apply* when you have your desired configuration.

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



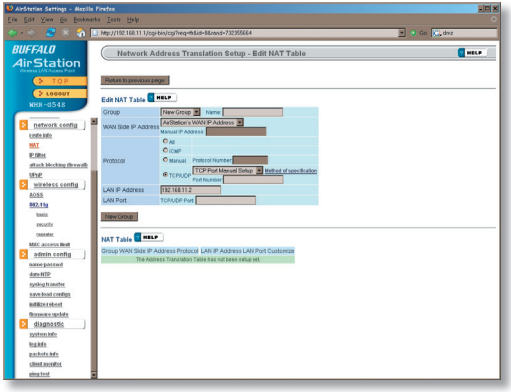
To configure a route manually, enter its *Destination Address* and *Gateway*. Enter a maximum number of hops allowable in *Metric* and click *Add*.



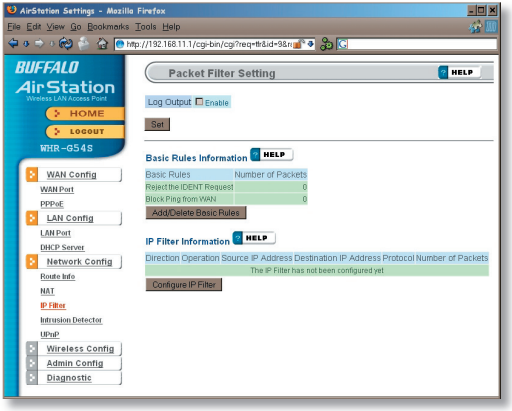
You may disable Network Address Translation and IPsec passthrough by unchecking the appropriate *Enable* boxes. If you have a DMZ, enter its IP address in the *IP Address of DMZ* box. Incoming packets containing no recognizable destination port information will be redirected to the DMZ's IP address.

Click *Apply* when done.

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



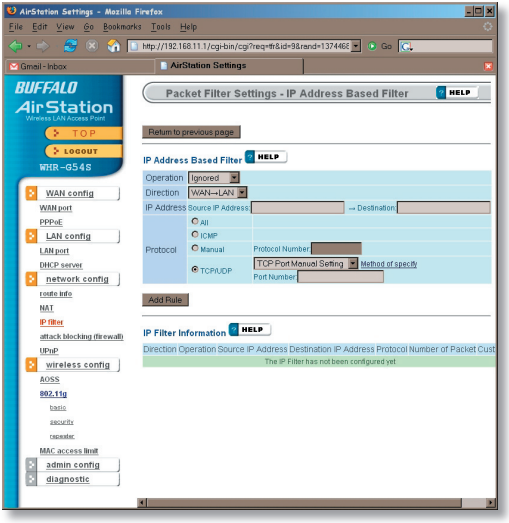
From this page you may manually add entries into the Address Translation Table. Click *Add New Group* when each is complete.



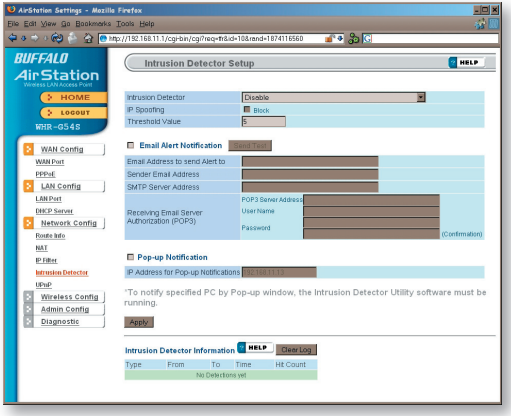
Your AirStation comes pre-configured with basic rules. You may choose which of these to use by clicking on *Add/Delete Basic Rules* and turning to page 36.

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

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*.



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.



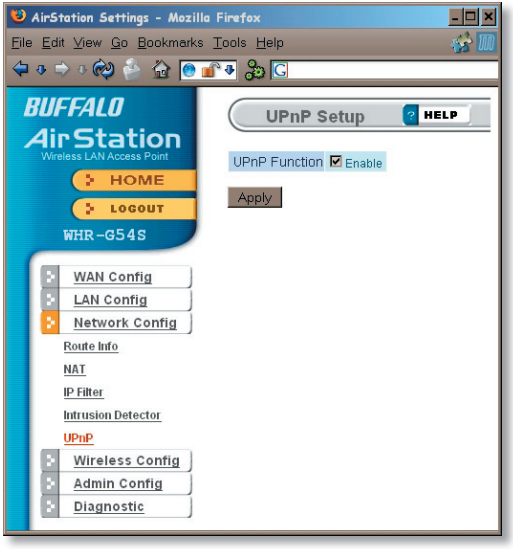
To enable intrusion detector, choose *Enable* or *Enable (Apply packet filter rules)* from the Intrusion Detector drop-down box. If packet filter rules are applied, packets will be filtered with packet filter rules before Intrusion Detector is applied.

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

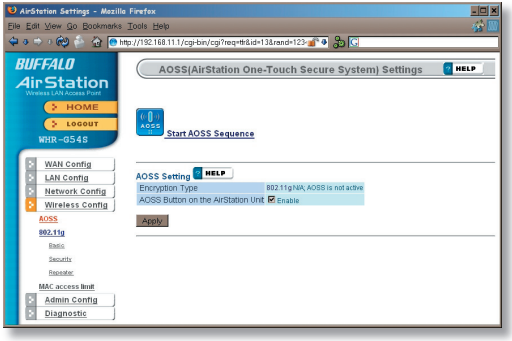
In the *Threshold Value* box, enter the number of times an event has to occur before you receive notification.

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).



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



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.