



XROADS NETWORKS

Network Appliance How To Guide: Tools

How To Guide

EDGE NETWORK APPLIANCE

How To Guide Tools

© XRoads Networks
17165 Von Karman • Suite 112
888-9-XROADS

Table of Contents

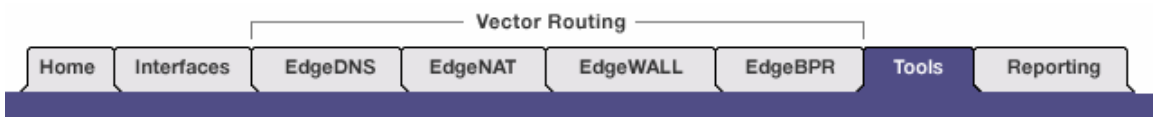
Tools Overview	3
C O M P O N E N T S	
Initial Setup	4
Verifying Connectivity	6
Adjusting Link Settings	8
Testing Bandwidth	10
Changing XOS VPN Params	11
Changing IPSec Params	12

Edge Configuration Series

Tools Overview

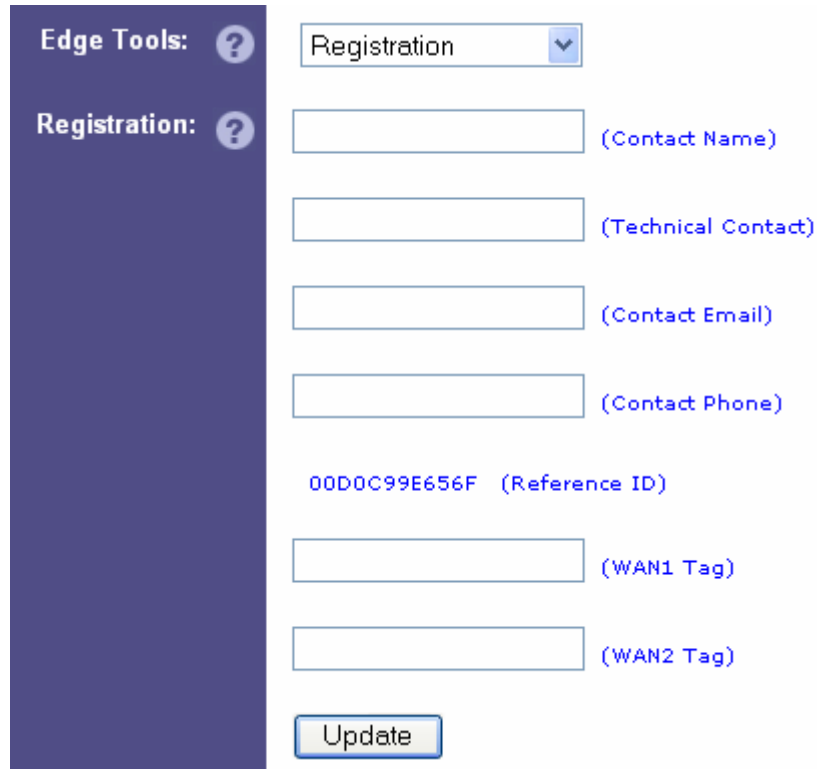
The Edge platform incorporates a number of tools for configuring and fine tuning the various system modules. These tools can be used by the administrator to verify connectivity, confirm how the routing is setup, change how the Edge tests the various network connections, and even modify how the packets are sent and received from the appliance.

The tools section can be accessed via the main tab selection Tools.



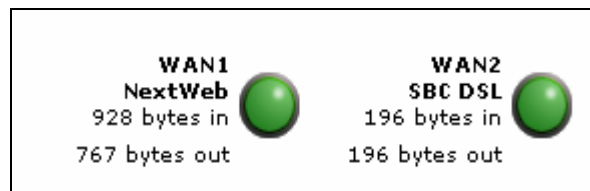
Initial Setup

When setting up the Edge platform one of the first steps should be to enter your registration information. Doing this ensures that you are kept up-to-date on the latest firmware releases, and provides for an easy method for recognizing each WAN interface (see below).



The screenshot shows a web interface for registration. On the left is a dark blue sidebar with 'Edge Tools: ?' and 'Registration: ?'. The main area has a 'Registration' dropdown menu. Below it are input fields for 'Contact Name', 'Technical Contact', 'Contact Email', and 'Contact Phone'. A 'Reference ID' is displayed as '00D0C99E656F'. There are also input fields for 'WAN1 Tag' and 'WAN2 Tag'. An 'Update' button is at the bottom.

When configured, the WAN tags provide simple designation for each WAN interface on the Home page.



Time/Date

Setting the time and date is very easy, the Edge platform uses NTP (Network Time Protocol) to ensure accurate time. This means that the Edge will automatically poll a publicly available time server (by default) and adjust the system clock to the appropriate time based on the time-zone selected.

The administrator is free to change the NTP server if another is preferred.

Admin Access

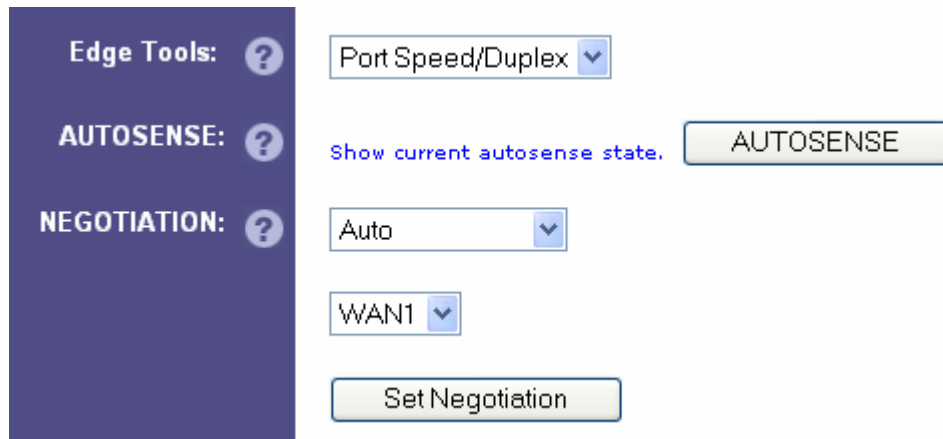
Used to change the primary login authentication, when updated you will be asked to log back in using the new password. This password also changes the CLI login.

Port Negotiation / Autosense

By default each interface is set to auto-negotiate its connectivity, however in some cases the directly connected device, router, switch, hub, modem, bridge, does not negotiate correctly. In those cases you may need to manually set the correct port speed and duplex settings.

NOTE: Typically if auto-negotiation does not work, use 10 / full.

CABLING: Keep in mind that you may need to use a cross-over cable when connecting the Edge platform directly to a router or firewall device. You should get a yellow or green link light indicating that the cable is working correctly.

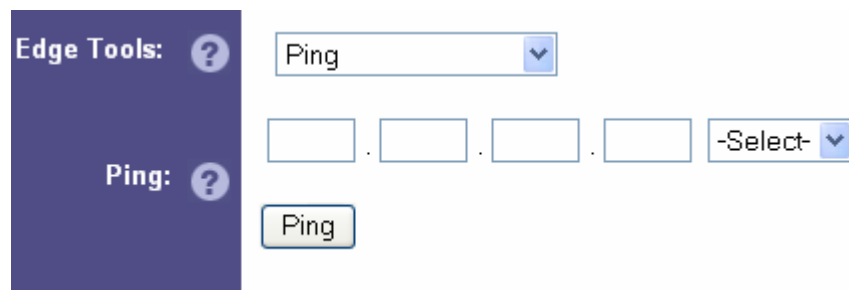


Verifying Connectivity

The following tools should be used when troubleshooting various connectivity issues.

Ping

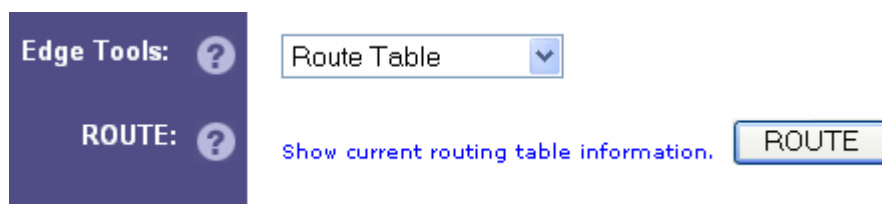
Sends a standard ICMP request to a device to determine its status and the route status... A good response says that the route is up and active.



NOTE: Make sure to select the port to use when sending out the ping.

Routing

Use to determine the correct status of the route configuration.



NOTE: The following is an example of a route report.

Routes:

```
216.237.18.41 interface wan1
192.168.1.254 interface wan2

192.168.100.0/24 via 10.200.10.2 interface tun1

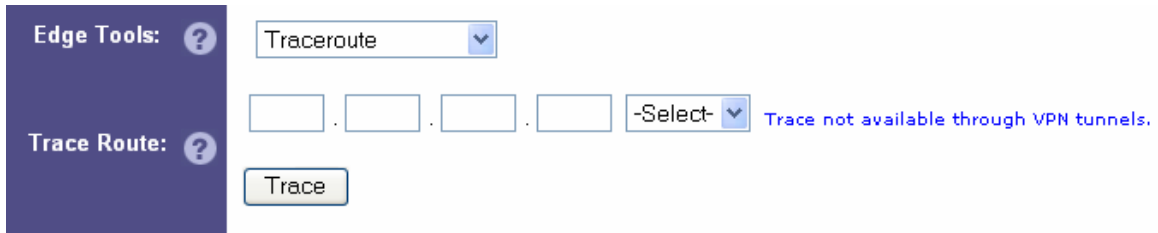
10.50.0.0/16 via 192.168.168.128 interface lan
10.1.0.0/16 via 192.168.168.128 interface lan
10.20.0.0/16 via 192.168.168.128 interface lan
10.30.0.0/16 via 192.168.168.128 interface lan
Gateway
via interface wan1 weight 8
via interface wan2 weight 2
```

Addresses:

```
int0 127.0.0.1/8 brd 127.255.255.255
int0 10.254.168.254/24
int0 10.254.168.253/24
int0 10.254.168.252/24
int0 10.254.168.251/24
int0 10.254.168.250/24
int0 192.168.168.1/24
int1
int1
int1
int2 192.168.1.100/24
int3 192.168.167.1/24
int3 10.200.10.1 peer 10.200.10.2/32
```

Traceroute

Use to verify the entire routing path between the Edge platform and a remote router and/or device on the network. Helpful when testing where an outage has occurred.



NOTE: Make sure to select the proper interface to use for the trace.

Arp

This tool can be used for various purposes; however it is typically used to reset the ARP table information when the Edge platform is first inserted into a new network environment.

- Click the ARP button will generate the current status of the ARP table.
- Click ResetARP will force local ARP table to update and will attempt to force the updating of the ARP tables of locally connected devices.
- The AutoShaping button is only used in custom deployments, it is not recommended for general use.

Edge Tools: ? Arp Table

ARP: ? Show current arp table information. ARP

60 (Default ARP Timeout Always Shown)

Update

AutoShaping (Will automatically populate traffic policies with the current ARP information)

ResetARP (When in proxy mode, this will attempt to reset ARP cache within the LAN network devices)

NOTE: You may add and delete ARP entries via this page, however it is not recommended.

Adjusting Link Settings

When setting up the WAN connections it may be required from time to time to adjust the Link Control settings. These are used by the Edge platform to determine whether a link is operating correctly and whether the link should be active or inactive.

Metrics

Changing the metrics is the easiest way for the administrator to affect link control. It is typically recommended that the "Metric Failure" be changed first, i.e. set higher in the event that a link is consistently going down.

Edge Tools: ? Link Control

Link Control: ?

180 (Route Flap Holdtime - Seconds)

5 (Metric Packets - Count default '5')

3 (Metric Timeout - Seconds default '3')

2 (Metric Failure - Count default '2')

NOTE: The route flap option is used to determine how long the Edge platform will wait after a link change state occurs. This should not be lowered beyond 45 seconds.

NOTE: The total number of seconds that a link must be down before a failure is determined can be calculated by multiplying the packets x timeout x failure.

Site Testing

When a failure is detected the Edge platform will begin a second series of tests to common websites, including the ones below.




<input type="text" value="www.google.com"/>	(Link Test Web Address #1)
<input type="text" value="www.yahoo.com"/>	(Link Test Web Address #2)
<input type="text" value="www.ebay.com"/>	(Link Test Web Address #3)
<input type="text" value="www.fedex.com"/>	(Link Test Web Address #4)
<input type="text" value="www.cnn.com"/>	(Link Test Web Address #5)
<input type="text" value="www.msn.com"/>	(Link Test Web Address #6)

If this third test fails the link will be turned down and deactivated.

Link Testing

This setting determines how the Edge performs its testing initial testing, if the gateway is unpingable, i.e GW-DOWN on the Home page, you may want to change the link testing to Probe Only, which may resolve the problem.

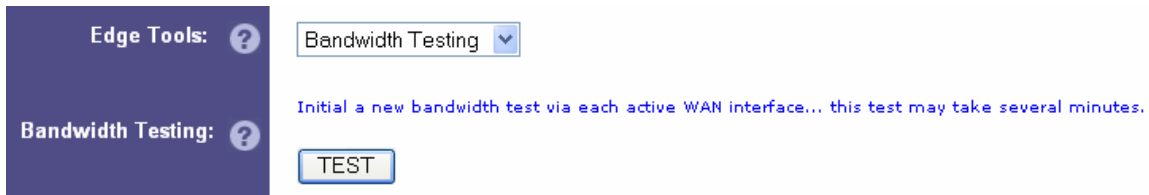


Gateway/Probe Probe Only Gateway Only

Bandwidth Testing

Performing a bandwidth test out to the Internet after inserting the Edge platform WILL NOT provide an accurate bandwidth speed. This is due to the bandwidth testing application only using a single session for the speed test. Because only a single session is used, the speed test will only use one of the available links for the test.

For this reason, the Edge includes its own bandwidth testing module.



This module will perform a bandwidth speed test by downloading a 1Mb file and then determine what the max download speed through each of the WAN links.

Bandwidth Speed Test - 03/15/07,02:12:22 PM



NOTE: The test takes up to five minutes to run, so do not attempt to re-run the test within a five minute period. Simply click the “Refresh” button to see if the update has occurred (as seen below).

The bandwidth report is being generated. New reports generally take several minutes to generate. Continue to click the Refresh button below to view the latest test results.

Bandwidth Speed Test - 03/15/07,02:17:37 PM

*** wan1 download time 26 seconds, speed 769 Kbps

*** wan2 download time 8 seconds, speed 2500 Kbps

*** wan3 download time 26 seconds, speed 769 Kbps

Total WAN Download Speed 4038 Kbps

Once the test has been completed the full download speed can be found for each link as well as the total download speed.

Changing XOS VPN Params

The XOS VPN parameters are used to adjust how the Site2Site tunnels work and how the optimization of those tunnels can affect the responsiveness of the traffic between the sites.

Caution: Do not change unless you are sure of what you are doing.

(TCP Window Scaling [latency ms] - default 80)

(TCP Window Scaling [Mbits per second] - default 100)

(TCP Retries - default 3)

(TCP Timeout - default 5)

(TCP MTU/MSS Size - default 1500)

(PMTU Discovery Threshold - default 1450)

(Tunnel Holdtime - default 30)

(Tunnel Test Timing - default 5)

TCP Windowing

These settings are used to determine how the Edge platform handles its TCP window sizing. The smaller you make these variables, the smaller the window sizing will be and thus the faster the acknowledgements. Smaller values can be used if a great deal of your traffic is small packets.

TCP MTU Settings

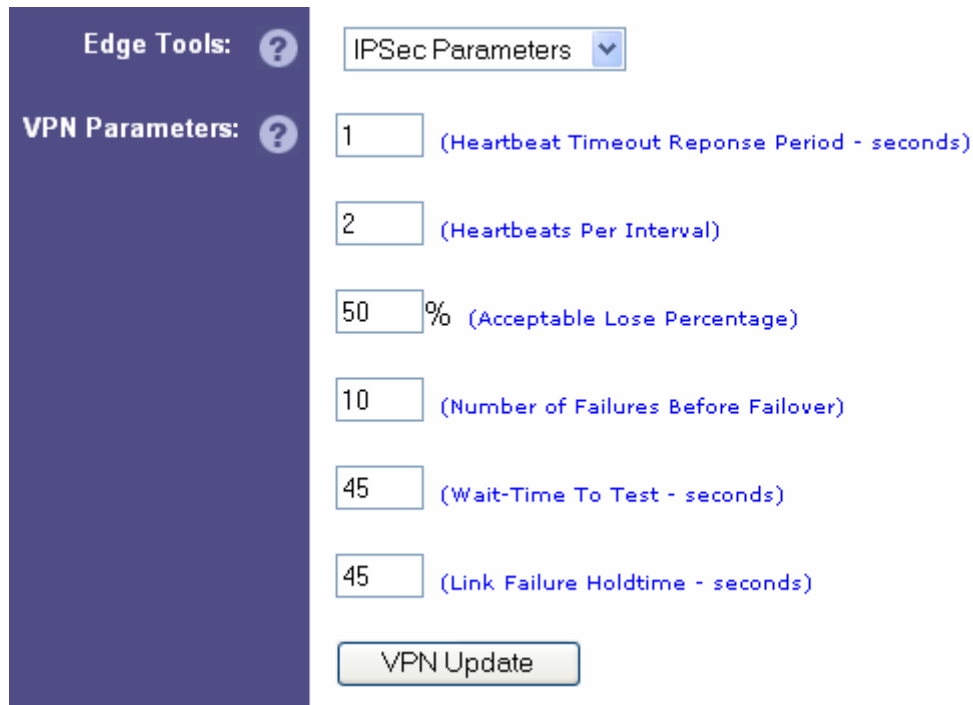
To be used when there may be a device within the route which is fragmenting the tunnel traffic. In these cases it may be required to pre-fragment the traffic in order to increase the speed and responsiveness of large packet data.

Tunnel Testing

Typically these settings should not be changed, however they can be adjusted if you feel the tunnels need to be more responsive to immediate network outages.

Changing IPSec Params

Typically these parameters only need to be changed in the event that you are having problems with the IPSec connection. If the IPSec tunnels are bouncing or going down under heavy traffic conditions, this is normally due to the testing mechanism not getting good responses. The methods used for this testing can be adjusted via the variable below.



The screenshot shows a configuration interface for VPN parameters. On the left is a dark blue sidebar with 'Edge Tools: ?' and 'VPN Parameters: ?'. The main area has a dropdown menu set to 'IPSec Parameters'. Below it are six input fields with their respective descriptions: '1 (Heartbeat Timeout Reponse Period - seconds)', '2 (Heartbeats Per Interval)', '50 % (Acceptable Lose Percentage)', '10 (Number of Failures Before Failover)', '45 (Wait-Time To Test - seconds)', and '45 (Link Failure Holdtime - seconds)'. At the bottom is a 'VPN Update' button.

Heartbeat Testing

The heartbeat settings are used to determine the number of attempts and the interval between each attempt within a single test.

Failures

This is a key variable which can be adjusted to decrease the sensitivity for temporary network problems or periodic high traffic volumes.

Wait-Time

This variable is used to determine how often a test occurs; this variable can also be changed to decrease IPSec VPN sensitivity.

Holdtime

This variable determines how long the testing system will pause after an outage is detected, which helps to hold down IPSec VPN flapping.