



April 2009

Common Application Guide

WAN Failover Using Network Monitor

Brief Overview of Application

To increase reliability and minimize downtime, many companies are purchasing more than one means of accessing the internet. The intent is to allow one internet connection to take over if the other fails. In the case of T1, this is easily accomplished. Since the layer 2 encapsulation (PPP, HDLC, Frame Relay) is where the negotiation takes place, the interface itself will always go down when connection is lost. As less expensive, more abundant connections using Ethernet such as cable, DSL, and fiber become more and more commonplace in a workplace environment, they create new failover problems. Since the router is often connected to an intermediary device, such as a cable modem, even if the connection is lost, the Ethernet connection between the router and the modem stays up. As far as the router is concerned, the connection is still good and traffic will continue to be transmitted.

Network Monitor was created, in part, to assist in situations like these. It allows the configuration of ping “probes”, that ping a certain destination from a certain source IP at a user specified interval. When the probe starts failing and hit the user specified threshold the router can take action to remove the route and divert traffic elsewhere. When the probe starts to pass again, the router can divert traffic back to the primary link.

Hardware/Software Requirements/Limitations

Network Monitor was introduced in 14 code, so the router must be running 14 code or greater. Additionally, the 3200 series, even with 14 code, is not compatible with Network Monitor.

Configuration in CLI and web GUI

Most of the configuration can be accomplished through the web, however one single command has to be entered via the CLI. This command enables “Fast NAT Failover”. Fast NAT Failover is designed to automatically clear all open firewall sessions when a route table change occurs. This is crucial because if the policy sessions were not cleared out, the router would still try to send traffic from existing sessions out from the failed IP address until the session timed out, resulting in a loss of connectivity.

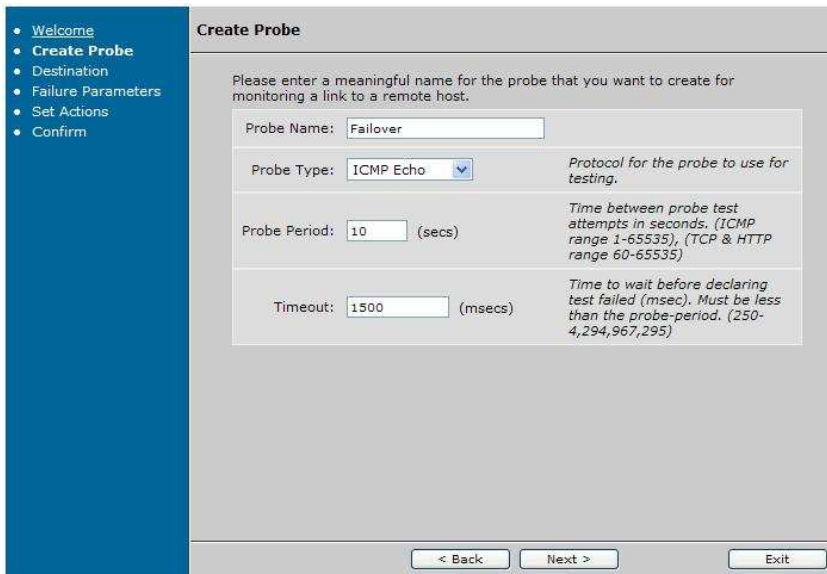


Configuring in the GUI

One of the tools that makes Network Monitor easy to configure is the wizard. Start by navigating to Network Monitor and clicking “Wizard”



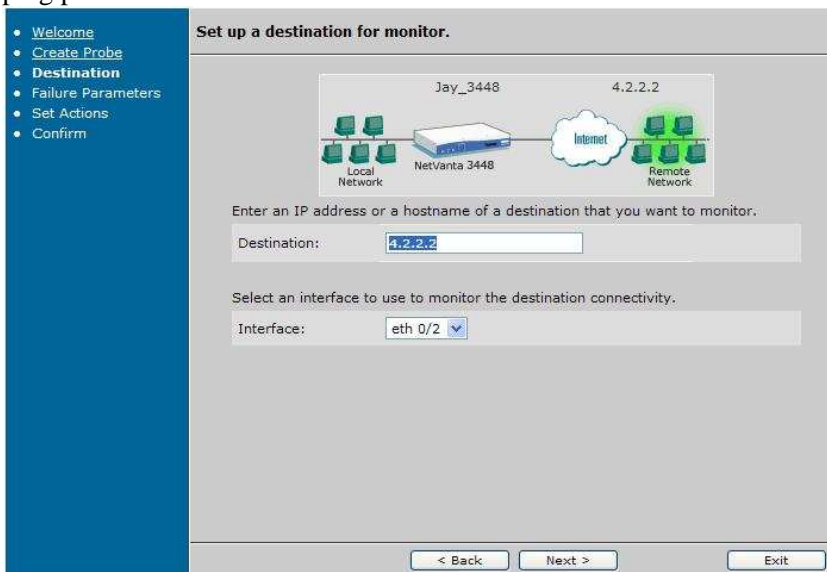
Click “Next” at the first wizard screen. Give the probe a unique name. The probe type should be set to ICMP echo. The probe period is the length of time between pings. There is no recommended time, but a period too long can affect failover time while a period too short can consume bandwidth. The timeout value should not need to be modified under normal circumstances. Click “Next”.

A screenshot of the "Create Probe" wizard screen. The screen has a blue sidebar on the left with a list of steps: Welcome, Create Probe (selected), Destination, Failure Parameters, Set Actions, and Confirm. The main area is titled "Create Probe" and contains the following fields and instructions:

- Probe Name: Failover
- Probe Type: ICMP Echo (dropdown menu). Instruction: Protocol for the probe to use for testing.
- Probe Period: 10 (secs). Instruction: Time between probe test attempts in seconds. (ICMP range 1-65535), (TCP & HTTP range 60-65535)
- Timeout: 1500 (msecs). Instruction: Time to wait before declaring test failed (msec). Must be less than the probe-period. (250-4,294,967,295)

At the bottom, there are three buttons: "< Back", "Next >", and "Exit".

At the next screen, enter the IP address the router will ping for the probe. This should be an address that will remain up almost 100% of the time. For the purposes of this example, a Level 3 DNS server has been chosen. Also, select the public interface connected to the cable modem. This determines the source IP address of the ping packet.

A screenshot of the "Set up a destination for monitor" wizard screen. The screen has a blue sidebar on the left with a list of steps: Welcome, Create Probe, Destination (selected), Failure Parameters, Set Actions, and Confirm. The main area is titled "Set up a destination for monitor." and contains a network diagram and the following fields:

- Network diagram showing a "Local Network" connected to a "NetVanta 3448" router, which is connected to the "Internet" (cloud), which is connected to a "Remote Network". The router is labeled "Jay_3448" and the remote network is labeled "4.2.2.2".
- Destination: 4.2.2.2
- Interface: eth 0/2 (dropdown menu)

At the bottom, there are three buttons: "< Back", "Next >", and "Exit".

Next, specify the number of failures before the router considers the link down as well as the number of successes before the router considers it back up. There is no recommended minimum, however setting the number of failures too low could cause the link to bounce in the event the ping is set to a short interval.

Set up failure mode.

Select the mode of failure to determine if the link to the destination is failing so that appropriate actions can be taken.

None

Consecutive *The probe will allow the specified number of consecutive test passes and failures before declaring probe state.*

Number of Failures:

Number of Successes:

Rate *The probe will allow the rate of test failures or successes before declaring probe state (X of Y).*

Number of Failures (X):

Number of Successes (X):

Total number of Tests (Y):

< Back Next > Exit

Next, set up the route failover. The interface or IP that is specified will be the default route that the router removes in the event of a failure.

Set up actions based on probe failure.

Set up an action to be performed once the probe reports failure (destination is unreachable over the link specified).

None *Do not perform any action.*

Disable static route *Create a default static route with the next hop IP or an interface you provide that becomes inactive when the probe fails.*

Next Hop IP: . . .

Next Hop Interface:

< Back Next > Exit

Finally, confirm all settings and click “Finish”.

Confirm Settings

Please review the settings that you have configured for network monitoring. You may use the "Back" to change any incorrect settings or "Finish" to complete your setup.

Probe Name:	Failover
Probe Type:	ICMP Echo
Probe Period:	10
Timeout:	1500
Destination (Interface):	4.2.2.2 (eth 0/2)
Type of Failure:	Consecutive Failures
Number of Consecutive Failures:	5
Number of Consecutive Successes:	5
Action:	Over-ride Static Route

< Back Finish Exit

Once the network monitor has been configured, a change must be made to the existing NAT statement in order to allow the failover.

If you do not currently have any firewall rules configured, navigate to Firewall Wizard and run the wizard. Select your primary interface as your WAN interface.

After running the firewall wizard, or if there are existing policies in place, Navigate to the private security zone and click on the Many:1 NAT pertaining to the Ethernet based connection.

Configure Policies for Security Zone 'Private'

New policies can be added to Security Zone 'Private' by clicking the "Add Policy" button. Existing policies can be modified or deleted or their evaluation order may be changed using the list below.

Add New Policy to Security Zone 'Private'

Add Policy to Zone 'Private'

Modify/Delete Policies in Security Zone 'Private'

To view or modify an existing policy, click the "Description" link in the desired row.

Priority	Description	Action
▲ ▼	Traffic to NetVanta	Advanced <input type="button" value="Delete"/>
▲ ▼	NAT list wizard-ics	Advanced <input type="button" value="Delete"/>

Traffic not matching one of the policies above will be blocked.

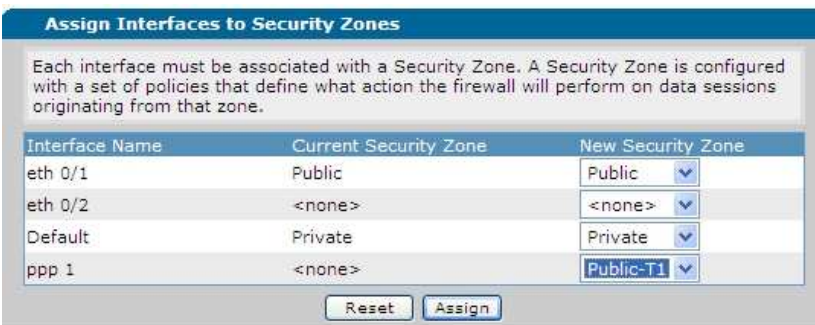
Change the “Destination Security Zone” to be the security zone assigned to the Ethernet interface. This will cause the router to check for a valid route out of that policy class before using the NAT. If the failover has occurred, the NAT will not be used.



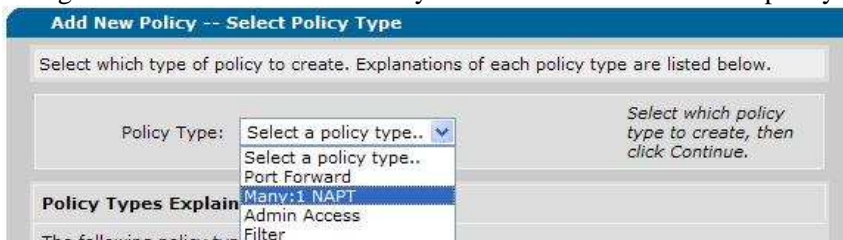
Next, navigate back to Security Zones and click to add a new security zone. Name it for your second internet connection and click Apply.



Back in Security Zones, under Assign Interfaces to Security Zones, use the drop down to assign your new Security Zone to your secondary interface and click Apply.



Navigate back to the Private Security Zone and click to add a new policy. Select Many:1 NAT.



Fill in the appropriate information for the T1 interface NAT. This is the policy that will allow traffic to be sourced from the T1 interface in the event of failover. Click “Apply” to complete the configuration.

Add New Policy to Security Zone 'Private'

Policy Type: Allows hosts in the 'Private' Security Zone to share a single public IP address for Internet access.

Policy Description: Optional description for this policy

Many:1 NATP Data

Allow all hosts in the 'Private' Security Zone to share the Public IP Address. The NetVanta will perform source address/port translation (NAPT) on all packets from hosts on this network

Specify selected hosts in the 'Private' Security Zone to share the Public IP Address.

disabled > Address: . . .

disabled > Mask: . . .

Public IP Address: Interface: All packets from the hosts selected above will appear to be sourced from this IP address.

Specified: . . .

Navigate to "Route Table" and create the route for the secondary ISP. It must have an administrative distance entered so that is only used when the primary route is removed by the probe.

Add a Static Route to the Route Table

Static Routes are often required to reach networks that are not learned via a dynamic routing protocol. Enter the appropriate information below to add a static route or click on a route below to use it as a template for a new route. [IP Routing](#) must be enabled in order to add static routes.

Destination Address: . . . Enter the network to add to the route table.

Destination Mask: . . . Enter the appropriate mask for this network.

Gateway:

Address . . . Enter the gateway address to reach this network.

Interface - OR -
Select the interface to be used as the gateway.

Administrative Distance (optional): The Distance metric for this network. (Optional parameter)

For the final part of the configuration, telnet to the unit. At the prompt, enter the following commands:

Router> **enable**

Router# **conf t**

Router(config)# **ip firewall fast-nat-failover**

This series of commands causes the router to clear out all existing firewall sessions in the event of a routing change and allows for a more immediate failover.

Configuring in the CLI

1. Navigate to the global config prompt and create the probe. This probe will be the ping that determines connectivity.

Syntax: **probe** <probe name> **icmp-echo**

EX: (config)# **probe FAILOVER icmp-echo**

2. Specify the time between pings. This is variable based on the amount of sensitivity desired as well as the amount of traffic that will be generated.

Syntax: **period** <time in seconds>

EX: (config-probe-FAILOVER)# **period 5**

3. Specify the destination for the probe. This IP address should be one that will remain up nearly 100% of the time, but will be unreachable if the internet were to fail.

Syntax: **destination** <hostname or IP address>

EX: (config-probe-FAILOVER)# **destination 4.2.2.2**

4. Specify the source address for the probe. This is the address the router will list as the source on the ICMP packet.

Syntax: **source-address** <ip address>

EX: (config-probe-FAILOVER)# **source-address 208.61.209.1**

5. Specify the failure tolerance for the probe. These numbers will determine how many pings must fail for the router to label the link as down and how many must pass for it to label it up again. In the example below, 5 consecutive failures will bring the link down while two consecutive passes will bring it back up again.

Syntax: **tolerance consecutive fail** <number of failures> **pass** <number of passes>

EX: (config-probe-FAILOVER)# **tolerance consecutive fail 5 pass 2**

6. Administratively enable the probe.

EX: (config-probe-FAILOVER)# **no shutdown**

7. Now, create the track. The track monitors the probe and can be linked to a static route in order to remove it when the probe fails.

Syntax: **track** <track name>

EX: (config-probe-FAILOVER)# **track WANTRACK**

8. Add the probe to the track.

Syntax: **test probe** <probe name>

EX: (config-track-WANTRACK)# **test probe FAILOVER**

9. Add the track to the static route the needs to be removed in the event the probe fails. This should be the default route for the primary interface.

Syntax: **ip route** <A.B.C.D A.B.C.D A.B.C.D> **track** <track name>

EX: (config)# **ip route 0.0.0.0 0.0.0.0 208.61.209.2 track WANTRACK**

10. Create an access list to match the ICMP traffic being sent from the probe.

Syntax: **ip access-list extended** <list name>

EX: (config)# **ip access-list extended pingprobe**

Syntax: **permit icmp any** <destination IP of probe>

EX: (config-ext-nacl)# **permit icmp any 4.2.2.2**

11. Create a route-map to force the ICMP traffic out of the primary interface. This will be critical because if the probe fails over along with the rest of the traffic, it will pass and the failover will be negated.

Syntax: **route-map** <map name> **permit** <sequence number>

EX: (config)# **route-map ICMP permit 10**

Syntax: **match ip address** <ACL name>

EX: (config-route-map)# **match IP address pingprobe**

Syntax: **set ip next-hop** <default gateway of primary interface>

EX: (config-route-map)# **set ip next-hop 208.61.209.2**

12. Assign the route map globally to the router. This will force all traffic generated by the router that matches the ACL out of the primary interface.

Syntax: **ip local policy route-map** <route map name>

EX: (config)# **ip local policy route-map ICMP**

13. Now, failover for NAT needs to be set up. There should be a separate security zone for each public interface. The primary NAT out to the internet must be linked to the appropriate policy. A secondary NAT must also be created in the event of failover. This will cause the router to monitor for valid routes out of that policy before the traffic goes through NAT. If failover has occurred, no valid route will exist and the router will move on to the secondary NAT.

Syntax: **nat source list** <ACL name> **address** <public IP> **policy** <policy attached to interface>

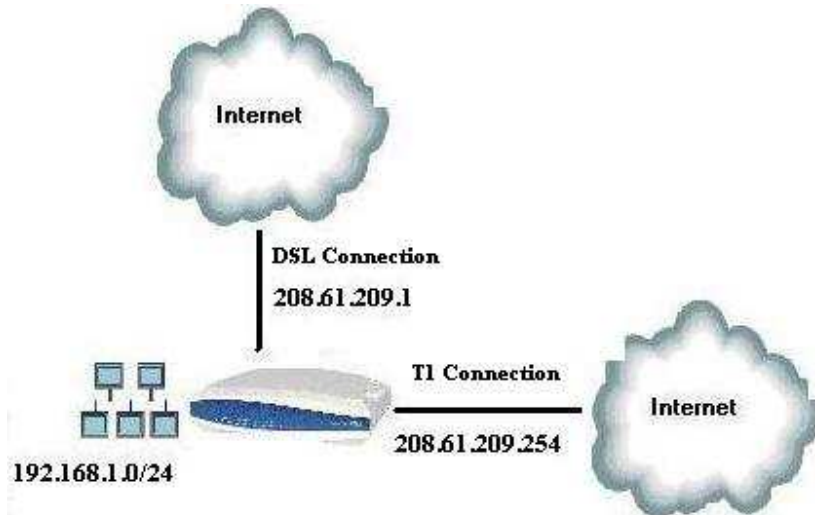
EX: (config-policy-class)# **nat source list matchall address 208.61.209.1 overload policy Public1**

EX: (config-policy-class)# **nat source list matchall address 208.61.209.254 overload**

14. Finally, enable fast-nat-failover from the global config prompt. This will cause the router to clear out all existing firewall sessions in the event of a route change. This way, all traffic will be immediately sent through the new interface with only slight delay rather than waiting for existing session to timeout.

EX: (config)# **ip firewall fast-nat-failover**

Example configuration



```
(config)# probe Failover icmp-echo
(config-probe-Failover)# destination 4.2.2.2
(config-probe-Failover)# source-address 208.61.209.1
(config-probe-Failover)# period 10
(config-probe-Failover)# tolerance consecutive fail 5 pass 2
(config-probe-Failover)# no shutdown
(config-probe-Failover)# track Failover
(config-track-Failover)# test if probe Failover
(config-track-Failover)# no shutdown
(config-track-Failover)# ip policy-class Public1
(config-policy-class)# ip policy-class Public2
(config-policy-class)# interface eth 0/1
(config-eth 0/1)# ip address 208.61.209.1 255.255.255.252
(config-eth 0/1)# access-policy Public1
(config-eth 0/1)# shutdown
(config-eth 0/1)# interface eth 0/2
(config-eth 0/2)# ip address 208.61.209.254 255.255.255.252
(config-eth 0/2)# access-policy Public2
(config-eth 0/2)# no shutdown
(config-eth 0/2)# route-map Failover permit 1
(config-route-map)# match ip address Failover-ACL
(config-route-map)# set ip next-hop 208.61.209.2
(config-route-map)# ip local policy route-map Failover
(config-route-map)# ip access-list extended Failover-ACL
(config-ext-nacl)# permit icmp any host 4.2.2.2
(config-ext-nacl)# ip access-list extended matchall
(config-ext-nacl)# permit ip any any
(config-ext-nacl)# ip policy-class Private
(config-policy-class)# nat source list matchall address 208.61.209.1 overload policy Public1
(config-policy-class)# nat source list matchall address 208.61.209.254 overload
(config-policy-class)# exit
```

```
(config)# ip firewall fast-nat-failover
(config)# ip route 0.0.0.0 0.0.0.0 208.61.209.2 track Failover
(config)# ip route 0.0.0.0 0.0.0.0 208.61.209.253
```