HP Network Node Manager i-series Software

Improving Monitoring Accuracy with ICMP

Software Version 8.13 Patch 6



The out-of-the-box configuration for NNMi exclusively uses SNMP to monitor nodes that support SNMP. Occasionally routers and switches get busy and do not respond to SNMP for periods of time. Sometimes NNMi incorrectly identifies these unresponsive nodes as down due to no SNMP response. You can make adjustments to the SNMP monitoring retry and timeout values, but even that may be insufficient to prevent false NodeDown notifications.

One way to improve this is to add ICMP monitoring to enhance the monitoring of SNMP capable nodes. This paper explains the steps to use to decrease the number of false NodeDown notifications. By following the example shown in this paper, you can implement a similar solution and improve the accuracy and reliability of notifications in NNMi.

NOTE: The author uses ICMP and ping interchangeably throughout this paper.

HP Network Node Manager i-series Software Improving Monitoring Accuracy with ICMP

LEVI.	٦С
	10

False Alarms	3
Adding ICMP for Better Results	5
The Wrong Approach	6
The Right Approach	
Creating an Interface Filter	
Create a Monitoring Policy	
Validate the Monitoring Policy	15
Validate the Node Status	17
Additional Configuration	
Conclusion	

False Alarms

The following example shows a router that gets too busy to respond to SNMP for long periods of time. Suppose we have a router called mimcisco5500. Using the out-of-the-box (default) settings, NNMi does not use ICMP (ping) to monitor nodes. Instead it strictly uses SNMP for monitoring. NOTE: There is one exception; NNMi uses ICMP to monitor non-SNMP nodes.

In the example shown in Figure 1, observe that NNMi shows mimcisco5500 as critical or down, but the router is actually up and just not responding to SNMP. In addition to the map notification, NNMi generates a NodeDown incident. Under these circumstances, you do not want to be alerted that mimcisco5500 is down.



Figure 1: False Alarm Example

You can see from the node form shown in Figure 2 that NNMi monitors this node using SNMP only; none of the IP addresses are being pinged.

🕲 Node : "mimcisco5500" - Mozilla Firefox	
File View Tools Actions Help	
🔄 🖹 😼 Save and Close 🗙 Delete Node 🔂	Node
Basics	General IP Addresses Interfaces VLAN Ports
Name mimdisco5500 Hostname mimdisco5500.superpoller21.mim Management Address 10.97.90.66 Status Critical Node Managed Management Mode Managed State State SNMP Agent State State State Not Responding State State State Not Responding State September 22, 2009 3:36:43 PM MDT SNMP Agent mimcisco5500.superpoller21.mim Discovery Image Device Profile ciscoWSX5302 Discovery State Discovery Completed Last Completed September 22, 2009 3:01:04 PM MDT	Ports Capabilities Custom Attributes Node Groups Component Health Diagnostics Incidents Status Conclusions Registration Custom Polled Instances Image: State State State Image: State
Notes	Updated: Total: 3 Selected: 0 Filter: OFF Auto refresh: OFF
Done	

Figure 2: Default Monitoring Uses SNMP not ICMP

You can see in Figure 3 that the outage lasted almost exactly five minutes, which corresponds to one polling cycle. One easy method to check outage duration from NNMi is to do the following:

- 1. Open the **Custom Incidents** workspace and filter on Message=Node Down.
- 2. Look at the Correlation Notes to see how long the outage lasted.

This feature is only available in NNMi 8.13 Patch 5 or later.

Figure 3: Outage Duration



Since mimcisco5500 is actually up and functioning in our example, this probably means that mimcisco5500 stopped responding to SNMP for a period of time. However, when the next polling cycle came around (five minutes by default), mimcisco5500 resumed responding to SNMP. You can confirm this by manually trying to ping mimcisco5500 while it is marked as down. If it responds to ping, it is not really down.

Adding ICMP for Better Results

Since mimcisco5500 responds to ping even when it does not respond to SNMP, you decide to add ICMP monitoring.

ping 10.97.90.66
PING 10.97.90.66 (10.97.90.66) 56(84) bytes of data.
64 bytes from 10.97.90.66: icmp_seq=0 ttl=59 time=3.33 ms
64 bytes from 10.97.90.66: icmp_seq=1 ttl=59 time=2.45 ms

Mimcisco5500 is a router. Suppose you decide to add ICMP monitoring to all of your routers.

First, check to see which monitoring policy is being used on this node. On the node form shown in Figure 4, select **Actions**->**Monitoring Settings**.

Figure 4: Checking Monitoring Policy

😻 Node : "mimcisco5500" - Mozilla	a Firefox	
File View Tools Actions He	lp	
Wode : "mimcisco5500" - Mozilla File View Tools Actions He Image: Save Layer 2 N Layer 3 N Image: Save Layer 3 N Node Gro Basics Ping (from Trace Rou Name Trace Rou Trace Rou Hostname Communic Status Po Node Status Po Configura Node Status Po Configura SNMP Agent State SNMP Supported Manage (I State Last Modified Manage (I State Device Profile Ciscowery Device Profile Ciscowery Show Attate Discovery State Discovery Last Completed Septem Septem	a Firefox p eighbor View up Map 1 server) isterver) ite (from server) (from dient) iton Settings Settings I iton Poll - Repert Menu Reset All) e 1.mim iton Poll - Report Menu Backed End Nodes SX5302 itor Polleted itor 22, 2009 3:01:04 PM MDT	Node
Notes	Updated: Total: 3 Selected: 0 Filter: OFF Auto refresh: 0) FF
Done		

As you can see in Figure 5, NNMI sets the polling using the Routers Node Group monitoring policy.



🥹 Monitoring Configuration for mimcisco5500.superpoller21.mim on no 💶 💌			
Monitoring Config mimcisco5500.su mimcisco5500	uration for perpoller21.mim on node		
SNMP Mo	nitoring Summary		
Fault SNMP Polling Enabled	true		
Fault Polling Interval	0 days 0 hours 1 minutes 0 seconds		
Management Mode	Managed		
Monitoring	Settings Applied		
Type Node	Settings		
Node Group Route	Node Group Routers		
Fault Polling Interval 0 days 0 hours 1 minutes 0 seconds			
D			
Done	1.		

The Wrong Approach

Your first thought might be to enable ICMP for all routers. Suppose you decide to do that now. IMPORTANT: Do not try this on your system right now. This is only for discussion purposes. Continue reading to the end of this paper for a better approach. Click Monitoring Configuration as shown in Figure 6.

Figure 6: Navigate to the Monitoring Configuration Workspace

🐸 HP Network Node Manager : deployhpux1.cnd
MP Network Node Manage
File Tools Actions Help
Workspaces
Incident Management
Topology Maps
Monitoring
Troubleshooting
Inventory
Management Mode
Incident Browsing
Support
Integration Module Configuration
Configuration
Communication Configuration
Discovery Configuration
Monitoring Configuration
Custom Poller Config_ation
Incident Configuration
Status Configuration
Node Croups
Node Group Map Settings
Interface Groups

Click the **Node Settings** tab and open the Routers selection as shown in Figure 7.

Figure 7: Open the Routers Selection

😻 Monitoring Configuration - Mozilla Firefox		
File View Tools Actions Help		
🚈 🛅 🏂 Save and Close 🚭	Monitoring Config	uration
Global Control	Interface Settings Node Settings Default Settings	
If disabled, previous device state and status values remain unchanged. See Help \to Using the Monitoring Configuration form.	When multiple settings are defined, NNMi applies them according to the Ordering number (lowest number first).	
Enable State Polling	1-4of 4	
Monitoring may be globally disabled for these object types and all previous state	C A OF EIFP ESFP ECHFP ECHPP PUI PIHIA ESPP Name	
will be reset.	🗖 🔟 🏹 100 - 🗸 🗸 - 🗸 🗸 Routers	
Enable Component	🗖 🔟 🚧 200 - 🗸 🖌 Networking Infrastructure I	
Health Polling	🗆 🔟 Open - 🧹 Microsoft Windows System:	
Redundancy Group	🗖 🔟 🖉 400 🗸 🗸 Non-SNMP Devices	
NNMi monitors each discovered Interface according to the first matching configuration		

Select the Enabled ICMP Fault Polling box; then click Save and Close as shown in Figure 8.

😻 Node Settings : "com.l	np.ov.nms.monitoring.groups.model.No	odeGroup{addToPerfSPIReports = true
File View Tools Act	tions Help	
🖄 🔡 🔀 Save and	Close 🎽 🗙 Delete Node Settings	3
(i) Changes are not comm	nitted until the top-level form is saved!	
Basics		Threshold Settings (Unlicensed)
Ordering	100	
Node Group	Routers 🖉 🛪	If the optional NNM iSPI for Performance
Fault Monitoring		
Enable ICMP Fault Polling		
Enable SNMP Fault Polling		
Enable Component Health Fault Polling		
Fault Polling Interval	0 Days 0 Hours	
Performance Monitorin	g (Unlicensed)	
Configuration for the optio	onal NNM iSPI for Performance.	

Figure 8: Enabling ICMP Fault Polling

Now all addresses on all routers will be pinged as shown in Figure 9.



[] Node : "mimcisco5500" - Microsoft Internet Explorer provided by	y Hewlett-Packard	
File View Tools Actions Help		
🚈 🔡 🎭 Save and Close 🛛 🗙 Delete Node 🚱		Node
Basics Imminisco5500 Hostname 10.97.90.97 Management Address 10.97.90.97 Status Minor Node Managed Management Mode Managed SNMP Agent State SNMP Agent State SNMP Agent State Imministration State Normal State Last Modified October 4, 2009 10:43:22 AM MDT SNMP Agent 10.97.90.97 Discovery Imministration Device Profile IciscoWSX5302 Discovery State Discovery Completed Last Completed October 4, 2009 10:43:55 AM MDT	General IP Addresses Interfaces VLAN Ports Ports Capabilities Custom Attributes Node Groups Component Health Diagnostics Incidents Status Conclusions Registration Custom Polled Instances Incidents Status Conclusions Registration Custom Polled Instances St. St. St. Address In Interface In Subnet Image: St. St. St. Address In Interface In Subnet Image: St. St. St. St. No. Image: St. <	

This approach has a few problems. First, many routers have addresses that will never be reachable by the NNMi management server. This causes these routers to always have a Minor status because not all of the addresses are reachable. This also causes NNMi to generate many AddressNotResponding alarms. Second, NNMi issuing so many pings causes undue ping traffic and strain on the NNMi management server. All you really want is NNMi to do a simple ping against just one address on the router. This is illustrated in Figure 10. So you decide to undo this change and consider a better solution.



Figure 10: Router Has Minor Status Due to Unreachable Addresses

The Right Approach

A better solution is to be more selective about the addresses you configure NNMi to ping. You will need to analyze your network to see what the best approach is for your environment. The ideal solution, in most cases, is to ping the management address on nodes; however this currently is not an option in NNMi. Instead, you should work with your network administrator to make a list of the addresses that would be best to monitor using ping.

NNMi distinguishes between interfaces and addresses, but the two are tightly coupled. NNMi does not provide monitor filtering at the address. Instead, you filter based on interfaces; then apply ICMP monitoring to these interfaces. This in turn causes NNMi to ping addresses that are hosted on these interfaces.

Many customers using Cisco routers will have a loopback interface and address on their routers. These interfaces often have the name 100. These interfaces may host the best address to ping for your environment. For this example, you do not have an 100 interface on this router. Instead you will use addresses hosted on the V1100 interface as your best addresses to ping. In this example, this happens to be your management VLAN, which should always be reachable by NNMi. You can change this example to use 100 if this is better for you.

Creating an Interface Filter

You need to create an interface group for the interfaces named VI100 residing on routers. To do this, select Interface Groups located in the Configuration workspace; then click New as shown in Figure 11.

Figure 11: Creating an Interface Group

🕲 HP Network Node Manager : deployhpux1.cnd.hp.com - Mozilla Firefox				
IP Network Node Manager				
File Tools Actions Help				
Workspaces	Interface Group -	Interface Groups		
Incident Management	(🔁 👍 🗙 🛛	😂 🕐 🗣 🖻		
Topology Maps				
Monitoring	New	▲ Name	AtVFL	AtFL
Troubleshooting		ISDN Interfaces	~	-
Inventory		Link Aggregation Interfaces	~	-
Management Mode		Point to Point Interfaces	~	-
Incident Browsing		Software Loopback Interfaces	~	-
Support		VLAN Interfaces	~	-
Integration Module Configuration		Voice Interfaces	~	-
Configuration		_		
Communication Configuration				
Discovery Configuration				
Monitoring Configuration				
Custom Poller Configuration				
Incident Configuration				
Status Configuration				
User Interface Configuration				
🕮 Node Groups				
Node Group Map Settings				
Interface Groups				
RAMS Servers				
Management Stations				
User Accounts and Roles				
User Principals				

Name this interface group IF_ping_addr_rtrs. Select the Routers node group; then set up an Additional Filter to choose interfaces with ifName = V1100 as shown in Figure 12.

Figure	12:	Filtering	Interfaces	with	ifName=VI10	0
--------	-----	-----------	------------	------	-------------	---

🕲 Interface Group : "IF_ping_addr_rtrs" - Mozilla Firefox	
File View Tools Actions Help	
🚈 📓 🛂 Save and Close 🏥 🗙 Delete Interface Group	Interface Group
Basics	IfType Filters Additional Filters
Name IF_ping_addr_rtrs Add to View Filter List Node Group Routers Notes	When using the like or not like operators, use an * (asterisk) to match zero or more characters in a string and a ? (question mark) to match exactly one character in a string. To create an inclusive IP address range, use the between operator. Valid example: ipAddress between 10.10.1.1 AND 10.10.1.255 Filter Editor Attribute Operator Value iffName IfName Image: string st
You can filter interface groups using IfType filters and Additional Filters. An interface must pass all of these filters to belong to a specified interface group. If a Node Group is defined, the interface must belong to a node that is a member of that Node Group. See Help → Using the Interface Group form. To test your interface group definition, select File → Save, then Actions → Show Members.	• ifName = V1100 AND
NNM iSPI Performance	

Now validate that this filter is working as expected. After saving the Interface Group shown above, select Actions->Show Members as shown in Figure 13.

Figure 13: Validate the Filter

😻 Interface Group : "IF_	_ping_addr_rtrs" - Mozilla Firefox		
File View Tools Ac	Show Members In erface Group Reporting - Report - enu	3	Interface Group
Basics Name Add to View Filter List Node Group	IF_ping_addr_rtrs Routers		IfType Filters Additional Filters When using the like or not like operators, use an * (asterisk) to match zero or more characters in a string and a ? (question mark) to match exactly one character in a string. To create an inclusive IP address range, use the between operator. Valid example: inAddress between 10. 10. 1. 1. AND 10. 10. 1.255

You should see the interfaces you expect as shown in Figure 14. In this simple example you only have one of these interfaces but in practice you should have many. The goal is to have one interface per router.

Figure 14: Expected Interfaces

IF_ping_addr_rtrs (Interfaces)	I 1 − 1 of 1	
IfType IfSpeed IfDescription	IfAlias	Status
ethernetCsmacd 100 Mbps Vlan 100	6:-> mimHp4k1sw:	Oct 4, : 📥
	IF_ping_addr_rtrs (Interfaces) IfType IfSpeed IfDescription ethernetCsmacd 100 Mbps Vlan 100	IF_ping_addr_rtrs (Interfaces) Image: If Content in the second secon

Create a Monitoring Policy

The next step is to create a monitoring policy associated with this interface group. You enable ping in this policy. Click **Monitoring Configuration** under the **Configuration** workspace as shown in Figure 15.

Pretwork Node Manager : deployhpux1.cn	id.hp.com - Mozilla Firefox	
MP Network Node Manag	ger	
File Tools Actions Help		
Workspaces	Interface Group - Interface Groups	
Incident Management	1 1 1 X 2 C 9 1	
Topology Maps		
Monitoring	▲ Name	A
Troubleshooting	IF_ping_addr_rtrs	•
Inventory	ISDN Interfaces	
Management Mode	🔲 📺 🔼 Link Aggregation Interfaces	
Incident Browsing	Point to Point Interfaces	
Support	🔲 📺 Software Loopback Interfaces	~
Integration Module Configuration	VLAN Interfaces	~
Configuration	Voice Interfaces	
Communication Configuration		
Discovery Configuration		
Monitoring Configuration		
Custom Poller Configuration		
Incident Configuration		
Status Configuration		
🖾 User Interface Configuration		
III Node Groups		
Node Group Map Settings		
Interface Groups		

Figure 15: Navigate to the Monitoring Configuration Workspace

Click the **Interface Settings** tab; then click the **New** button as shown in Figure 16. Take note of the current ordering values. This new policy must be a higher priority (a lower number) than any current policy. In this example, any number lower than 100 is fine.

Figure 16: Click New to Start a New Interface Monitoring Policy

🕹 Monitoring Configuration - Mozilla Firefox	
File View Tools Actions Help	
🚈 🛅 🛂 Save and Close	Monitoring Configuration
Global Control	Interface Settings Node Settings Default Settings
If disabled, previous device state and status values remain unchanged. See Help → Using the Monitoring Configuration form. Enable State Polling Monitoring may be globally disabled for these object types and all previous state will be reset.	When multiple settings are defined, NNMi applies them according to the Ordering number (lowest number first).
Enable Component	🔲 🖾 100 - 🗸 ISDN Interfaces 📥
Health Polling	🔲 📓 🙆 200 - 🗸 Point to Point In
Enable Router 🔽 Redundancy Group Polling	□ 🔲 🖂 300 - 🗸 VLAN Interfaces

Enter an Ordering value, then select the Interface Group you previously defined, IF_ping_addr_rtrs. Next, check the **Enable ICMP Fault Polling** box as shown in Figure 17. Click **Save and Close** all the way out to the top level.

Figure 17: Enabling ICMP Fault Polling

🕲 Interface Settings - Mozilla Firefox	
File View Tools Actions Help Image: Save and Close Image: Save and Close Image: Save and Close Image: Save and Close Image: Save and Close	Interface Settings
Basics Ordering Interface Group ITE ping addr. rtrs PDD	Threshold Settings (Unlicensed) If the optional NNM ISPI for Performance is enabled, set the low and high values to
Fault Monitoring Enable ICMP Fault	Getermine Interface performance state.
Polling Fault Polling Interval	
Performance Monitoring (Unlicensed)	1

Validate the Monitoring Policy

Now open the node form again and look at the IP Addresses tab. Notice that NNMi is now monitoring only one address using ICMP as shown in Figure 18. You may need to execute a status poll on the node to make sure you see the new status.

Node : "mimcisco5500	" - Microsoft Internet Explorer provide	by Hewlett-Packard	
Actor	nd Close X Delete Node		Nod
Basics	mimcisco 5500	General IP Addresses Interfaces VLAN Ports Ports Capabilities Custom Attributes Node Groups Component Health Diagnostics	5
Hostname Management Address Status	10.97.90.97 10.97.90.97 Normal		
Node Management Mode	Managed 💌	St St Address In Interface In Subnet □	
SNMP Agent State SNMP Supported State	I✓ Normal	Image: Constraint of the state of	
State Last Modified SNMP Agent	October 4, 2009 10:43:22 AM MDT		
Discovery Device Profile	ciscoWSX5302		
Discovery State Last Completed	Discovery Completed October 4, 2009 10:40:55 AM MDT		
Notes			

Figure 18: Monitoring One Address Using ICMP

To confirm that the address is being monitored using your newly created policy, open the Address form for address 10.97.90.97. Then select **Actions**->**Monitoring Settings** for this address as shown in Figure 19.

Figure 19: Select Monitoring Settings

🕲 IP Address : "10.9	97.90.97" - Mozilla Firefox			
File View Tools	Actions Help			
A B Save	Layer 2 Neighbor View Layer 3 Neighbor View Node Group Map Path View			IP Address
Basics Address Prefix Length Status	Ping (from server) Trace Route (from server) Trace Route (from dient) Telnet (from dient) Conifouring Settings Configuration Pol		Incidents Capabilities Status Conclusions Registration	
Management Mode Direct Management Mode	Manage Unmanage Out of Service			A A
IP Address State	Desservation			
State Last Modified	October 4, 2009 10:56:34	AM MDT		
In Interface Hosted On Node	VI100 mimcisco5500	∰ ▼		
In Subnet	10.97.90.96/27	r 👘		

As you can see in Figure 20, ICMP Polling Enabled is set to true; that is due to the monitoring policy applied to the IF_ping_addr_rtrs filter. This is what you expected.

Figure 20: Monitoring One Address as Expected

🥹 Monitoring Configuration for 10.97.90.97 on node mimcisco5500 - Mo 💶 🗙			
Monitoring Co mimcisco5500	nfiguration for 10.97.90.	97 on node	
TCM	IP Monitoring Summary		
Eault ICMP Polling En	abled true		
Fault Polling Interval	0 days 0 hours 5 minutes 0 seconds		
Management Mode	Managed		
Monito	oring Settings Applied	\triangleright	
Туре	Interface Settings	.0	
Interface Group	IF_ping_addr_rtrs		
Node Group	Routers		
Fault Polling Interval	0 days 0 hours 5 minutes 0 seconds		
Done		11.	

Validate the Node Status

Finally, bring up the node form again and check the status and conclusions. You may need to run a status poll against the node to make sure it has accurate status. You can see in Figure 21 that the node status is Normal and conclusions on the node are good.

Node: "mimcisco550	0" - Mozilla Firefox		
👍 🔡 😼 Save and	Close X Delete Node		Noc
Basics		General IP Addresses Interfaces VLAN Ports Capabilities	
Name	mimcisco 5500	Custom Attributes Node Groups Component Health Diagnostics	
Hostname	10.97.90.97	Incidents Status Conclusions Registration Custom Polled Instances	
Status Node Management Mode	Normal Managed	Outstanding Status Conclusions	
SNMP Agent State — SNMP Supported		Stat Time Stamp Conclusion	11
State	Normal	🔲 🛅 🖉 10/4/09 11:45 PM NodeUp	
State Last Modified	October 4, 2009 10:43:22 AM MDT	🔲 📓 🧭 10/4/09 11:45 PM InterfacesUpInNode	
SIMP Agent	10.97.90.97	Till AllResponsiveAddressesInNode	
Discovery		III 2 10/4/09 11:45 PM Responsive AgentInNode	
Device Profile	ciscoWSX5302		
Discovery State Last Completed	Discovery Completed October 4, 2009 10:40:55 AM MDT		

Figure 21: Validate the Node Status

As you can see from the status poll results shown in Figure 22, reliability and accuracy are increased since NNMi now does both an ICMP poll against the reachable address and SNMP monitoring. This will reduce false notifications.

Figure 22: Status Poll Results

😻 Status Poll of 10.97.90.97 - Mozilla Firefox
Status Poll of 10.97.90.97
Using client timeout value of 600 secs
**** Poll started for node 10.97.90.97 at 2009-10-05 08:59:49 (management station time) ****
Policy: IP Address Availability ICMP (Ping) Monitoring Target: 10.97.90.97
Object roundTripTime
10.97.90.97 0 (Responding)
Policy: SNMP Agent Availability Monitoring Target: 10.97.90.97 Poller: NnmSnmpPoller, Target Responding: true, Poll Successful: true, Poll Duration: 3 mSec sysUpTime 16705153 (Normal)
Policy: SNMP Interface Health
Target: 10.97.90.97 Poller: NnmSnmpPoller, Target Responding: true, Poll Successful: true, Poll Duration: 6 mSec Object ifAdminStatus ifOperStatus
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$
**** Poll has completed for node 10.97.90.97 at 2009-10-05 08:59:51 (management station time) ****

Additional Configuration

Repeat this process for other network gear such as switches. The process may be simpler for switches because many times a switch has only one address. In that case, you can create a monitoring policy for switches and enable ICMP polling for the node group without having to identify specific interfaces.

Conclusion

By adding selective ICMP monitoring to the monitoring policies of NNMi, you increase the reliability and accuracy of monitoring, resulting in fewer false notifications when monitored nodes are simply too busy to respond to SNMP in a timely manner. If you follow the steps presented in this paper, you can improve NNMi monitoring accuracy.