HP Automated Network Management

Solution Version: 9.10

Concepts Guide

Document Release Date: June 2011 Software Release Date: June 2011



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2010–2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe is a trademark of Adobe Systems Incorporated.

AMD is a trademark of Advanced Micro Devices, Inc.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Intel, Itanium, and Intel Xeon are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the New users - please register link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport user ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1	Introduction to ANM	7
	Network Management Concepts	8
	ANM Products	. 10
	HP Network Node Manager i Software	. 11
	HP Network Automation Software	. 12
	HP Network Node Manager iSPI Performance for Metrics Software	. 13
	HP Network Node Manager iSPI Performance for Traffic Software	. 14
	HP Network Node Manager iSPI Performance for Quality Assurance Software	. 15
	NNM iSPI Network Engineering Toolset Software	. 16
2	Solution Benefits	17
2	Secondria 1. Identify and correct an out of compliance device shange	. 17
	Scenario 1: Identify and correct an out-of-compliance device change	. 10
	Process without ANM	. 10
	Process with ANM	. 10
	Comparie Q. Troublasheet returnsh fault increas	. 19
	Dracess Without ANM	. 19
	Process without ANM	. 19
	Process with ANM	. 19
	Denenits 2. Dene library ID-4 - library to the annumints ID-6 - library	. 20
	Scenario 3: Re-address IPv4 addresses to the appropriate IPv6 addresses	. 20
	Process without ANM	. 20
	Process with ANM	. 21
	Benefits	. 21
	Scenario 4: Troubleshoot application performance problems from a network context	. 21
	Process Without ANM	. 21
	Process with ANM	. 22
	Benefits	. 22
	Scenario 5: Ensure edge routers maintain expected service levels	. 23
	Process Without ANM	. 23
	Process with ANM	. 23
	Benefits	. 23
	Scenario 6: Use baseline data to identify abnormal system utilization	. 24
	Process Without ANM	. 24
	Process with ANM	. 24
	Benefits	. 25
	Scenario 7: Identify and correct error rate and utilization problems	. 25
	Process Without ANM	. 25
	Process with ANM	. 25
	Benefits	. 26

appreciate your feedback!

1 Introduction to ANM

Automated Network Management (ANM) is a solution that integrates network fault detection, performance monitoring, configuration management and compliance, as well as diagnostic and automation tools. ANM enables the ITILv3 best practices in the network domain—namely event, incident, and problem management; change configuration; and release and deploy management.

ANM enables the IT organization to:

- Reduce the Mean Time to Repair (MTTR).
- Increase the Mean Time Between Failures (MTBF).
- Become policy compliant.
- Reduce mean time to change network configuration.
- Increase the service level agreement (SLA) with faster return on investment (ROI).

ANM is comprised of six individual, but integrated, products that are brought together in the HP Automated Network Management Suite:

- HP Network Node Manager i Software (NNMi)
- HP Network Automation Software (NA)
- HP Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics)
- HP Network Node Manager iSPI Performance for Traffic Software (NNM iSPI Performance for Traffic)
- HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA)
- NNM iSPI Network Engineering Toolset Software (NNM iSPI NET)

ANM Advanced includes additional iSPI Points license keys and adds the capability for the iSPI Points to be used with the NNM iSPIs for advanced services:

- HP Network Node Manager iSPI for MPLS Software (NNM iSPI for MPLS)
- HP Network Node Manager iSPI for IP Multicast Software (NNM iSPI for IP Multicast)
- HP Network Node Manager iSPI for IP Telephony Software (NNM iSPI for IP Telephony)

ANM provides the following capabilities for efficient network management:

- Network change and configuration management
- Network performance management
- Network fault management
- Network run-book automation
- Network diagnostics

These capabilities enable the following actions:

- Network diagnostics
- Automated event enrichment
- Network performance and metrics management (including traffic management)
- Discovery, inventory, and topology management
- Network fault management
- Compliance and configuration monitoring
- Network change, configuration, and deployment management
- Network event and incident management
- Change automation as a result of a network fault

The HP Network Node Manager Smart Plug-ins (NNM iSPIs) provide valuable insight into the current health and ongoing trends in your network. They assist with processes for increasing availability and performance management functionality while lowering associated support costs and improving capacity management and planning.

Network Management Concepts

As networks continue to expand, network services and topologies increase in complexity. In addition, many networks must now comply with regulations and security best practices, all of which results in a complex infrastructure with multiple protocols, technologies, and vendors to support. Centrally managing the network infrastructure in a secure, automated, and efficient fashion becomes vital to the network's performance and for preventing additional security vulnerabilities and complete outages, which can cause increased liability, lost revenues, and lost productivity.

In this complex situation, the need for managing and monitoring can be divided into three major fields:

• **Availability and Incident Management:** A basic network management requirement is to know whether a network outage is presently occurring, and, if so, the root cause of the outage. Network managers need immediate visibility into the source of the root cause, be it hardware failure or any other environmental reason.

Network managers also need to see their network diagram as it is in reality, which devices exist on the network and how they are connected.

• **Performance Analysis:** Most network management problems are those where no outage is occurring but a customer complains that the network service level is poor—affecting the business quality of service (QoS). In this case, network managers need advanced troubleshooting tools for understanding the root cause of this behavior. These tools can show basic real-time and historical performance data (for comparison purposes), such as utilization and errors, as well as IP traffic analysis examining if the source of the problem is an application that overloads the network. These tools also provide internet protocol service level agreement (IP SLA) information, which shows whether the QoS polices are correctly configured.

• **Change and Configuration Management and Compliance:** Everyday tasks such as changing the configuration on devices (as a result of problems or other infrastructure changes) and adding new devices to the network can consume a lot of time. When these tasks are performed manually on a large number of devices, configuration mistakes can result in poor network performance or, in a worst case scenario, a network outage.

Proper network configuration management requires that all configurations be made according to required compliance policies and that an archive of the configuration changes be retained.

ANM Products explains how ANM can provide for these network management needs with easy-to-use products that can make day-to-day operations easier and more efficient.

Figure 1 displays which HP Network Management Center products fulfill the needs described in this chapter. Chapter 2, Solution Benefits elaborates how the ANM solution products that are part of this center fulfill those needs.



Figure 1 HP Network Management Center Products

ANM Products

HP Automated Network Management enables customers to reduce costs and increase agility through process automation across all network operations. Unlike point product approaches, ANM is an integrated solution portfolio that automates event, performance, change and configuration management, and other IT processes.

Figure 2 shows the ANM products in relation to primary network management needs. The following sections describe each of these products.



Figure 2 Relationship of the ANM Products

HP Network Node Manager i Software

NNMi provides smart network fault and availability monitoring using common network protocols such as SNMP and ICMP to help you maintain a healthy network across your organization. NNMi can discover network nodes (such as switches and routers) on an automatic and continuing basis, providing an up-to-date representation of the network topology (Layers 2 and 3).

NNMi uses an accurate picture of the network to pinpoint network problems by using topology-based root cause analysis (RCA). Together, RCA, advanced correlation features, and a *management by exception* incident management model provide a dynamic fault management solution for an ever changing network environment.

NNMi also monitors device health indicators such as CPU and memory utilization along with interface performance metrics such as utilization and interface errors. Real-time performance indicators can be monitored at intervals as fine as one second through live performance graphs.

From an operational point of view, NNMi is the center of ANM. You can access each of the other tools in the solution through the NNMi console, the ANM single pane of glass.



Figure 3 NNMi

HP Network Automation Software

NA is an enterprise-class network device change and configuration management tool. It eliminates human error in device configuration changes while also maintaining compliance standards through a policy-based change management model. NA maintains a complete audit trail of all device changes, including a key stroke log of command line changes made through the NA telnet proxy.

NA supports thousands of network device model and operating system combinations from the major vendors, including Cisco, Nortel, Juniper, HP, 3Com, F5, Alcatel–Lucent, and Extreme.

NA minimizes MTTR using configuration archiving and deployment and tracks the following information:

- Changes made to network devices.
- Initiator of each change.
- Current device configurations.
- Device configuration compliance with organizational standards.

Figure 4 NA

HP Network Automat	ion Reports • Admin •	Help -							
S Home Back G		unde .							
aarch	Home	í.							
	My Homepage	Statistics D	Jashboard						
or Hostname	My Tasks							My Device Groups	
Search Connect	Pty Tasks							40Groups Bar Corp	
Search For	Task Name					Schedule Date	Status	Bellevue	
	Update Device	Software				Jun-23-20 11:00:00	Pending	<u>CiscoDyna</u> CiscoRouter2600.105.12	
Workspace	Showing 1 to	-life) Vie						CiscoRouter2600.IOS.12	
Current Device Group	Snowing a ta	SK(SJ. MS	W All					<u>CiscoSwitch</u> Core Bouters	
	Recent Chan	nes Past 1	donth 🗸					Default Customer	
My Favorites	Date:	Develop	Channed Bu			8.481mm		Default Function Default Site	
twork Status Report	bate	Device	Changed By	Comments		Action		DellDevices	
licy Activity arch For Single Search	Jul-01-10	lab-2621	manager_auto			Compare to previous	View Config	 Detected Devices6179111 Detected Devices6179501 	
atistics Dashboard sk Templates	14:25:57	ſ	(details)					Salaria Salaria	
Ivice Password Rules	Jul-01-10	lab-2621	🐻 ntc2ext-	-gw3				Add to Favorites	Help
irtitions in "Site"	14:25:20								
ompliance Center - Home	Jul-01-10	lab-2621	Hostname	ntc2ext-gw3					
	12:01:49		Device IP	172,19.1.1	Startup and Ru	inning Configurations o	liffer		
Ny Settings	Jul-01-10	c1841-ror	Last Enanchot Atte	Mar. 19.11 09:03:31	View Startup C	Compare Startup with Run	ning Synchronize		
/ Workspace	11:07:31		Last Snapshot Res	Configuration unchanged					Watch Device
/ Permissions	Jul-01-10	c1841-ror	Manu a Edit a	Devision & Connect #					Harst States
Jick Launch	11:06:13		View • Eur. •	Provision Connecs -					
	Jun-29-10	WS-C375	1 Lines Changed	0	1 Lines Inserted		2 Lines D	eleted	
	13:47:47		Show differences	with context O Show full text O Show	UNIX-style diff	Deploy to running o	onfiguration		
	Jun-29-10	Cisco 298	Deploy to startup co	nfiguration and reboot		Deploy to startup co	onfiguration and reboot		
	13:37:00	78	Compare this with pi	revious configuration		This is the curren	t configuration		
	Jun-28-10	Lab-C292	Older Configuration	on		Newer Configura	tion		
	17:50:08		Device ntc2ext	t-gw3 (172.19.1.1)		Device ntc2ex	t-gw3 (172.19.1.1)		
	Jun-22-10	Lab-C292	Date May-10	0-11 20:03:21		Date May-1	1-11 14:03:24		
	17:16:34		Changed By N/A			Changed By N/A			
	Jun-22-10	lab.2521	Configuration Comments			Configuration			
	10:01:37	INC AVER	267 shutdown			shutdown			267
	10101107		268 j 269 i provface Ta	atTthernet2/20		!	herner2/20		268
	Showing 10 o	of 52 chang	270 description	connection to traffic 2950		no ip address			270
			271 ip address	172.20.2.161 255.255.255.248		1. C			221
	Recent Event	ts Past 2 W	273 ip route-ca	che flow		ip route-cache	flow		272
	Event Summa	ary				shutdown			273
	Task Complete	d	274 speed 100			speed 100			274
	Contra Contra I		275 duplex full			duplex full			275
	Device Group P	Additied	276 j			1			276
	Task Started		402 network 10.	6.3.144 0.0.0.7 area 0		network 10.6.3.	144 0.0.0.7 area 0		402
			403 network 10. 404 network 172	8.8.8 0.0.0.3 area 0 15 100 0 0.0.0 255 area 31		network 10.8.8. network 172.16	8 0.0.0.3 area 0	91	403
			405 network 172	.16.101.0 0.0.0.255 area 31		network 172.16.	101.0 0.0.0.255 area	31	405
			406 network 172	.16.103.0 0.0.0.255 area 31		network 172.16.	103.0 0.0.0.255 area	31	404
			408 network 172	16.181.32 0.0.0.31 area 0 2.19.1.0 0.0.0.255 area 30		network 172.19.	181.32 0.0.0.31 area 1.0 0.0.0.255 area 3	0	408
			409 network 172	.20.2.152 0.0.0.3 area 0		network 172.20.	2.152 0.0.0.3 area 0		409
			410 network 172			nerwork 192 159	1 0 0 0 0 255 area	2	410
			412 1			!		~	411
			413 router bop 2	16		router bgp 26			412

HP Network Node Manager iSPI Performance for Metrics Software

NNM iSPI Performance for Metrics provides the performance reporting foundation (the Network Performance Server, or NPS) for ANM. NNMi is the polling engine for both fault and performance. NNM iSPI Performance for Metrics provides the performance database for up to 13 months of data retention and the reporting tool for both predefined and custom reports.

The main capabilities of NNM iSPI Performance for Metrics are:

- Historical graphs of performance data.
- Performance metrics and baseline threshold monitoring.
- Performance baseline reports.
- Performance forecast reports'.

Figure 5 NNM iSPI Performance for Metrics

Current Status												
Username: admin		(p)	NNM iSPI	Performance				Interface	Health - Inte	erfaceMetrics	- Тор N	
Package: Interface_Health		Options	s <u>Show Bookm</u>	<u>ark Help</u>								
Folder: InterfaceMetrics Report: Top N		7			1.15-00 PM ()	a that was a first	la Nama - akaŭ					
Status: Ready		1 May	/ 19, 2011 12:15:001	PM - May 19, 2011	1:15:00 PM (Last	I Hour), Noc	ie Name = htc2t	ext-gw5.ntc2.i	np.com			
		Σ Gro	uped by: Qualifie	d Interface Nam	e : Interface Ty	/pe						
Reports												
- California - Cal	^	Rank	Qualified	Interface	Volume -	Percent	Utilization	Utilization		Utilization	Utilization	Bar Chart
Charling InterfaceMetrics			Interface Name	туре	Bytes (sum)	or ALL for	In -	Out -	Utilization	Forecast	Forecast	Volume -
Baseline Sleeve						Volume	Average	Average	(avg)	Baseline (4	Baseline (4	Bytes
Calendar						- Bytes (sum)	(avg)	(avg)		(avg)	(avg)	(sum)
Chart Detail		1	Fa3/37 on	ethernetCsmacd	6,725,696,350	49,70%	9.31%	6.17%	13,45%	6,27%	16,84%	
Dashboard		-	(ntc2ext-		-,,,,							
Executive		2	Fa3/1 on (ntc2ext-	ethernetCsmacd	4.061.291.946	30.01%	0.11%	9,46%	8.91%	0.13%	6,79%	
Headline			gw3.ntc2.hp.com)									
Headline - Wireless LAN		3	Fa3/47 on (ntc2ext-	<u>ethernetCsmacd</u>	2,740,893,649	20.26%	5.95%	-0.03%	6.06%	6.23%	-24.43%	
Heat Chart			gw3.ntc2.hp.com)									
Managed Inventory		4	Polon (ntc2ext- aw3.ntc2.hp.com)	propVirtual	1,225,221	0.01%	-0.51%	0.17%	0.01%	47.00%	-3.66%	1
Most Changed		5	Fa3/45 on	ethernetCsmacd	1,216,147	0.01%	-0.40%	-1.94%	0.02%	93.57%	-6.82%	1
Overview			(ntc2ext- aw3.ntc2.hp.com)									
Peak Period		6	Fa3/48 on	ethernetCsmacd	890,456	0.01%	0.00%	0.00%	0.00%	0.00%		1
Threshold Sleeve			(ntc2ext- gw3.ntc2.hp.com)									
Top N		z	Fa3/46 on	ethernetCsmacd	156,421	0.00%	0.00%	2.14%	0.00%	0.00%	-0.43%	1
Top N Chart			(ntc2ext- gw3.ntc2.hp.com)									
📧 🚞 iSPI Quality Assurance			<u>Others</u>		0	0.00%						
📧 🧰 iSPI Traffic		Hide C	hart									
📧 🧰 Avaya IP Telephony		1	<u></u>									
🗄 🧰 Cisco IP Telephony				Do	tails for Top 1	0 Qualifi	ad Interface	Nama : Int	orfaco Tur			
🗄 🧰 Custom Collection	-			De	calls for Top I	o Quatine	eu internace		епасе тур	Je .		
		6,	,000,000,000					Comb	ined Elemen	t Name		
Report History		5.	000.000.000				-	Fa	3/37 on (ntc2 3/1 on (ntc2e	ext-gw3.ntc2.hp xt-gw3.ntc2.hp.o	.com) : ethern :om) : etherne	etCsma tCsmacd
								Fa	3/47 on (ntc2	ext-gw3.ntc2.hp	.com) : ethern	etCsmacd
Time Control	_	Ling 4,	,000,000,000					Po	3/45 on (ntc2ext-	ext-gw3.ntc2.np.co	m):propvirtua .com):ethern	at etCsma
Hour / Day Filters		3ytes	~~~~~					Fa	3/48 on (ntc2	ext-gw3.ntc2.hp	com) : etherne	etCsma
		<u> </u>						Fa	3/46 on (ntc2	ext-gw3.ntc2.hp	.com):ethern	etCsmacd
lopology Filters		l 10 2,	,000,000,000									
BI Server												
		1,	.000,000,000									
Dashboard Reportlets												
Cross Launching			12:10 1	2:15 12:20 12:25	12:30 12:35 12:40	12:45 12:50	0 12:55 13:00	13:05				

HP Network Node Manager iSPI Performance for Traffic Software

NNM iSPI Performance for Traffic extends NNMi performance monitoring by collecting NetFlow, sFlow, J-Flow, and IPFIX IP flow records exported from routers. These data enrich available network performance information. For example, you can use NNM iSPI Performance for Traffic data to understand why a network connection experiences high utilization.

NNM iSPI Performance for Traffic performs the following tasks:

- Aggregates the IP flow records.
- Correlates the obtained IP flow records with NNMi for context-based analysis.
- Generates maps to view the traffic flow information on your network.
- Generates performance reports by exporting data to the NPS.

Figure 6 NNM iSPI Performance for Traffic



HP Network Node Manager iSPI Performance for Quality Assurance Software

NNM iSPI Performance for QA extends NNMi to monitor the quality of traffic flow in the network by collecting data (using SNMP) from pre-configured IP SLA, RPM, and DISMAN-PING-MIB QA probes on the selected network elements. These data provide for monitoring the probes, displaying the service level data on site-to-site orientation, and threshold alarming.

NNM iSPI Performance for QA, in conjunction with NNMi, performs the following tasks:

- Discovers the pre-configured QA probes for various network elements.
- Provides for configuring additional QA probes.
- Monitors the status and test results of QA probes; alerts when configured thresholds are breached.
- Displays QA probe results in the NNM iSPI Performance for QA views.
- Generates performance reports by exporting data to the NPS.

Figure 7 NNM iSPI Performance for QA

QA Probes 🔷 QA Pro	obe										
0 5 5 5											
▼ QA Probe Details			Sta	te Thresh	old State Baselin	ne State	Status	Conclusions Incider	Registration		
Status	Normal		•								
Name	NTC to endnode12 ping	NTC to endnode12 ping									
Owner	dougg		2	🖬 😂	×			1 - 11 of 52			
Service	ICMP Echo	Ξ.	Ser	Life Last Oco	curren e e Cor S	ource Node	Message				
Admin Index	20		8	Q 4/14/11 7	:03:41 PM 🚺 nt	c2ext-gw2	QA Probe N	VTC to endnode12 ping fa	iled to run. Reason: O	ipi 🔨	
Manager	Local		0	Q 4/14/11 6	:59:41 PM 🚺 nt	c2ext-gw2	QA Probe I	NTC to endnode12 ping fa	iled to run. Reason: O	ipi 🗏	
			8	Q 4/14/11 6	:59:28 PM 🚺 nt	c2ext-gw2	High round	trip time for the QA Probe	NTC to endnode12 p	in	
 Source/Destination 	Info		8	Q 4/14/11 6	:49:41 PM	c2ext-gw2	QA Probe I	VTC to endnode12 ping fa	iled to run. Reason: O	ine internet	
Source	ntc2ext-gw2	-	8	4/14/11 6	:45:28 PM 🚺 nt	c2ext-gw2	High round	trip time for the QA Probe	NTC to endnode12 p	in	
Source IP Address	10.6.1.33		8	Q 4/14/11 6	:39:42 PM 🚺 nt	c2ext-gw2	QA Probe N	NTC to endnode12 ping fa	iled to run. Reason: O	(pr	
Source Interface			8	Q 4/14/11 6	:39:28 PM 🚺 nt	c2ext-gw2	High round	trip time for the QA Probe	e NTC to endnode12 p	in	
Source Site	wanywan		8	Q 4/14/11 6	:25:41 PM 🚺 nt	c2ext-gw2	QA Probe I	NTC to endnode12 ping fa	iled to run. Reason: O	(p)	
Source Port			8	Q 4/14/11 6	:21:41 PM 🔥 nt	c2ext-gw2	QA Probe N	NTC to endnode12 ping fa	iled to run. Reason: O	pi	
			llod	-	-27-10 PM MDT	Total	52 Sala	cted: 1 Eilter: OEE	Auto refreeh: (DEE	
				3160 571971112			02 0000				
Destination	endnode12	×	Cobo	ated. 5/19/11/02	21.101.1101						
Destination Analysis	endnode12		() ()	NNM iS	Pl Performance			Quality Assura	nce - QAMetrics - Mos	st Changed	
Destination Analysis Incident Summary : R	endnode12 RoundTripTimeHigh 😴	Details 😂	Option	NNM iSi Show Book	Pl Performance mark <u>Help</u>			Quality Assura	nce - QAMetrics - Mos	st Changed	
Destination Analysis Incident Summary : R	endnode12 koundTripTimeHigh 🍘 High round trip time for the QA Probe HTC to endnode12 ping. The reason for	Details 😳 Correlation N	Option V Ma	NNM iSi Show Bookr y 18, 2011 1:10:00	PI Performance mark <u>Help</u> AM - May 18, 2011 2:1	0:00 AM (Last 1	Hour)	Quality Assura	nce - QAMetrics - Mos	st Changed	
Destination Analysis Incident Summary : R	endnode12	Details 😨 Correlation N	Option Ma X Gr	NNM iSi Show Bookr y 18, 2011 1:10:00 ouped by: QA Pro	PI Performance mark Help AM - May 18, 2011 2:1 obe Name : QA Prol	0:00 AM (Last 1	Hour)	Quality Assura	nnce - QAMetrics - Mos	st Changed	
Destination Analysis Incident Summary : R Message	endnode12 toundTripTimeHigh 3 High round trip time for the QA Probe ITC to endnode12 ping. The reason for this state is, the measured value 207.0 meecs is higher than the upper bound of 100.0 mescs. The date and time for 100.0 mescs. The date and time for	Details 😴 Correlation N Category Family	Option ▼ Ma ∑ Gr	NNM iSi Show Bookr y 18, 2011 1:10:00 ouped by: QA Pro	PI Performance mark Help AM - May 18, 2011 2:1 obe Name : QA Prol	.0:00 AM (Last 1 be Type : Sou Change o	Hour) Irce Site : De: f Round Tr	Quality Assure stination Site ip Time (msecs) (ave	nce - QAMetrics - Mos	st Changed	
Destination Analysis Incident Summary : R Message	endnode12 toundTripTimeHigh 3 High round trip time for the 0A Probe IITC to endnode12 ping. The reason for this state is, the measured value 207.0 maecs is higher than the upper bound of 1000, msecs. The date and time for the measurement is 2011-04-14 18:45:27.147.	Details Correlation N Category Family Correlation N	Option Option ▼ Ma ∑ Gr Rank	NNM ISI Show Book y 18, 2011 1:10:00 ouped by: QA Pro QA Probe Na	PI Performance mark Help AM - May 18, 2011 2:1 obe Name : QA Prole	0:00 AM (Last 1 be Type : Sou Change 0 Source Site	Hour) Irce Site : De f Round Tr Destination	Quality Assura stination Site ip Time (msecs) (avg Previous Period	nice - QAMetrics - Mos a) Current Period	st Changed	Change
Destination Analysis Incident Summary : R Message Severity	endnode12 NoundTrpTimeHigh 3 High round trip time for the QA Probe ITC to endnode12 ping. The reason for this state is, the measured value 207.0 msecs is higher than the upper bound of 100.0 msecs. The date and time for the measurement is 2011-04-14 18:45:27.147.	Details Correlation N Category Family Correlation N Origin	Option ▼ Ma ∑ Gr Rank	VINM ISI NNM ISI Show Bookr y 18, 2011 1:10:00 ouped by: QA Probe Na	Pl Performance mark Help AM - May 18, 2011 2:1 obe Name : QA Prole Type	0:00 AM (Last 1 be Type : Sou Change 0 Source Site	Hour) Irce Site : De f Round Tr Destination Site	Quality Assure stination Site ip Time (msecs) (avg Previous Period From May 18, 2011 121:000 AM	a) Current Period From: Nay 18, 2011 11:10:00 AM	st Changed Growth Rate (%)	Change
Destination Analysis Incident Summary : R Message Severity Lifecycle State	endnode12 NoundTripTimeHigh 3 High round trip time for the QA Probe NTC to endnode12 ping. The reason for this state is, the measured value 207.0 msecs is higher than the upper bound of 100.0 msecs. The date and time for the measurement is 2011-04-14 18:45:27.147. Constant Registered	Details Correlation N Category Family Correlation N Origin Last Occurre	Option Option ▼ Ma ∑ Gr Rank	NNM ISI Show Bookr y 18, 2011 1:10:00 ouped by: QA Probe Na	PI Performance mark Help AM - Mey 18, 2011 2:1 obe Name : QA Prob Type	0:00 AM (Last 1 be Type : Sou Change o Source Site	Hour) Irce Site : Des f Round Tr Destination Site	Quality Assure stination Site ip Time (msecs) (avg <u>Previous Period</u> From May 18, 2011 From May 18, 2011 11:1000 AM	2) Current Period From: Nay 18, 2011 110:00 AM To: Nay 18, 2011 210:00 AM	St Changed	Change
Destination Analysis Incident Summary : R Message Severity Lifecycle State RCA Active	endnode12 RoundTripTimeHigh Record TripTimeHigh Record TripTimeHigh Record TripTimeHigh Record TripTimeHigh Record TripTimeHigh Record TripTimeHigh Record TripTimeHight Record TripTimeHight	Details 3 Correlation N Category Family Correlation N Origin Last Occurre Source Node	Option Option ▼ Ma Σ Gr Rank	NNM iSI Show Book y 18, 2011 1:10:00 ouped by: QA Pro QA Probe Na	PI Porformance mark Help AM - May 18, 2011 2:1 obe Name : QA Prob Type TCP Connect	0:00 AM (Last 1 be Type : Sou Change o Source Site wanvuan	Hour) Irce Site : Des f Round Tr Destination Site	Quality Assure stination Site fp Time (msecs) (avg Previous Period From: May 18, 2011 12:10:00 AM To: Way 18, 2011 11:0:00 AM 79:08) Current Period From: May 18, 2011 11:00:00 AM To: May 18, 2011 21:00:00 AM 5.03	Growth Rate (%)	Change -74.06
Destination Analysis Incident Summary : R Message Severity Lifecycle State RCA Active Source Object	endnode12 RoundTripTimeHigh High round trip time for the QA Probe NTC to endnode12 ping. The reason for this state is, the measured value 207.0 msecs is higher than the upper bound of 100.0 msecs. The date and time for the measurement is 2011-04-14 18:45:27.147. Registered false NTC to endnode12 ping (Q A Test Table View Data)	Details Correlation N Correlation N Category Family Correlation N Origin Last Occurre Source Node Source Obje	Coption ▼ Ma ∑ Gr Rank 1 2	NINM ISI Show Books y 18, 2011 1: 10:00 ouped by: QA Pri QA Probe Na UTC to Toronto tractionest ski yao Winter P	PI Performance mark Help AM - May 18, 2011 2:1 obe Name : QA Prol me QA Probe Type <u>TCP Connect</u>	0:00 AM (Last 1 be Type : Sou Change 0 Source Site wanywan mountaintop	Hour) irce Site : De f Round Tr Destination Site doucasite mountaintop	Quality Assure stination Site fp Time (msecs) (avy Previous Period From: May 18, 2011 12:10:00 AM To: May 18, 2011 11:10:00 AM 79:08 23.62) Current Period From: Nay 18, 2011 1:1000 AM 5:03 27:23	Growth Rate (%) -93.64% 15.31%	Change -74.06 3.62
Destination Analysis Incident Summary : R Message Severity Lifecycle State RCA Active Source Object Created/Opened	endnode12 Regulation of the QA Probe High round trip time for the QA Probe ITC to endnode12 ping. The reason for this state is, the measured value 207.0 msecs is higher than the upper bound of 100.0 msecs. The date and time for the measurement is 2011-04-14 Registered Registered false NTC to endnode12 ping (Q A Test Table View Data) 4/14/11 06:45 PM (Open for 34.8 days)	Correlation N Category Family Correlation N Origin Last Occurre Source Node Source Obje	Coption ▼ Ma ∑ Gr Rank 1 2 3	NNM iSI Show Book y 18, 2011 1:10:00 ouped by: QA Pro QA Probe Ne QA Probe Ne NTC to Toronto de you to Writer P de news de scho	PI Performance mark Help AM - Mey 18, 2011 2: 1 obe Name : QA Prolo Type TCP Connest ICP Connest UOP Eduo sseen ICMP Eduo	0:00 AM (Lest 1 be Type : Sou Change o Source Site wanvuan mounteintop mounteintop	Hour) irce Site : De f Round Tr Destination Site douacete mountaintoo	Quality Assure stination Site tip Time (msecs) (avg Previous Period From May 18, 2011 112:10:00 AM To: May 18, 2011 111:00 AM 79:08 23:62 26:73	3) Current Period From: Nay 18, 2011 11:10:00 AM To: Nay 18, 2011 12:10:00 AM 5:03 27.23 30.27	Growth Rate (%) -93.64% 15.31% 13.22%	Change -74.06 3.62 3.53
Destination Analysis Incident Summary : R Message Severity Lifecycle State RCA Active Source Object Created/Opened	endnode12 toundTripTimeHigh 3 High round trip time for the QA Probe IITC to endnode12 ping. The reason for this state is, the measured value 207.0 mescs is higher than the upper bound of 100.0 msccs. The date and time for the measurement is 2011-04-14 HighSiz 147. Second Second Second Second Second Second Second Registered false IITC to endnode12 ping (Q A Test Table View Data) 4/14/11 06:45 PM (Open for 34.8 days)	Correlation N Category Family Correlation N Origin Last Occurr Source Node Source Obje	Coption Cop	NINM IS NINM IS NINM IS NINM IS Show Book Y 18, 2011 1:10:00 Ouped by: QA Pro QA Probe Na QA Probe Na QA Probe Na NITC to Toronte Mittagenesi Statement Statement Statement Statement Statement	PI Performance mark Help AM - Mey 18, 2011 2: 1 obe Name : QA Prole Type TCP Connect Type TCP Connect ark: LOP Echo Issoen ICMP Echo	0:00 AM (Lest I be Type : Sou Change o Source Site wannuan mountaintoo mountaintoo mountaintoo	Hour) irce Site : De f Round Tr Destination Site douccette mountaintoe mountaintoe mountaintoe	Quality Assure stination Site tp Time (msecs) (avg Previous Period From May 18, 2011 10:000 AM To: May 18, 2011 11:000 AM 79.08 23.62 26.73 28.87	g) Current Period From: Nay 18, 2011 11:10:00 AM To: Nay 18, 2011 12:10:00 AM 5.03 27.23 30.27 29.13	Growth Rate (%) -93.64% 15.31% 13.22% 0.92%	Change -74.06 3.62 3.53 0.27
Destination Analysis Incident Summary : R Message Severity Lifecycle State RCA Active Source Object Created/Opened	endnode12 koundTripTimeHigh C High round trip time for the QA Probe NTC to endnode12 ping. The reason for this state is, the measured value 207.0 msecs is higher than the upper bound of 100.0 msecs. The date and time for the measurement is 2011-04-14 18:45:27.147. Registered Registered false NTC to endnode12 ping (Q A Test Table View Data) 4/14/11 06:45 PM (Open for 34.8 days)	Correlation N Category Family Correlation N Origin Last Occurs Source Node Source Obje	Coption Max Gr Rank 1 2 3 4 5	NINM IS NINM IS NINM IS Show Book Show Book Y 18, 2011 1:10:00 Ouped by: QA Pro QA Probe N QA Probe N NITC to Toronto de Vale Show Nine F de Showboat to 1 Io Toronto to Brie	PI Performance mark Help AM - May 18, 2011 2:1 Dobe Name : QA Probe Type CAP Probe Type TCP Connect CAP Echo Isseen ICMP Echo Isboe TCP Connect ICMP Echo	0:00 AM (Lest 1 be Type : Sou Change o Source Site wannuan mountaintoo mountaintoo mountaintoo doucoatia	Hour) Irce Site : De f Round Tr Destination Site douacete mountaintoo mountaintoo mountaintoo ferandavay	Quality Assure stination Site fp Time (msecs) (avy Frevious Period From: May 18, 2011 12:10:00 AM To: Way 18, 2011 11:0:00 AM 79:08 23:62 26:73 28:87 1.17	2) Current Period From: Nay 18, 2011 1:10:00 AM 5:03 27:23 30:27 29:13 1:00	Growth Rate (%) -93.64% 15.31% 13.22% 0.92% -14.29%	Change -74.06 3.62 3.53 0.27 -0.17
Destination Analysis Incident Summary : R Message Severity Lifecycle State RCA Active Source Object Created/Opened	endnode12 RoundTripTimeHigh C High round trip time for the QA Probe INTC to endnode12 ping. The reason for this state is, the measured value 207.0 msecs is higher than the upper bound of 100.0 msecs. The date and time for the measurement is 2011-04-14 16:45:27.147. C Constant Registered faise INTC to endnode12 ping (Q A Test Table View Data) 4/14/11 06:45 PM (Open for 34.8 days)	Details Correlation N Category Family Correlation N Origin Last Occurre Source Nobe	Coption Coption Max Rank 1 2 3 4 5 6	NINM IS NINM IS NINM IS Show Books Show Books Show Books NIC to Taronto NIC to Taronto NIC to Taronto Starobat to 1 Starobat to 2 Starobat to 2	PI Performance mark Help AM - Mey 18, 2011 2:1 Jobe Name : QA Probe Type ICP Connest Type ICP Connest and UDP Echo Sector ICP Connest ICPP Echo	0:00 AM (Lest 1 be Type : Sou Change 0 Source Site wannuan mountaintoo mountaintoo douscaite douscaite	Hour) Ince Site : De f Round Tr Destination Site douccelle mountaintop mountaintop mountaintop farandaway farandaway	Quality Assura stination Site ip Time (msecs) (avg <u>Previous Period</u> From May 18, 2011 12:10:00 AM To: May 18, 2011 11:10:00 AM 79:08 23:62 26:73 28:87 1.17 1.42	a) Current Period From: May 18, 2011 1:10:00 AM 5:03 27.23 30.27 29.13 1.00 1.25	st Changed Growth Rate (%) 15.31% 13.22% 0.92% -14.27% -11.76%	Change -74.06 3.62 3.53 0.27 -0.17 -0.17
Destination Analysis Incident Summary : R Message Severity Lifecycle State RCA Active Source Object Created/Opened	endnode12 koundTripTimeHigh 3 High round trip time for the QA Probe INTC to endnode12 ping. The reason for this state is, the measured value 207.0 msecs is higher than the upper bound of 100.0 msecs. The date and time for the measurement is 2011-04-14 10x4s27.147. Source Control (1) 10x4s27.147. Source Control (1) Registered false NTC to endnode12 ping (Q A Test Table View Data) 4/14/11 06:45 PM (Open for 34.8 days)	Correlation N Category Family Correlation N Origin Last Occurrs Source Noble	Copilian Copili	NINM IS Show Books Show	PI Performance mark Helg AM - May 18, 2011 2: 1 Jobe Name : QA Probe Type TCP Connect TCP Connect TCP Connect COP Echo Issoen ICMP Echo Issoen ICMP Echo 12 COMP Echo 12 COMP Echo	0:00 AM (Lest 1 be Type : Soi Change o Source Site wennente mountaintoo mountaintoo doucosite doucosite mountaintoo	Hour) Irce Site : De f Round Tr Destination Site douagete mountaintog mountaintog farandaway farandaway mountaintog	Quality Assura stination Site ip Time (msecs) (avg <u>Previous Period</u> From May 18, 2011 12:10:00 AM To: May 18, 2011 1:10:00 AM 79:08 23:62 26:73 28:87 1:17 1:42 39:43	a) Current Period From: May 18, 2011 1:10:00 AM 5:03 27:23 30:27 29:13 1:00 1:25 39:29	Growth Rate (%) -93.64% 15.31% 13.22% 0.92% -14.29% -11.76% -0.36%	Change -74.06 3.62 3.53 0.27 -0.17 -0.17 -0.14
Destination Analysis Incident Summary : R Message Severity Lifecycle State RCA Active Source Object Created/Opened	endnode12 toundTripTimeHigh 3 High round trip time for the QA Probe INTC to endnode12 ping. The reason for this state is, the measured value 207.0 msecs is higher than the upper bound of 100.0 msecs. The date and time for the measurement is 2011-04-14 Highs/27.147. Registered Highs/2014 False NTC to endnode12 ping (Q A Test Table View Data) 4/14/11 06:45 PM (Open for 34.8 days)	Correlation N Category Family Correlation N Origin Last Occurre Source Noble	2 Grieven (Construction) Construction (Construction) Con	NINM IS NINM IS NINM IS Show Books Show Books Show Books NING 10 1000 NING 2 NING 2	PI Performance mark Help AM - Mey 18, 2011 2: 1 Jobe Name : QA Prole Type TCP Connect UDP Echo States TCP Connect CMP Echo LIZO COMP Echo LIZO COMP Echo LIZO COMP Echo LIZO COMP Echo	0:00 AM (Lest 1 be Type : Sou Change o Source Site wannuat mountaintoo mountaintoo mountaintoo doucoasite mountaintoo doucoasite	Hour) Irce Site : De f Round Tr Destination Site douccels doucels douccels douccels douccels dou	Quality Assura stination Site ip Time (msecs) (avg <u>Previous Period</u> From May 18, 2011 12:10:00 AM To: May 18, 2011 11:10:00 AM 79.08 23.62 26.73 28.87 1.17 1.42 39.43 1.00	a) Current Period From: May 18, 2011 1:10:00 AM To: May 18, 2011 2:10:00 AM 5:03 27:23 30:27 29:13 1:00 1:25 39:29 1:00	st Changed Growth Rate (%) -93.64% 15.31% 13.22% 0.92% -14.29% -11.76% 0.36% 0.00%	Change -74.06 3.62 3.53 0.27 -0.17 -0.17 -0.14 0.00

NNM iSPI Network Engineering Toolset Software

NNM iSPI NET extends the powerful network management capabilities of NNMi by providing additional troubleshooting and diagnostic tools.

NNM iSPI NET provides the following functionality:

- SNMP trap analytics that provide summary and detailed information about SNMP trap traffic in the network.
- Trap storm detection at a more granular level than NNMi provides.
- Visio export functionality for storing NNMi topology map data in Microsoft® Visio files.
- Diagnostic flows that provide automatic gathering and analysis of information from network devices, using commands running in the devices over SSH or telnet. Running diagnostic flows when a network outage occurs is helpful for investigating the root-cause.

Figure 8 NNM iSPI NET

🕼 Network Node Manager	т т	Total Traps Received (by Node) at 7:07 AM								
File View Iools Actions Help	'	Total maps Received (by Node) at 7.07 AM								
C Find Node			This report displays the total number of traps received since NNMI was last starled.							
Incident II Q Find Attached Switch PurL.		i otal trap Count eince 5/10/11 4:19 PM (5.6 cays ago): 4,896								
A Topology 🚠 MIB Browser	1	Graph	incoming	trape for these top	6 eourcae.					
Note NM Status		R	efrech th	e current	view, or view anoth	er Trap Analytics Re	eport:			
Status Distribution Graphs		P	Recent Top Trap Rate (by Node)							
NNM Self-Montoring Graphs	▶٩		Re T	ecent Top	Trap Rate (by SNMP Received (by SNMP					
Netv Trap Analytics (iSPI NET only)) Recent Top Trap Rate (by Node)									
NISIO EXPORT (ISPI NET ONLY)	Recent Top Trap Rate (by SNMP OID)		Count	Graph	First Trap Time	Last Trap Time	Trap Source IP	Trap Source Hostname		
Signed in Users	Total Tropa Roocivod (by Nodo)	7	2299		5/10/11 4:19 PM	5/18/11 7 04 AN 5.6 days	172.16.181.6	pm.nto2.hp.com		
Switt 📑 Sign In/Out Audit Log	Total Trape Received (by SNI/P OID)	into	1973	B	5/10/11 4 22 PM	5/16/11 6 53 AN 5.6 daye	16 78 56 35	vwancoder-1 fc usa tip com		
Security Reports			208		5/10/11 4:27 PM	5/16/11 5 24 AN 5.5 days	172.19.1.18	toronto-aw1.ntc2.hp.com		
💕 sandbox	sendbox				5/11/11 11:06 AM	5/15/11 11:40 AM 4 daya	127 0.0.1	localhost.localdomain		
🎁 skiing	Sking			8	5/10/11 4:25 PM	5/16/11 5:10 AN 5.5 days	172.19.1.04	tuva-sw1.ntc2.hp.com		
offices			y		5/11/11 9:57 AM	5/12/11 8 45 PM 1.5 days	16.78.51.254	vail		
iptavaya	Updated: 5/16/11 07:06 47 AN MDT	80	7		5/11/11 9 38 AM	5/13/11 7:18 AN 1.9 days	172 18 30 2	particity		
🐺 Monitoring 🛛 🕹	Analysis		4	ð	5/11/11 10:20 AM	5/12/116.06 PM 1.3 days	172.16.0.2	atcamboat		
P Troubleshcoting ×	Node Summary toronto 😜	Delails	2	8	5/11/11 2:03 PM	5/11/11 0 04 PM 6 hours	16.78.56.28	ntc2ext-gw2.ntc2.hp.com		
Inventory	System Name toronto.ntc2.hp.com	clusions (2	8	5/11/11 10:41 AM	5/11/11 10:56 /M 15.2 minutes	172.10.4.0	aspen		
Management Mode *	Status 📀 Normal Node	e Manege	2	6	5/10/11 8:03 PM	5/11/L1 2 03 PM 10 hours	172.19.1.1	nto2ext gw3.nto2.hp.com		
S Cisco IF Telephony 🛛 😵	Address 172.19.1.20 System Toront System	tem Conti tem Loca	2	6	5/13/11 9 34 AM	5/13/11 10:27 AM 52.5 minutes	172 19 1 254	locodo-gw1 dc2 bp com		
🕼 Nortel IP Telephony 🛛 🕹 😵	Security Group group-L	ice Profile	1	ð	5/10/11 S:03 PM	5/10/11 8 03 PM 0 seconds	16.78.56.1	corc6500-1.ntc2.hp.com		
😽 Avaya IP Telephony 🛛 😵	Incidents Total:17 Opon:7 Las: Hour:0 Last Day 1 FirstFri Mar 11 Last:10:59 AM P Ad	ide caleg iddresses	1	8	5/14/11 2:03 PM	5/14/11 2:03 PM 0 acconda	16.78.56.37	vwansw-1.fe usa.hp.com		
₩ Quality Assurance ¥	Tropa Total:7 Types:1 Mos: Inter	nterfaces (5)	1	8	5/10/11 2:00 PM	5/13/11 2 03 PM	16.70.56.09	wan-bo1-sw.fc.usa.hp.com		
Integration Module Configuration	Nude	e Compo	1		6/12/11 6:48 PM	5/12/11 8 48 PM 0 seconds	172 20.10 3	aspen		

2 Solution Benefits

ANM provides for complete network management using HP Software network management products. Wherever possible, these products automate network management tasks, thereby minimizing the time network engineers must spend on network maintenance.

The ANM products automatically synchronize network device topology and inventory data between the network monitoring (NNMi) and network configuration (NA) systems. This shared information supports launching NA views from the NNMi console in the context of the current object. Device inventory synchronization provides the following benefits:

- Up-to-date and compliant asset management information.
- Rapid device and service deployment to production.
- Discovery of inventory in one tool and synchronization of this information automatically to all other tools.
- Contextual cross-launching into the various ANM user interfaces, saving time and reducing MTTR.
- Common understanding of network inventory and network topology in all operations of the solution.

Single sign-on among the ANM products keeps users focused on the task at hand because they do not need to log on to each product as they move among the ANM consoles.

Many network management scenarios benefit from the use of ANM for end-to-end network management. This chapter describes the following scenarios that show the power of ANM:

- Scenario 1: Identify and correct an out-of-compliance device change on page 18
- Scenario 2: Troubleshoot network fault issues on page 19
- Scenario 3: Re-address IPv4 addresses to the appropriate IPv6 addresses on page 20
- Scenario 4: Troubleshoot application performance problems from a network context on page 21
- Scenario 5: Ensure edge routers maintain expected service levels on page 23
- Scenario 6: Use baseline data to identify abnormal system utilization on page 24
- Scenario 7: Identify and correct error rate and utilization problems on page 25

Scenario 1: Identify and correct an out-of-compliance device change

Incorrect device configuration is a common cause of network problems. ANM can monitor the network for devices with non-compliant configurations and can generate notifications when a device configuration is outside of this expected configuration. ANM provides tools for comparing the current device configuration to the previous device configuration and for resetting the device to use a previous configuration.

Process Without ANM

In this scenario, an unauthorized configuration change is made to a device. With no automated notification of the device configuration change, the network operator must determine that the device is misconfigured. This awareness usually happens only when a problem is encountered or when a manual configuration audit is performed. At this point, the network operator performs the following steps:

- 1 Locate the device and examine the change in the configuration management system.
- 2 Inspect the device configuration, comparing it against documented expectations, and determine that the configuration change is out of compliance.
- 3 Recreate or restore the good configuration to the device.
- 4 Verify that device is correctly configured.

Process with ANM

This scenario uses functionality from the following ANM products:

- NNMi
- NA

ANM can be configured to enable the following process:

- 1 NA receives a syslog event (or another change trigger), captures the new configuration, and automatically runs a compliance check on the new configuration.
- 2 NA sends an SNMP trap that describes the non-compliance to NNMi. NNMi displays this trap in the Open Key Incidents view.
- 3 From the NNMi incident, open the NA Device Configuration Diffs page to see a comparison of the current device configuration with the previous device configuration.
- 4 In NA, run the Deploy to Running Config task to roll back the device configuration.
- 5 NA restores the good configuration to the device and captures the new configuration. Then, NA automatically checks for compliance against the new configuration.

Benefits

In this scenario, ANM provides the following benefits:

- More efficient operations.
- Automatic change detection.
- Automatic compliance checking.
- Configuration and compliance awareness in single incident view, which reduces MTTR.
- Increased security and service availability, which increases ROI.

Scenario 2: Troubleshoot network fault issues

When a device fault occurs, it is helpful to gather information about the device at the time of the fault. ANM can query a device automatically and provides tools for responding to device fault incidents.

Process Without ANM

In this scenario, the ACL configuration on a router blocks traffic with a destination address of 224.0.0.5. Because OSPF depends on this address to broadcast hello packets, the router cannot establish adjacency with the neighboring router. With no automation, the network operator responds to a network fault incident with a thorough diagnostic procedure that includes connecting directly to the router to investigate and update the configuration. The process is similar to the following steps:

- 1 Categorize the network fault incident.
- 2 Log on to the router to run a diagnostic that identifies the cause of the incident.
- 3 On the router, update the configuration.
- 4 On the router, visually inspect the configuration to verify that it is correct.

Process with ANM

This scenario uses functionality from the following ANM products:

- NNMi
- NA

ANM can be configured to enable the following process:

- 1 NNMi determines that an OSPF neighbor state has changed and generates an OSPFNbrStateChange incident for that router. This incident triggers NA to gather information about the router.
- 2 NA runs a show neighbor device diagnostic to determine the OSPF neighbors of the router and then stores the task ID of the diagnostic as an attribute of the NNMi OSPFNbrStateChange incident.
- 3 From the NNMi incident, open the diagnostic report and determine that the OSPF adjacency is stuck in the INIT state.

- 4 In NA, view the diagnostic report of the OSPF neighbor router and observe the ACL configuration error.
- 5 In NA, modify the ACL of the OSPF neighbor router to permit hello packets.
- ⁶ To prevent this problem from recurring, create an NA device policy that the problem ACL is not permitted on this device or any other relevant device. Violations of this policy are handled by Scenario 1: Identify and correct an out-of-compliance device change.

Benefits

In this scenario, ANM provides the following benefits:

- Configuration data available at the point of need.
- More efficient operations.
- Reduced network downtime.
- Fewer network performance issues.
- Increased security and service availability, which increases ROI.

Scenario 3: Re-address IPv4 addresses to the appropriate IPv6 addresses

When completed manually, the process of re-addressing an IPv4 network to use IPv6 addresses is time-consuming and error prone. ANM can automate both the collection of current IPv4 addresses in use and the setting of IPv6 addresses on managed devices.

Process Without ANM

In this scenario, a network engineer manually collects IPv4 information from each device and then manually configures each interface with an IPv6 address. The process is similar to the following steps:

- 1 Determine the current IPv4 addresses of each device:
 - a Log on to the device.
 - b Determine and record the IP address of each interface in a spreadsheet file.
- 2 In the spreadsheet file, map each IPv4 address to an IPv6 address.
- 3 Configure each device with IPv6 addresses:
 - a Log on to the device.
 - b Referring to the spreadsheet file, configure the correct IPv6 address on each interface.
 - c Visually inspect the configuration to verify that it is correct.

Process with ANM

This scenario uses functionality from the following ANM products:

- NNMi
- NA

ANM can be configured to enable the following process:

- 1 In the NNMi console, filter the IP Addresses inventory view to show only the area of the network to be re-addressed, and then export that list to comma-separated values (CSV) format.
- 2 With the CSV file open in a spreadsheet application, map each IPv4 address to an IPv6 address, and then save the spreadsheet file in CSV format.
- 3 Create a script that configures the new IPv6 addresses.
- 4 In the NA console, assign a scheduled task to run the script against the appropriate devices at the appropriate time.

Benefits

In this scenario, ANM provides the following benefits:

- Automation of the data collection and configuration processes.
- Reduced risk of re-addressing errors.

Scenario 4: Troubleshoot application performance problems from a network context

Unexpected network traffic across important network interfaces is a common cause of application performance problems. ANM can monitor the utilization of important interfaces and can generate notifications when that utilization is beyond the acceptable level. ANM provides tools for updating the device configuration to block unauthorized traffic on important interfaces.

Process Without ANM

In this scenario, unauthorized traffic consumes so much bandwidth across a network interface that the application using that interface experiences delayed response times. With no automated notification of the increased traffic, the network operator is usually unaware of the increased traffic until an application user submits a complaint against the application. At this point, the network operator performs the following steps:

- 1 Determine which communication paths and servers the application uses.
- 2 Run traceroute to determine the routed infrastructure for the application traffic.

- 3 Study each router in the routed infrastructure:
 - a Log on to the router.
 - **b** Examine the routing table to identify the interfaces associated with the application path.
 - c Gather performance metrics for the router as a whole and for the individual interfaces involved in the application path.
- 4 Gather traffic metrics from sniffer or probe tools deployed on the application path. Examine this data to determine which abnormal or unauthorized traffic is interfering with target application traffic across over-utilized routers.
- 5 Log on to the appropriate network devices to block unauthorized traffic or to reroute the application traffic through alternate, less utilized routes.

Process with ANM

This scenario uses functionality from the following ANM products:

- NNMi
- NA
- NNM iSPI Performance for Metrics
- NNM iSPI Performance for Traffic

ANM can be configured to enable the following process:

- 1 NNMi generates a management event incident to indicate that interface utilization is beyond acceptable boundaries for an important network interface.
- 2 View the NNM iSPI Performance for Traffic Interface Traffic 1 Minute Top Applications report for the volume - In Bytes and Volume-Out Bytes metrics grouped by source host name, destination host name, and application name. This report reveals competing traffic from an unauthorized application.
- 3 In the NA console, run a Batch Insert ACL Line task to modify multiple ACLs to multiple devices to block unauthorized traffic.
- 4 Network traffic across the interface returns to acceptable levels, and the interface utilization incident automatically closes in the NNMi console.

Benefits

In this scenario, ANM provides the following benefits:

- Proactive management of network utilization issues for increased service levels on mission critical applications.
- One set of tools for detecting, troubleshooting, and fixing the cause of network utilization issues, which reduces MTTR.
- Proactive remediation of network configuration issues that affect critical services across the entire network.
- Automated collection of performance and traffic data.
- Detection and blocking of unauthorized traffic.

Scenario 5: Ensure edge routers maintain expected service levels

From a network management point of view, it is important to keep servers available to all users. From a business management point of view, it is important to receive the level of service purchased from an Internet service provider (ISP). ANM can monitor the responsiveness of devices that are outside of the company's network and can generate notifications when responsiveness goes below acceptable levels.

Process Without ANM

In this scenario, something within the ISP's network degrades the effectiveness of an edge router that carries application traffic to the Internet. With no automated notification of the reduced edge router performance, the network operator is usually unaware of the problem until an application user submits a complaint against the application. At this point, the network operator performs the following steps:

- 1 Determine which communication paths and servers the application uses.
- 2 Troubleshoot the communication and application paths to isolate the problem to the edge router.
- 3 Notify the ISP of the problem.

Process with ANM

This scenario uses functionality from the following ANM products:

- NNMi
- NNM iSPI Performance for QA

ANM can be configured to enable the following process:

- 1 NNMi generates a management event incident to indicate that a particular metric of an IP SLA test from the edge router is beyond acceptable boundaries.
- 2 Notify the ISP of the problem.

Benefits

In this scenario, ANM provides the following benefits:

- Assurance that the network adheres to all SLAs necessary to support critical applications.
- Effective monitoring of the ISP to ensure delivery of contracted services.

Scenario 6: Use baseline data to identify abnormal system utilization

Irregular traffic patterns can signal inappropriate use of the network. ANM can determine normal traffic patterns and can generate notifications when traffic patterns are outside the normal range.

Process Without ANM

In this scenario, company customers complain about the slowness in accessing the company's main web site across the Internet. At this point, the network operator performs the following steps:

- 1 Examine the network utilization of the web servers and the outside router to observe high utilization.
- 2 Use sniffers, run performance tools, and examine firewall logs to determine the source of the slowness.
- 3 Determine that the web site URL is being loaded with many HTTP requests. The requests seem to be an attack on the web site.
- 4 Close all connections to the web site, which brings the web site completely down.
- 5 Contact security specialists for assistance with the situation.

Process with ANM

This scenario uses functionality from the following ANM products:

- NNMi
- NA
- NNM iSPI Performance for Metrics
- NNM iSPI Performance for Traffic

ANM can be configured to enable the following process:

- 1 NNMi generates a management event incident to indicate a deviation from normal behavior with regards to utilization on the interfaces involved in the path to the web site.
- 2 View the NNM iSPI Performance for Traffic Conversations for Applications Top N report for the interface identified in the incident to determine which traffic is affected, including sources and destinations.
- 3 Determine that the web site URL is being loaded with many HTTP requests. The requests seem to be an attack on the web site.
- 4 In the NA console, modify the ACLs on the device hosting the web server to deny traffic from the sources of the attack.
- 5 Network traffic across the interface returns to acceptable levels, and the interface utilization incident automatically closes in the NNMi console.

Benefits

In this scenario, ANM provides the following benefits:

- Proactive management of network utilization issues for increased customer satisfaction.
- One set of tools for detecting, troubleshooting, and fixing the cause of network utilization issues, which reduces MTTR.
- Detection and blocking of unauthorized traffic.
- High quality service delivery.

Scenario 7: Identify and correct error rate and utilization problems

A high error rate on an interface usually causes the workstation, server, or any other device connected to that interface to work significantly slower. ANM can monitor interfaces and generate notifications when the error rate, or utilization, or both crosses pre-defined thresholds.

Process Without ANM

In this scenario, a critical application responds slowly and eventually times out, but the problem clears on its own. Because this failure happens intermittently during peak usage periods, the application is moved to a more powerful server. This change does not prevent the application from timing out. Eventually a duplex mismatch is discovered. Correcting the duplex configuration resolves the timeout issue.

Process with ANM

This scenario uses functionality from the following ANM products:

- NNMi
- NA
- NNM iSPI Performance for Metrics

ANM can be configured to enable the following process:

- 1 NNMi generates a management event incident to indicate a high error rate on an interface. The connection table on the incident details tab indicates a duplex mismatch.
- 2 From the NNMi console, open the device configuration difference page for the router on each end of the connection to see which duplex is configured on this interface and to check if the device configuration has been changed recently.
- ³ Open an NNM iSPI Performance for Metrics interface health report for the LAN collision rate and LAN collision count metrics grouped by qualified interface name. Also open an NNM iSPI Performance for Metrics interface health report for the LAN FCS error rate and LAN FCS error count metrics grouped by qualified interface name. This combination of reports shows one side of the connection with high errors while the other side has high collisions. This information is indicative of duplex mismatch.

- 4 From NA, update the switch configuration.
- 5 Check the interface performance history in the NNM iSPI Performance for Metrics reports to verify that the error problem no longer occurs.

Benefits

In this scenario, ANM provides the following benefits:

- Proactive detection of network configuration errors before they impact application performance.
- One set of tools for detecting, troubleshooting, and fixing the cause of network utilization issues, which reduces MTTR.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click *here*.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to **ovdoc-nsm@hp.com**.

Product name and version: $ANM\ 9.10$

Document title: *ANM Concepts Guide*

Feedback: