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

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

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.

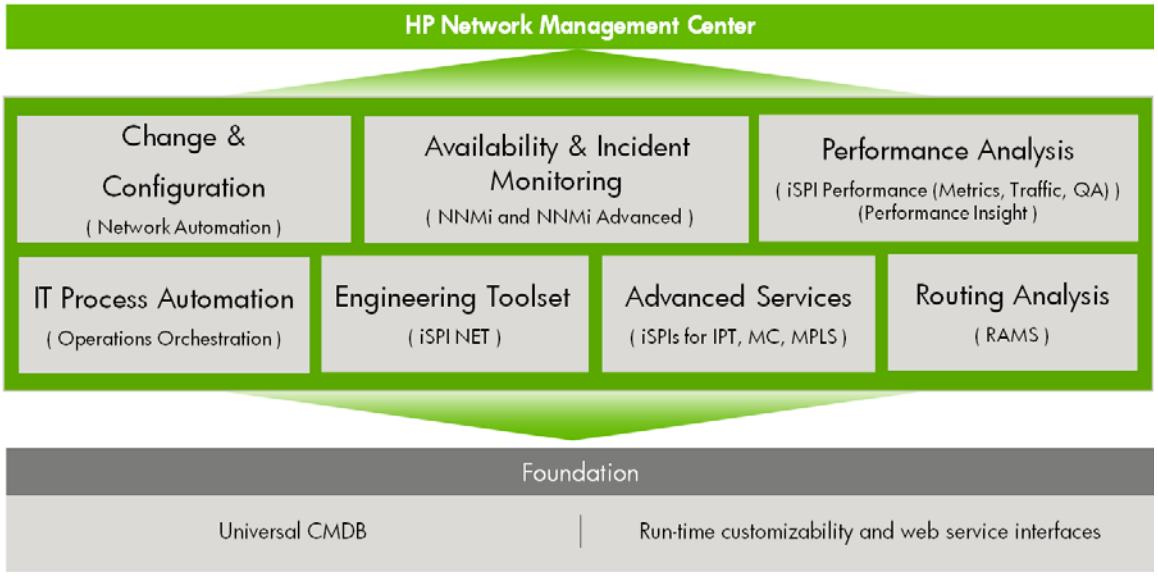
- **Change and Configuration Management and Compliance:** Everyday tasks such as changing the configuration on devices (as a result of problems or other infrastructure changes) and adding new devices to the network can consume a lot of time. When these tasks are performed manually on a large number of 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

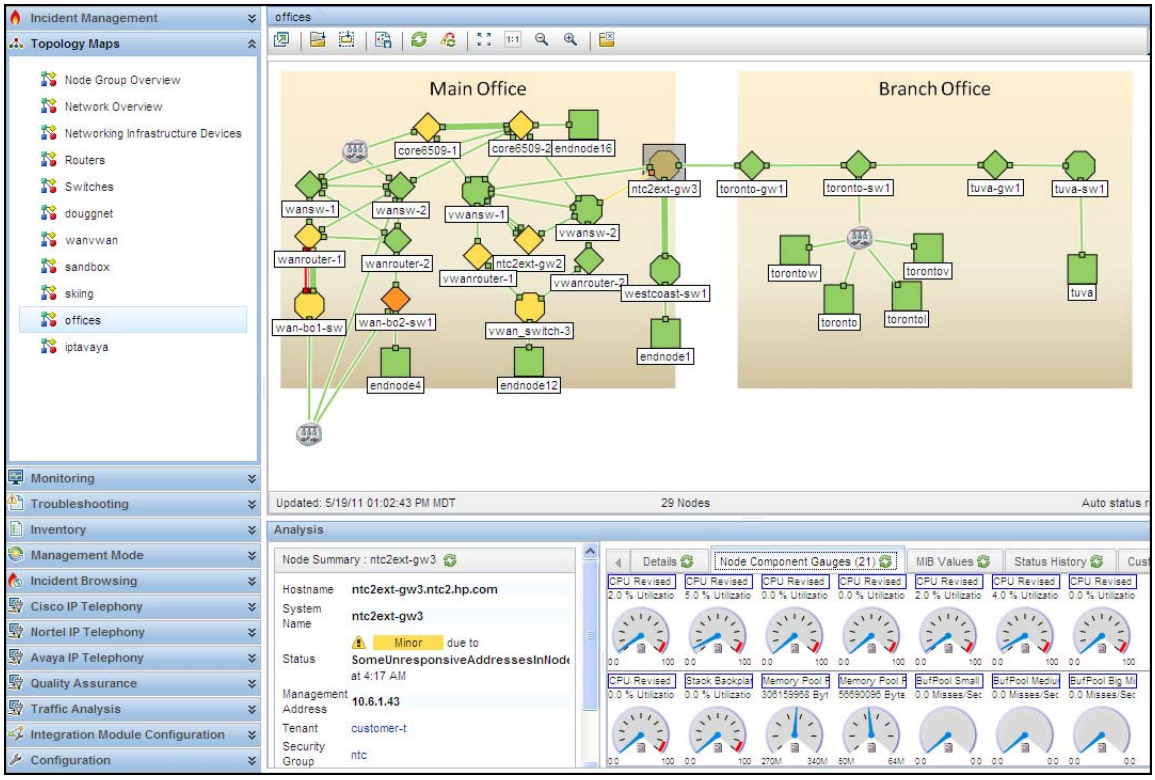
NNMi provides smart network fault and availability monitoring using common network protocols such as SNMP and ICMP to help you maintain a healthy network across your organization. NNMi can discover network nodes (such as switches and routers) on an automatic and continuing basis, providing an up-to-date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

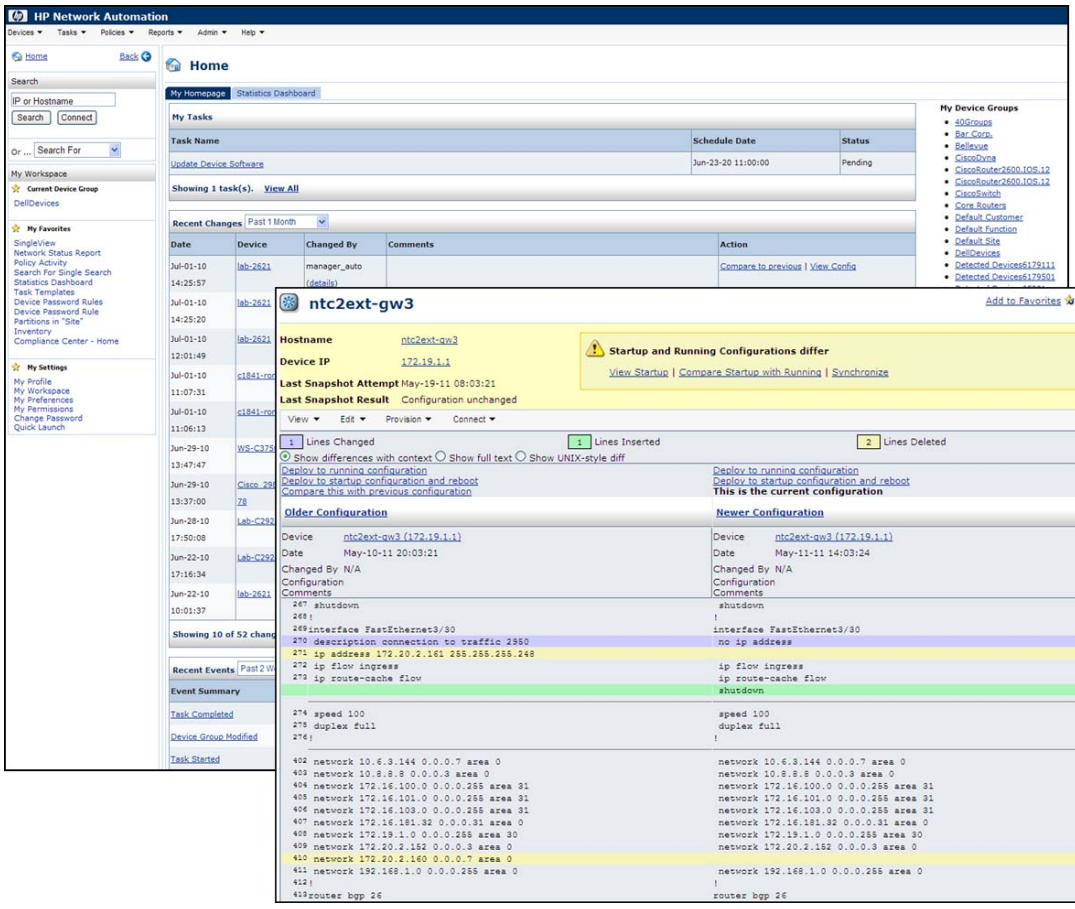
NA is an enterprise-class network device change and configuration management tool. It eliminates human error in device configuration changes while also maintaining compliance standards through a policy-based change management model. NA maintains a complete audit trail of all device changes, including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



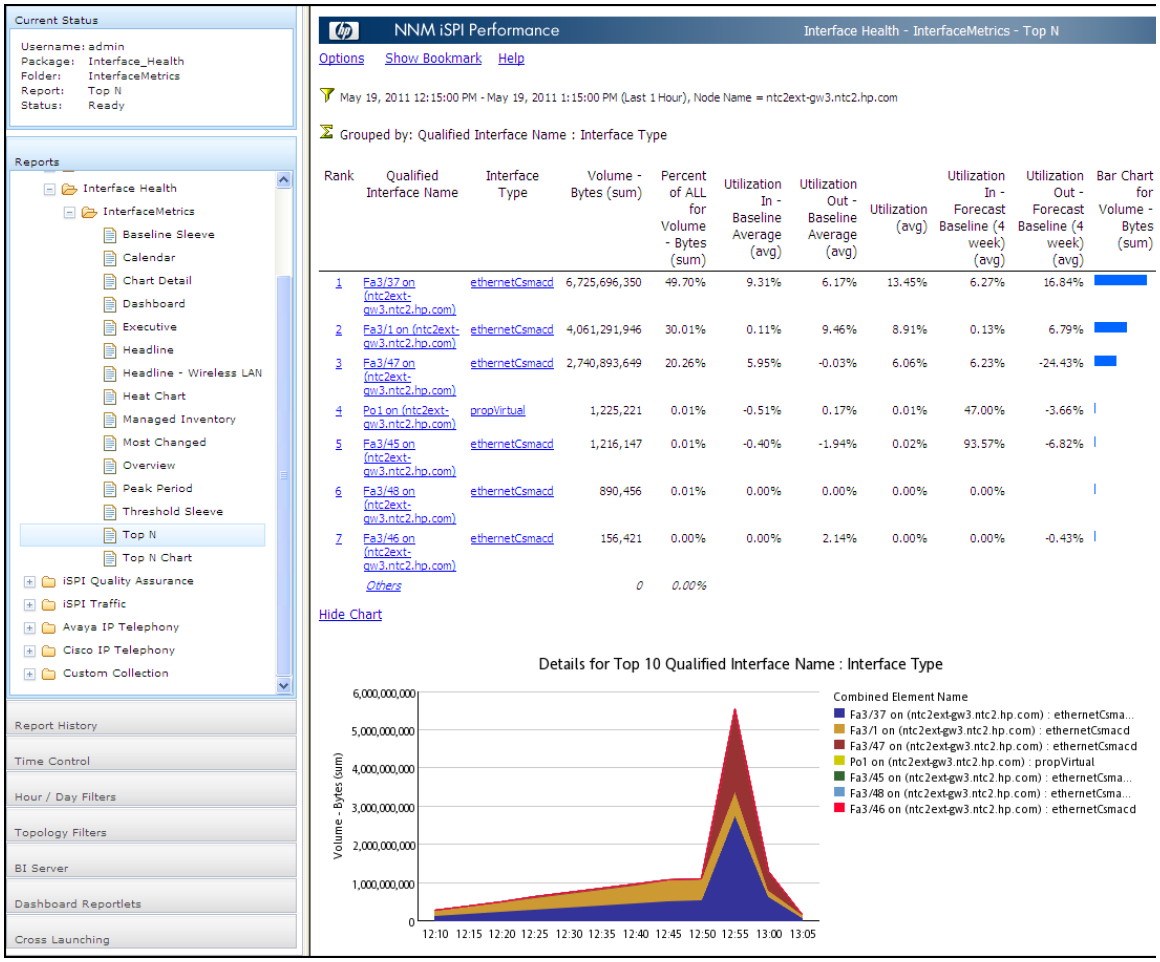
HP Network Node Manager iSPI Performance for Metrics Software

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



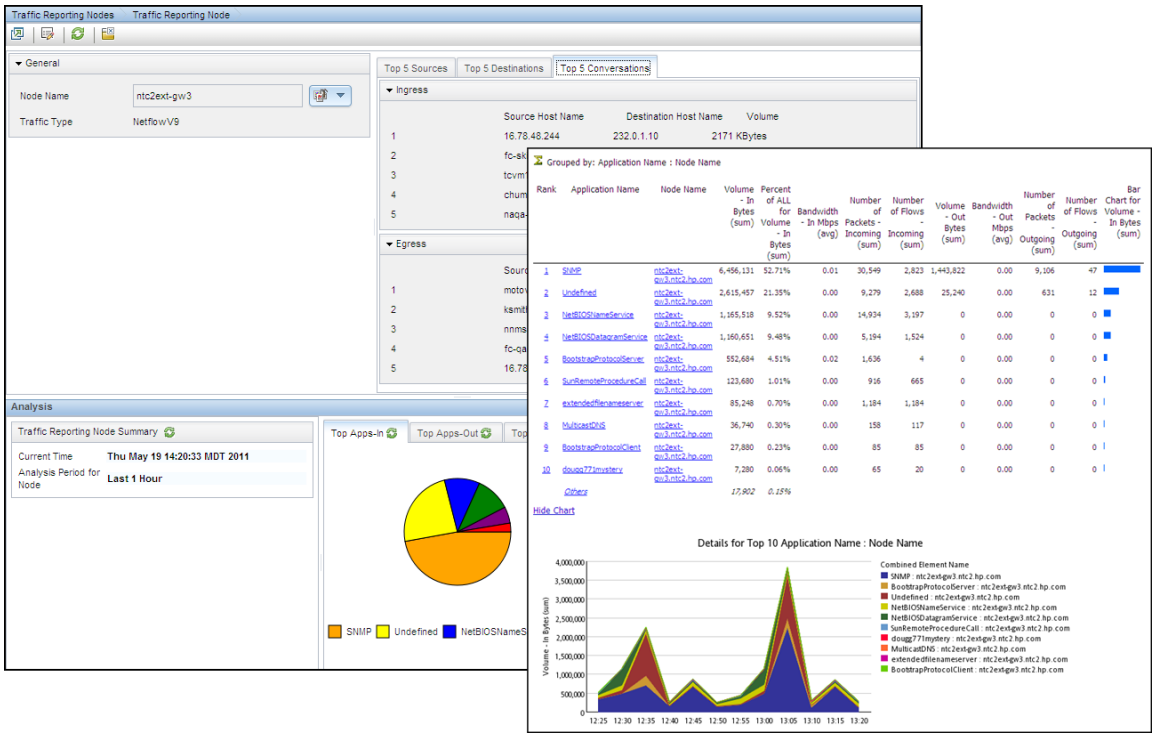
HP Network Node Manager iSPI Performance for Traffic Software

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



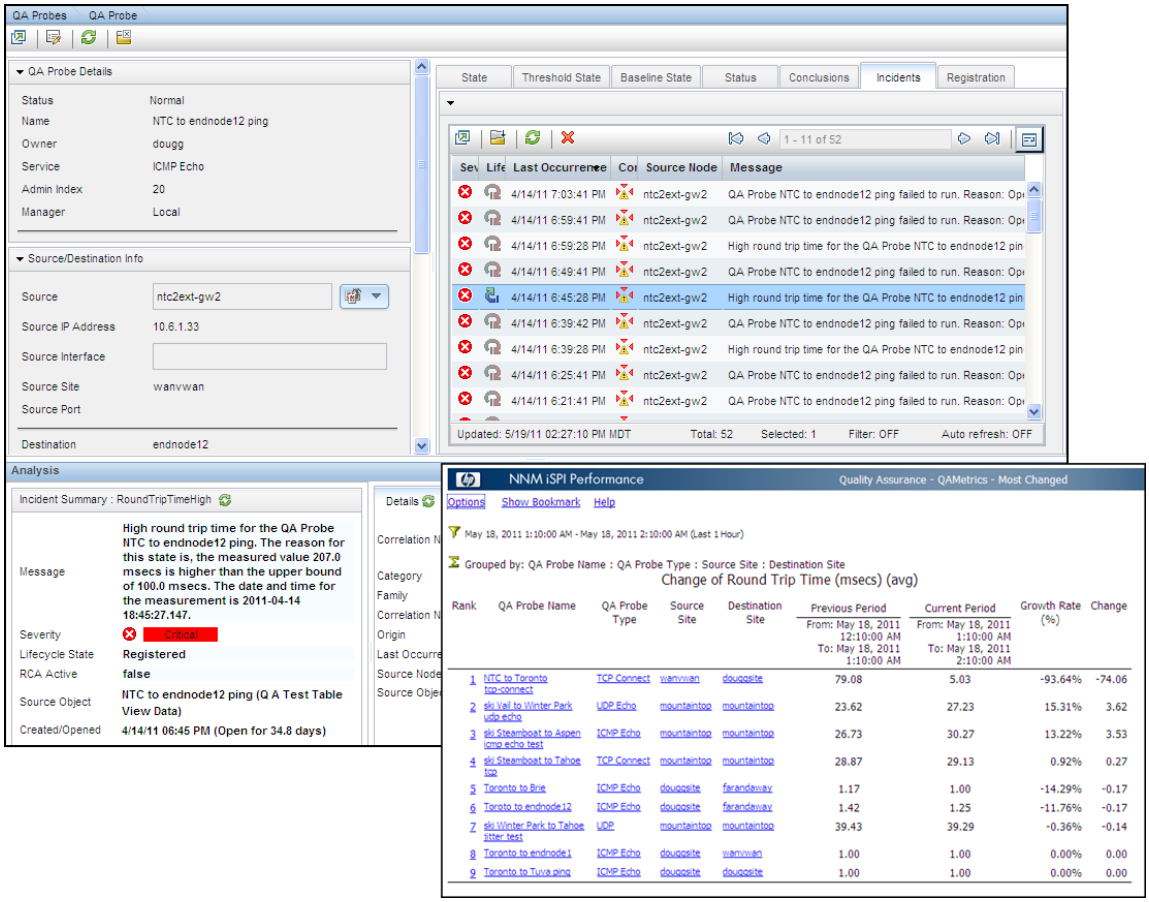
HP Network Node Manager iSPI Performance for Quality Assurance Software

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



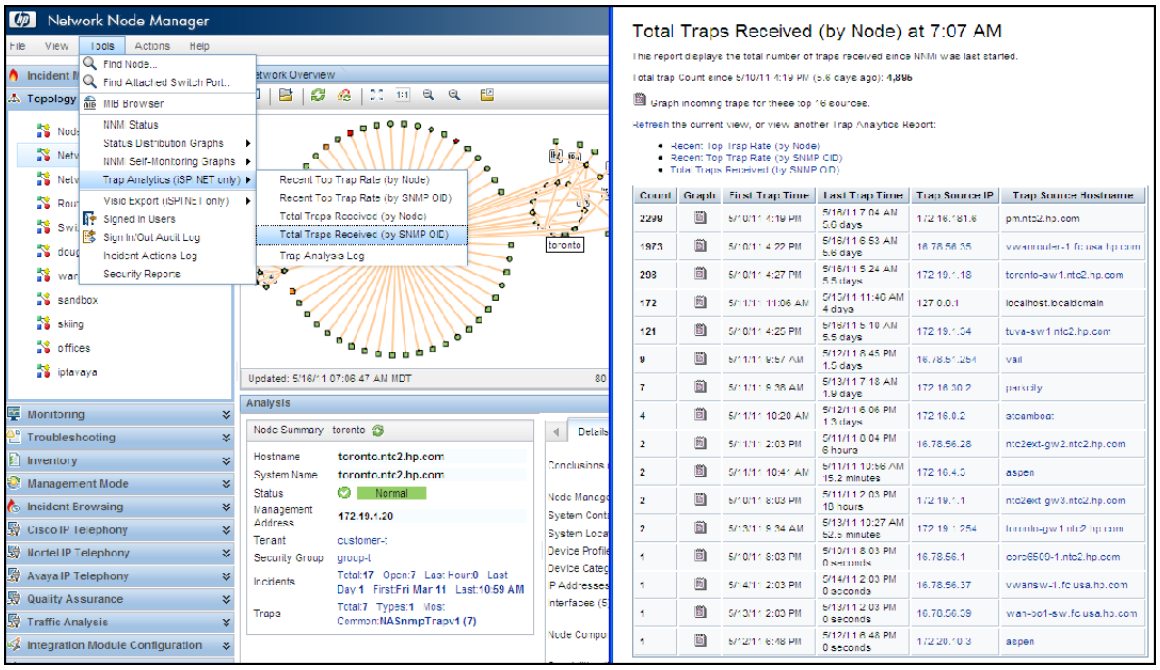
NNM iSPI Network Engineering Toolset Software

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



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

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: