Automated Network Management Solution (ANM)

HP Network Node Manager i, iSPIs for Performance, NET iSPI, and HP Network Automation

Solution Version: 9.0

Solution Concept Guide

Document Release Date: May 2010
Software Release Date: May 2010

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 Notices

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel®, Pentium®, and Intel® Xeon™ are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows NT®, and Windows® XP are U.S registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

Acknowledgements

- This product includes software developed by Apache Software Foundation (http://www.apache.org/licenses).
- This product includes OpenLDAP code from OpenLDAP Foundation (http://www.openldap.org/foundation/).

- This product includes GNU code from Free Software Foundation, Inc. (http://www.fsf.org/).
- This product includes JiBX code from Dennis M. Sosnoski.
- This product includes the XPP3 XMLPull parser included in the distribution and used throughout JiBX, from Extreme! Lab, Indiana University.
- This product includes the Office Look and Feels License from Robert Futrell (http://sourceforge.net/projects/officelnfs).
- This product includes JEP - Java Expression Parser code from Netaphor Software, Inc. (http://www.netaphor.com/home.asp).

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 web site at:

http://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 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

Table of Contents

Welcome to This Guide

This guide provides general information about the Automated Network Management Solution (ANM)—what the solution can accomplish and for whom.

This chapter includes:

How This Guide Is Organized

This guide contains the following chapters:

Chapter 1 Introduction to ANM

Provides a brief description of the Automated Network Management (ANM) Solution and illustrates a typical deployment.

Chapter 2 ANM Customer Scenarios

Provides sample customer scenarios implementing the ANM Solution capabilities. This section demonstrates what you can achieve with this solution.

Who Should Read This Guide

This guide explains the motivation to install and use the ANM Solution. It describes what the solution implementation will achieve, which ITIL processes it will answer, and describes the workflow between the products comprising the solution.

This guide is intended for:

- Customers
- Presales and sales personnel
- PSO
- Anyone who wants to learn about the solution, its workflow, and its contribution

The information in this guide may duplicate information available in other ANM documentation, but is provided here for convenience.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

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

To register for an HP Passport user ID, go to:

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

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

1

Introduction to ANM

This chapter includes:

Concepts

References

Note: If you have any feedback or comments about this document, please contact solutionpackagingandscp@hp.com.

Concepts

ANM – Overview

Automated Network Management (ANM) is a solution that integrates network fault detection, performance monitoring, configuration management and compliance, as well as incorporating the diagnostic and automation tools. It 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 Failure (MTBF),
- become policy compliant,
- reduce Mean Time to Change network configuration,
- and increase the SLA with faster ROI.

The ANM Solution is comprised of six individual, but integrated products that are brought together in the HP Network Management Center. The products that comprise the ANM Solution are:

- HP Network Node Manager i 9.0
- HP Network Automation 7.6
- HP Network Node Manager iSPI Performance for Metrics 9.0
- HP Network Node Manager iSPI Performance for Traffic 9.0
- HP Network Node Manager iSPI Performance for Quality Assurance 9.0
- HP Network Node Manager iSPI Network Engineering Toolset 9.0

In the following chapter, you will find examples that illustrate common scenarios for personas responsible for Network Operations / Engineering. These personas require the solution to provide the following capabilities for efficient management of their network:

- Network Change and Configuration Management,
- Network Performance Management,
- Network Fault Management,
- Network Run-Book Automation,
- and Network Diagnostics.

Using these capabilities, the following high level generic actions can be completed by the user:

- 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

Note: The Smart Plug-ins (SPIs) provide valuable insight into the current health and ongoing trends in your network, allowing you to increase availability and performance, while lowering associated support costs and improving capacity management and planning.

Network Management Concepts

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

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

- **Availability and Incident Management:** One of the basic needs of a Network Engineer is knowing if there is a network outage occurring on their network, along with the ability to recognize the root cause of the outage. Network Engineers need to know if the source of the root cause is hardware failure or any other environmental reason. They need this information as soon as possible.

  Network Engineers also like to have the ability to see their network diagram as it is in reality, who is connected to whom, and which devices exist on their network.

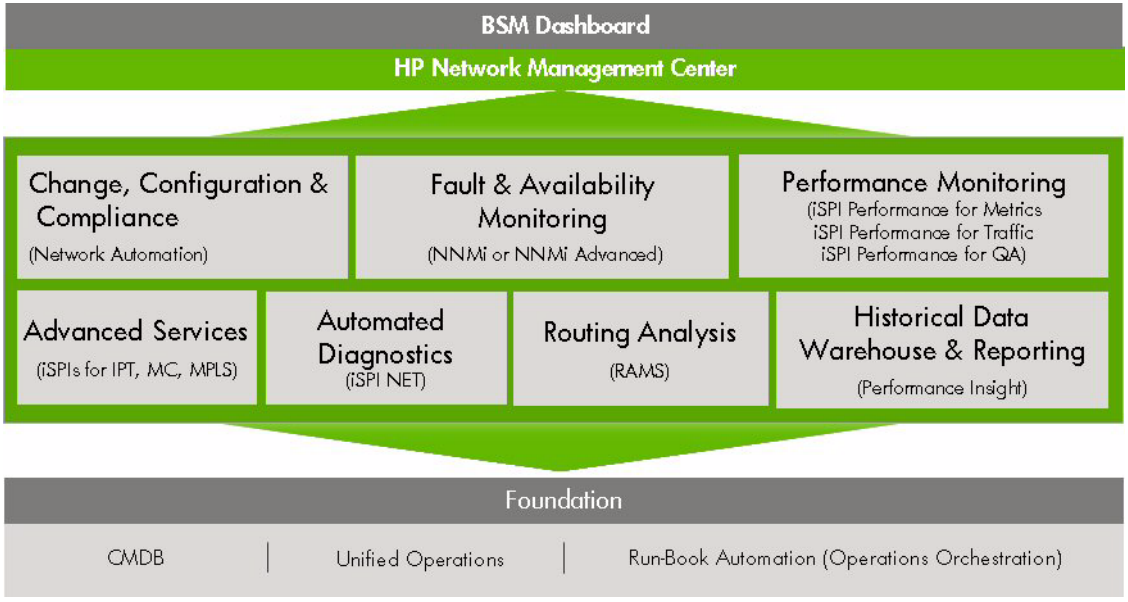
- **Performance Analysis:** Most of the problems that Network Engineers encounter are problems where no outage is occurring, but the customer still complains that the service level they receive from the network is poor—even affecting the business QoS. In this scenario, the Network Engineers will have more advanced needs for troubleshooting the incident. They will need to have a tool that will help them analyze what the root cause is of this behavior—a tool that will show them basic real-time and historical performance data (for comparison purposes), such as Utilization and Errors, and show them an IP traffic analysis examining if the source of the problem is an application that overloads the network. This tool needs to show them IPSLA information so they will be able to see if the QoS polices were configured correctly.

- **Change and Configuration Management and Compliance:** When managing a large network is your responsibility, such as the Network Engineer, everyday tasks that consume most of your time are tasks such as changing the configuration on devices as a result of problems or other infrastructure changes, adding a new device to the network, and so on. While performing these tasks on a large number of devices, you or your colleagues can make mistakes and perform changes incorrectly which can result, in a worst case scenario, in an outage.

  Another need for the Network Engineer is to make sure that all configurations were made according to their instructions, and to have an archive of those configurations. These needs are very common for any Network Engineer who is responsible for many network devices.

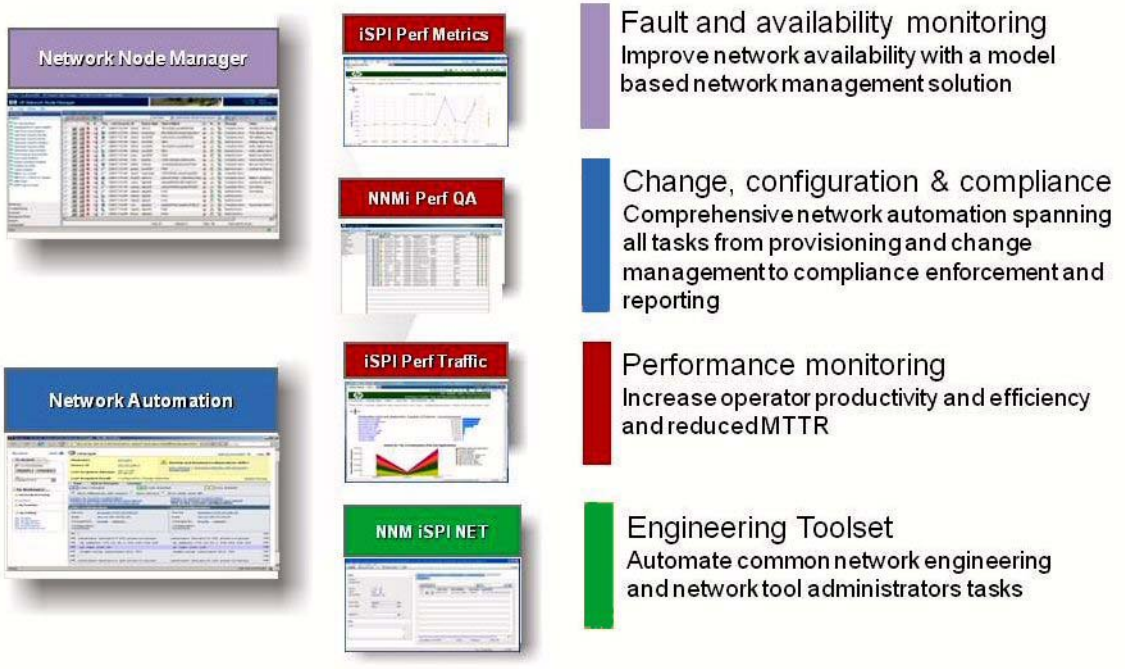
The following section will explain how the ANM Solution can provide Network Engineers with the ability to handle all of these needs with easy-to-use products that can make their day-to-day work easier and much more efficient.

The following diagram displays which HP Network Management Center products can fulfill the needs described in this chapter. The next chapter elaborates on how the ANM solution products that are part of this center fulfill those needs.



ANM Solution Product Relationships

HP Automated Network Management enables customers to reduce costs and increase agility by unifying automation across all network operations. Unlike point product approaches, HP offers an integrated solution portfolio that automates event, performance, change and configuration management, plus automated IT process automation.



HP Network Node Manager i Software (NNMi)

HP Network Node Manager i Software (NNMi) contains a toolset to help you maintain a healthy network across your organization. NNMi provides smart network fault and availability monitoring using common network protocols like SNMP and ICMP. NNMi can discover network nodes (such as switches and routers) on an ongoing basis, providing an up-to-date representation of the network topology (Layers 2 and 3).

As NNMi maintains an accurate picture of the network, it also helps you handle problems through management by exception—the ability to pinpoint network problems by using event correlation and root cause analysis (RCA), and locating device-attached nodes. Unlike other network management software, NNMi applies sophisticated RCA algorithms to an accurate, ever-changing view of network topology to support dynamic fault management.

NNMi also allows you to monitor your device's health in terms of power and temperature (according to the support matrix) and view live performance graphs.

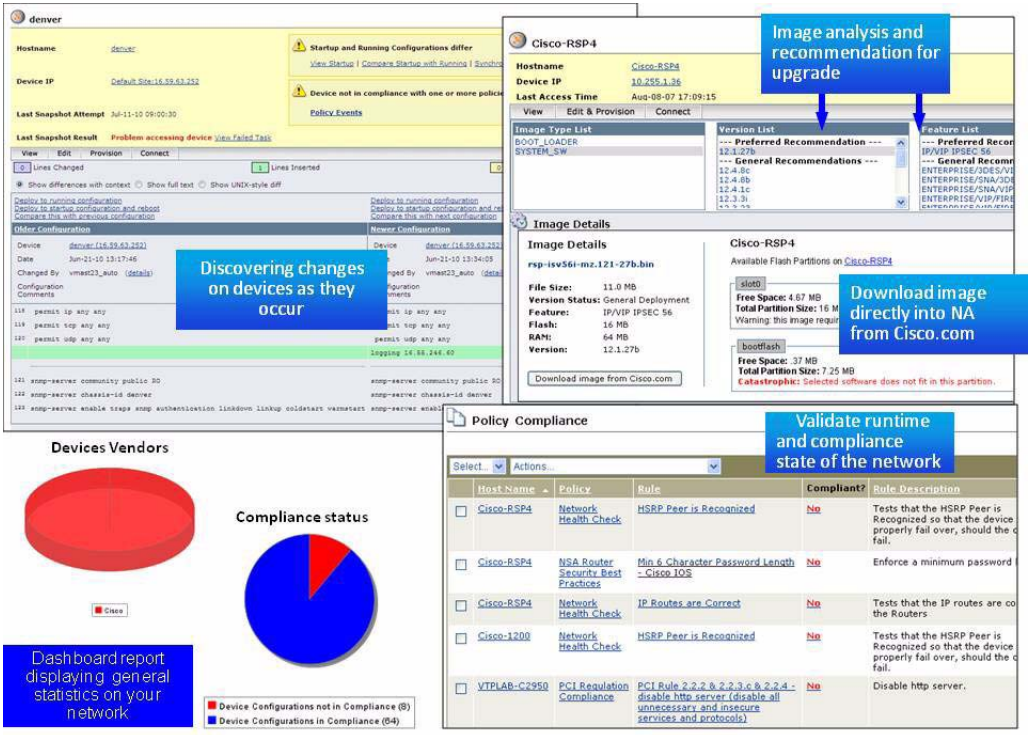
NNMi is the center of this solution from an operational point of view. From its GUI, you can access each of the other products in the solution.

HP Network Automation (NA)

HP Network Automation (NA) provides an enterprise class solution that tracks and regulates configuration and software changes across routers, switches, firewalls, load balancers, and wireless access points. NA provides visibility into network changes, enabling IT staff to identify and correct trends that could lead to problems, while mitigating compliance issues, security hazards, and disaster recovery risks. NA also captures full audit trail information about each device change.

NA supports more than 500 device types and models from the major vendors in the market; such as Cisco, Nortel, Juniper, HP and 3Com, F5, Alcatel–Lucent, Extreme, plus more.

NA lets Network Engineers know what changes have been made to network devices, who applied them, what the current configuration is, if the configuration complies with organizational standards, and also minimizes MTTR using configuration archiving and deployment.



HP Network Node Manager iSPI Performance for Quality Assurance (QA iSPI)

HP Network Node Manager iSPI Performance for Quality Assurance (QA iSPI) extends the capability of NNMi to monitor the quality of traffic flow in the network. QA iSPI collects data (using SNMP) from pre-configured QA probes on the selected network elements and gives the Network Engineers the ability to monitor these probes, display the service level data on site-to-site orientation, and also configure thresholds on the data collected by these probes. By connecting this iSPI to the Network Performance Server (part of the iSPI Performance for Metrics), Network Engineers can analyze the collected data through graphs and charts.

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

- Discover the pre-configured QA probes defined for various network elements
- Monitors the QA probes' status and their test results
- Display the QA probe results on the NNM iSPI Performance for QA views

HP Network Node Manager i Software Smart Plug-in Performance for Metrics (Metrics iSPI)

HP Network Node Manager i Software Smart Plug-in Performance for Metrics (Metrics iSPI) provides the core performance management capability to NNMi by gathering and monitoring the metric data polled by NNMi from different network elements. With the combination of NNMi and the iSPI Performance for Metrics, you can monitor the operational performance of the network infrastructure by collecting data on the main and common performance metrics; such as Error Rate, Interface Utilization, CPU, Memory Utilization, and more.

The main capabilities of the Metrics iSPI are:

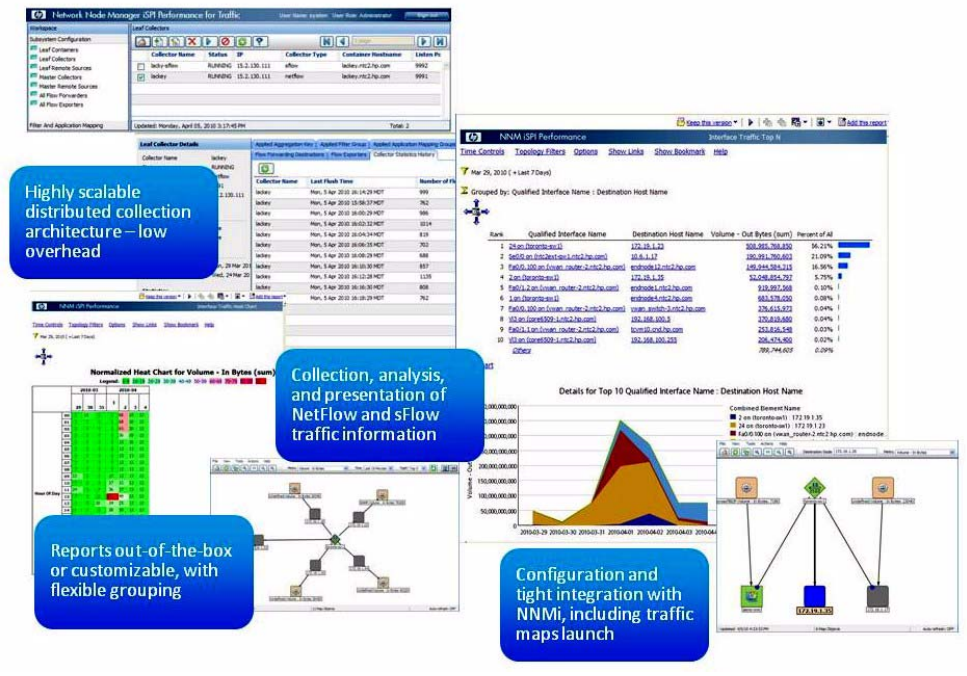
- Historical graphs of performance data
- Performance threshold monitoring
- Performance review on a network path between two devices (E2E)

HP Network Node Manager iSPI Performance for Traffic (Traffic iSPI)

HP Network Node Manager iSPI Performance for Traffic (Traffic iSPI) extends the capability of NNMi to monitor the performance of the network. By collecting IP flow records that are exported by the routers, NNM iSPI for Traffic enriches the data available for the Network Engineers to analyze common network performance. For example, it enables you to understand why your 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 performance reports by exporting data to the Network Performance Server (NPS)
- Generates maps to view the traffic flow information on your network.



HP NNM iSPI Network Engineering Toolset (NET iSPI)

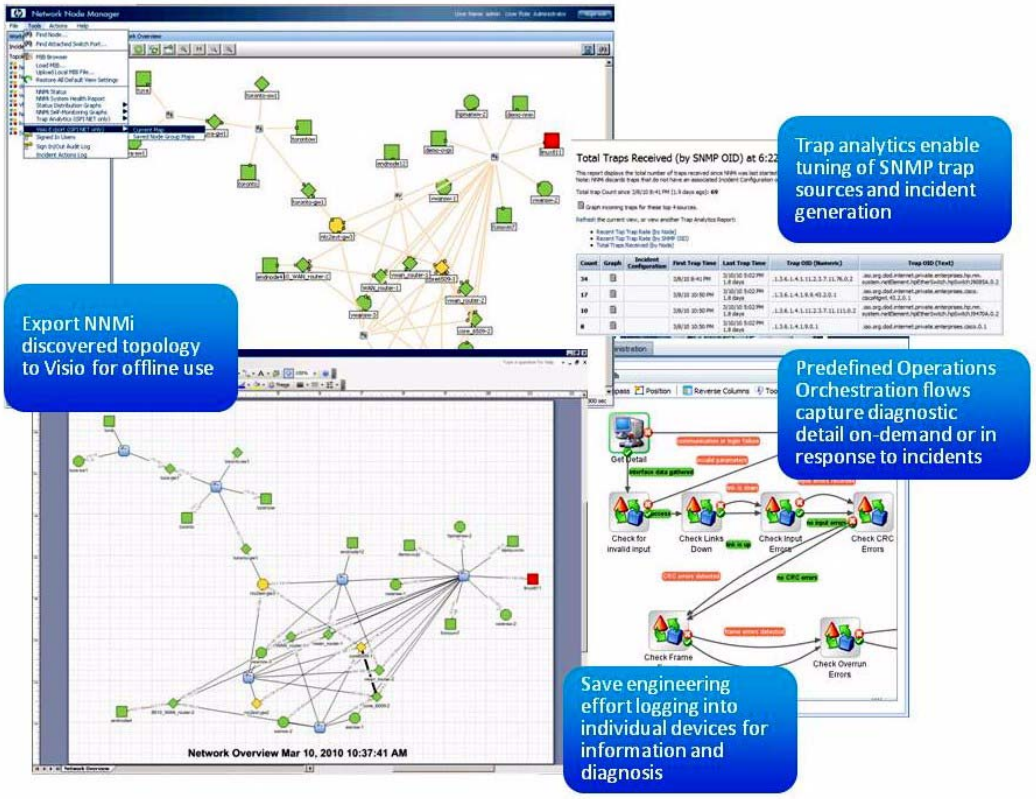
HP NNM iSPI Network Engineering Toolset (NET iSPI) extends the powerful network management capabilities of NNMi by providing additional troubleshooting and diagnostic tools for Network Engineers.

NNM NET iSPI provides the following functionality:

- SNMP trap analytics provide summary and detailed information about SNMP trap traffic in the network.
- Visio export functionality exports NNMi topology map data to Microsoft Visio files.
- Diagnostic flows 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 very helpful for troubleshooting—even investigating the root-cause afterwards.

The NNM NET iSPI diagnostic flows and diagnostics server, which must be installed separately from NNMi (on the NNMi management server or on a separate computer) provide the following:

- The diagnostic flows automatically gather diagnostic information when NNMi detects certain network incidents.
- The diagnostics server is an embedded packaging of HP Operations Orchestration (HP OO). If you already have the full HP OO product, you can install the NNM NET iSPI diagnostic flows on that server.



Personas

ANM Solution outcomes and uses are designed to feed the needs of the following personas in the organization:

- **Operator:** Responsible for monitoring the operation of the network infrastructure. This persona triages and troubleshoots incidents related to the network infrastructure, along with other infrastructure incidents.
- **Network Engineer:** Responsible for designing and managing the network of the organization, and also providing for second level support of network problems. This persona is usually the highest authority for deciding about large network changes.
- **Network Technician:** Responsible for the first level of support for network problems, plus implementing approved network changes.

Reference

Terms and Definitions

NA

HP Network Automation

NNMi

HP Network Node Manager i

NNMi Advanced

HP Network Node Manager i Advanced

RAMS

HP Route Analytics Management System

iSPI NET

Smart Plug-In Network Engineering Tool

iSPI Perf

Smart Plug-In for Performance

OO

HP Operations Orchestration

ITIL

Information Technology Infrastructure Library: A collection of volumes intended to assist and promote effective and efficient IT Service Management practices in organizations.

SM

HP Service Manager

2

ANM Customer Scenarios

The scenarios described in this chapter are an illustration of what you can accomplish with the Automated Network Management (ANM) Solution.

These scenarios also demonstrate how the solution products help you implement two ITILv3 service life cycles —Service Transition and Service Operation— which can result in higher SLA and faster ROI.

Concepts

➤ ANM Use Case Overview on page 23

Tasks

➤ ANM Use Cases on page 24

Concepts

ANM Use Case Overview

The ANM Solution provides for all the needs of network management using the network management products of HP Software. This is accomplished in an automated fashion wherever possible, thus minimizing the Network Manager's time spent on network maintenance.

In the following sections, specific customer scenarios, or key examples of common actions, are provided in order to show the effectiveness of ANM through its ability to provide automated end-to-end management capability for networks.

Tasks

ANM Use Cases

This chapter describes the following customer scenarios:

The use cases are presented in the following format:

- **CORE Story:** Presents the scenario without ANM, which is commonly done manually by one or more personas using more than one system.
- **Using ANM:** Presents the scenario with ANM. This section also presents the benefits of using ANM in this scenario.

Automatic device inventory synchronization between monitoring and configuration management systems

CORE Story

1. Operator manually prepares the list of devices to be added.
2. Operator adds devices to device configuration management system.
3. The same devices are added to the monitoring system.
4. Both systems pull the devices' information.
5. Verify the devices are added to both systems and are synchronized.
6. Manage the configuration and monitor the status of the devices.

Using ANM

Process

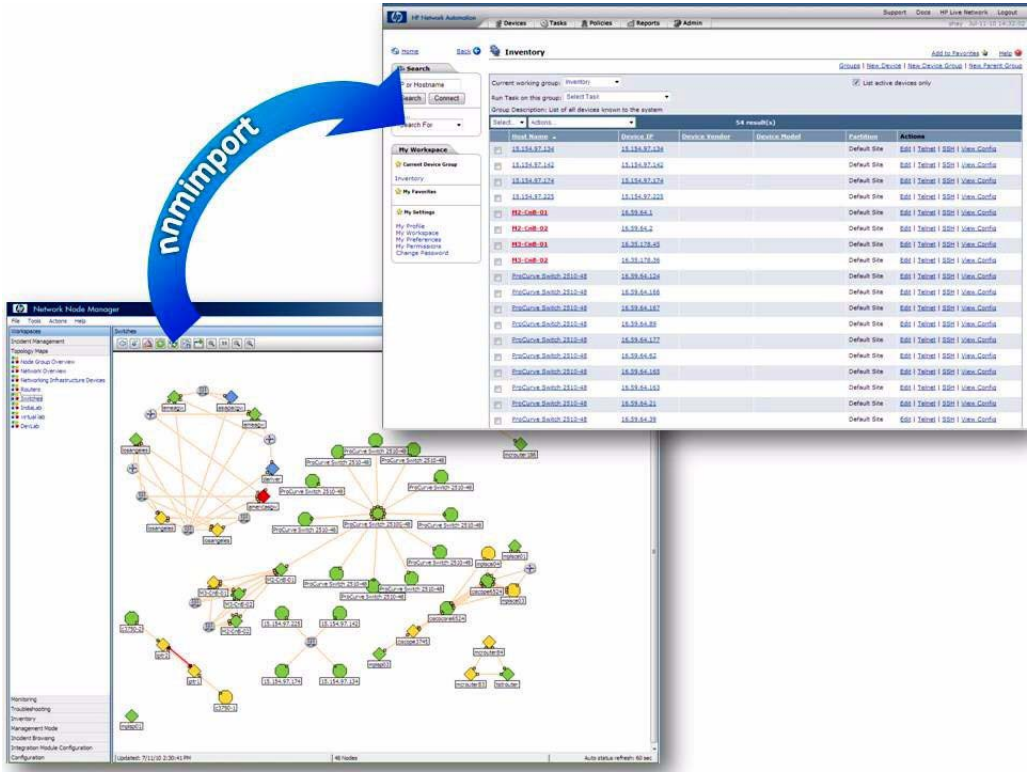
1. User prepares an NNMi loadseed file that defines the set of devices to enter into monitoring, and loads it.
2. NNMi discovers the seeded devices, adds the new devices to the NNMi topology, and begins monitoring the devices for fault and performance conditions.
3. User executes a **nnmimport.bat** or **nnmimport.sh** script. This adds the NNMi devices to NA's device list, including a reference to a UUID—the unique ID of the device within NNMi's topology database.

Note: Steps 1-3 can be fully automated by configuring Auto-Discovery in NNMi and by scheduling the nnmimport script to be run every few hours or days (using **Windows Scheduler** in a Windows server or **crontab** in a Linux/Unix server.)

---

4. NA discovers the drivers specific to the newly-added devices, takes snapshots of the devices, and runs diagnostics on the devices.
5. NNMi adds the devices to NNM iSPI for Performance and provides SNMP performance metrics to be utilized in NNM iSPI Performance for Metrics.

6 The products within the ANM Solution now share a common understanding of network inventory and network topology that are utilized in all other operations of the solution.



Note: The following requirements must be met for ANM to provide these capabilities:

- NA–NNMi integration is installed and configured properly.
- SNMP community strings used in SNMP communication with the end devices are configured in NNMi such that they can be utilized in the discovery of devices.
- Device credentials used to communicate with the end devices are configured as password rules in Network Automation.
- Within Network Automation, a rule is configured to run discover driver when a device is added.

Benefits

1. Greatly reduced device and credential management time
2. Up-to-date and compliant asset management information
3. Rapid device enter-to-management process, thus service deployment to production
4. Single view of device inventory between the two systems

Automatic remediation of an out-of-compliance device configuration change

CORE Story

1. Unauthorized device configuration change occurred.
2. If configured, Operator is notified about the change in the monitoring system.
3. Network Engineer examines the change in the configuration management system.
4. Network Engineer determines that the configuration change is out of compliance.

5 Network Engineer or Network Technician restores the correct configuration to the device if it was previously backed up.

6 Network Engineer verifies the device is restored and the incident is closed.

Using ANM

Process

1 Device configuration is changed out-of-band.

2 NA receives a SYSLOG, automatically submitting a **Take Snapshot** task to verify if the configuration was changed, and then runs a compliance check on the new configuration.

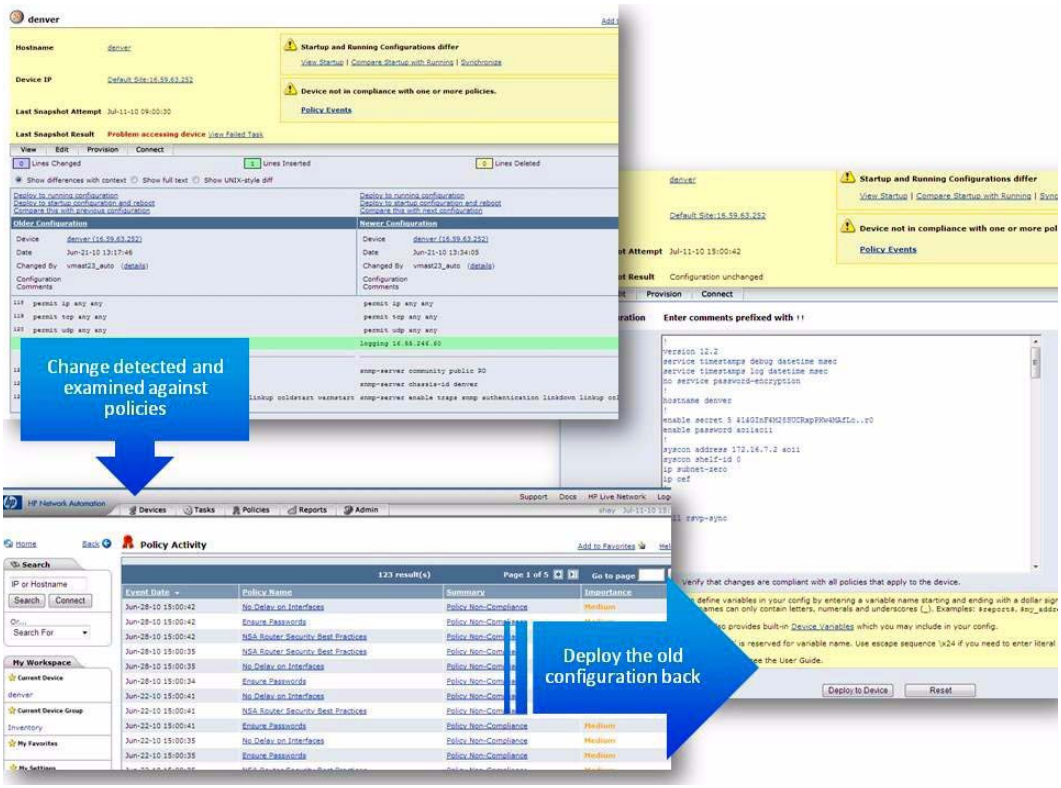
3 New configuration is out of compliance. NA sends a trap to NNMi reflecting this in the NNMi console.

4 The Operator alarms the Network Engineer about the NNMi incident and cross launches **View HP NA Configuration Diff**.

5 Network Engineer views the change and decides to roll back the change. On the previous configuration saved in NA, Network Engineer runs the **Deploy to Running Config** step within NA.

6 NA restores and verifies the correct configuration to the device.

7 NNMi incident is closed manually by the Operator.



Note: For the described use case to be fulfilled:

- customer-specific NA policies are configured, along with event rules.
- NNMi-NA integration is installed and configured properly.

Benefits

1 Around-the-clock detection and enforcement of network changes

2 Automation of the governance process through the use of NA Event Rules functionality

3. Reduced network downtime by avoiding unknown problematic changes in devices by using the compliance checks
4. Reduced network downtime achieved more quickly, thus increasing service availability and gaining a higher ROI

Run-Book automation to remediate a network fault or performance incident

CORE Story

1. Device fault and performance incident occurs.
2. Operator categorizes the incident.
3. Operator runs a diagnostic—troubleshoots and identifies the incident.
4. Operator or Network Engineer resolve the issue.
5. Operator verifies the issue has been fixed.
6. Operator closes the incident.

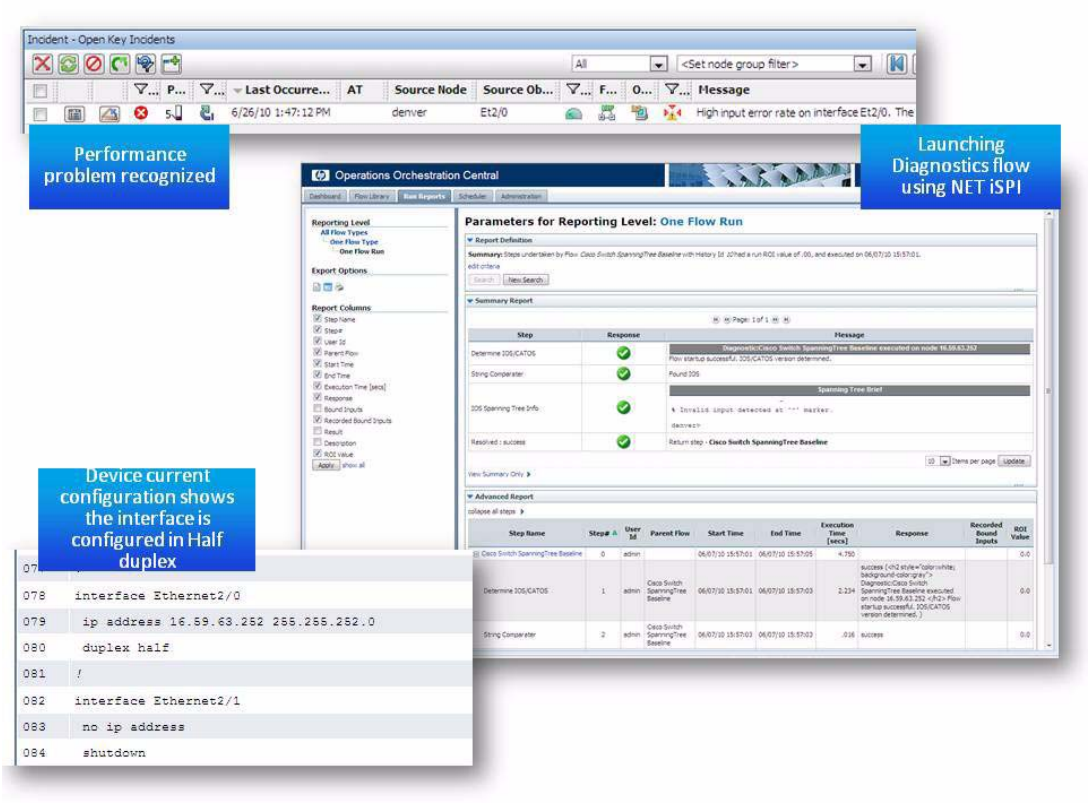
Using ANM

Process

1. Device fault and performance incident occurs due to excessive line CRC errors on the interface. (It is assumed that thresholds and actions are configured.)
2. NNMi triggers an automatic diagnostic when it receives the **InterfaceInputErrorsHigh** incident.
3. NNM iSPI NET automatically runs the diagnostic and enriches the incident with a link to the diagnostic report.
4. Operator views the incident and diagnostic data, and observes that CRCs are high on this interface.
5. Network Engineer launches additional diagnostics against the router. (These diagnostics show that the OSPF adjacency running across this interface is unstable.)
6. Network Engineer selects the node in the map and cross launches into NA in the context of this router.

7 Network Engineer discovers that the cause of the CRC errors is a duplex mismatch configuration. Using NA, the Operator configures the problem port to match the other side of the connection and the errors stop. OSPF is no longer flapping.

8 NNMi incident is either closed manually by the Operator at this time or, when the root cause of the CRC errors is remedied and the configuration is brought back to normal, automatically closed by NNMi.



Benefits

1 Minimized network downtime and performance issues

2 Increased service availability, thus higher ROI, by providing the Network Engineer with the necessary tools and data for faster real-time troubleshooting

Troubleshooting application performance problems from a network context

CORE Story

1 Network Engineer receives a phone call or trouble ticket that network performance is negatively affecting application performance.

2 Operator determines which server-to-server communications are involved in the application by using traceroute and communications involved in the application, and uses traceroute to determine the routed infrastructure utilized to transit traffic on behalf of the application.

3 From the individual routers, the routing table is checked to understand the individual interfaces associated with the application path.

4 Performance metrics from each device on the device itself are gathered, as well as the individual interfaces involved in the network path.

5 Traffic metrics via sniffer/probe tools deployed within the network path are gathered to determine which abnormal or unauthorized traffic is interfering with target application traffic across over-utilized routers.

6 Network devices are logged on to to block unauthorized traffic, or reroute target application traffic through alternate, less utilized routes.

Using ANM

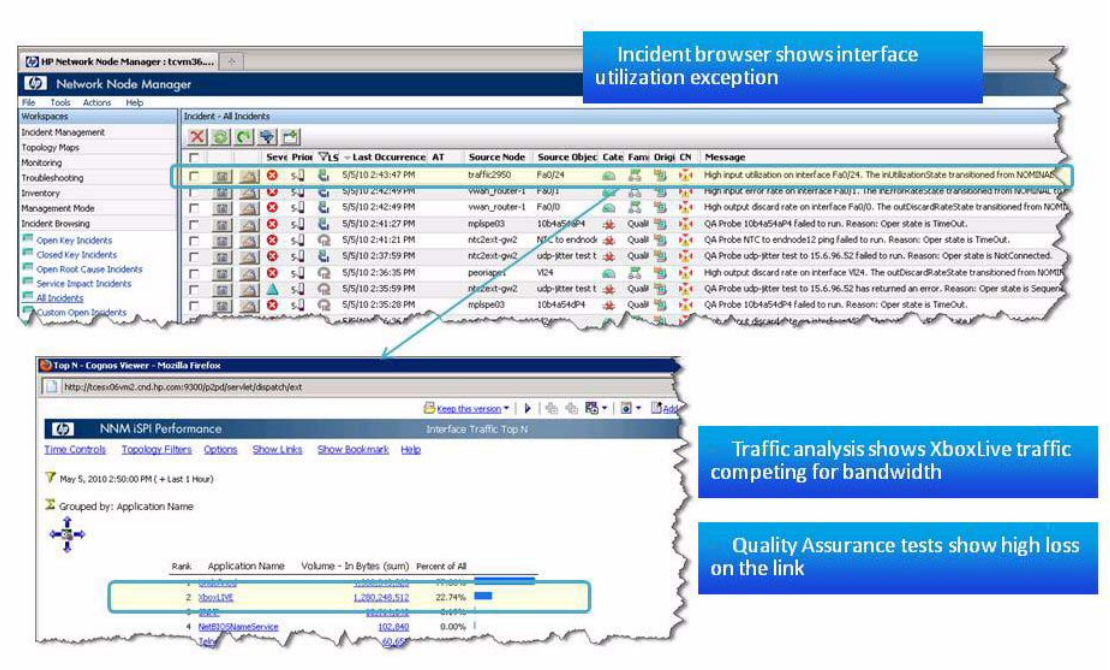
Process

1 NNMi receives a notification that interface utilization is beyond acceptable boundaries for an important network interface.

2 NNM iSPI Performance for Traffic is launched to understand the application traffic transiting the interface. Inspection reveals a critical application is part of the network traffic over the interface, and the available bandwidth is potentially below what is necessary for proper operation of the application.

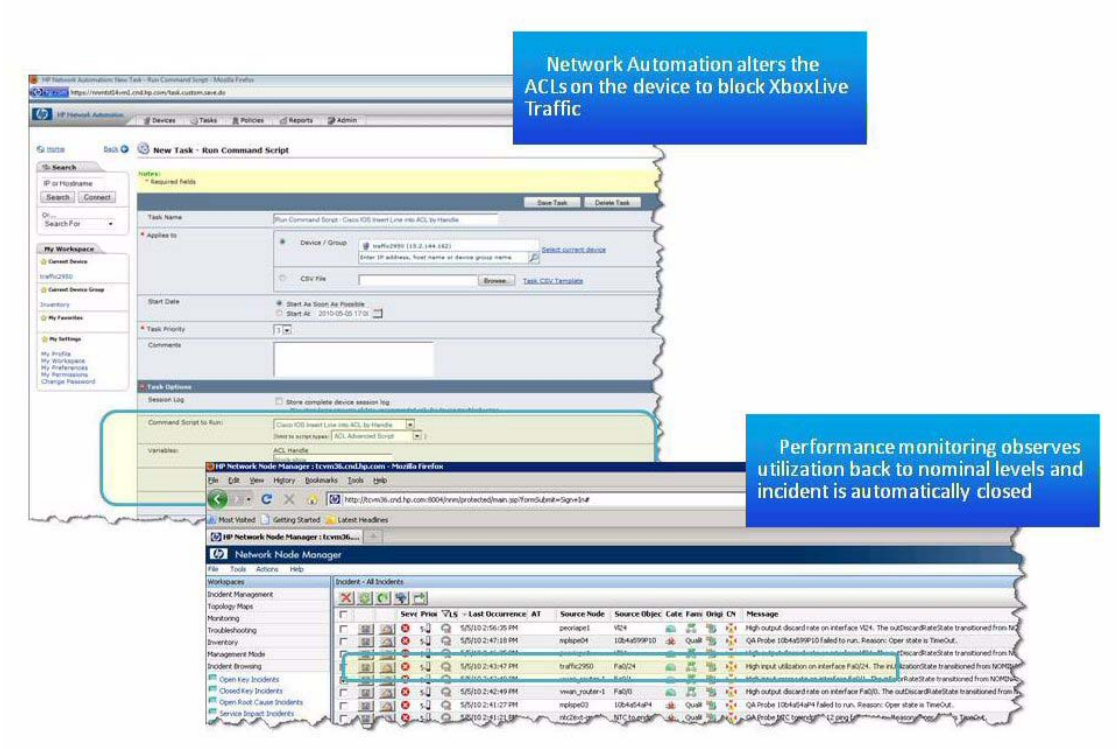
Additionally, using the NNM iSPI Performance for QA, an IPSLA test between the routers in the network path of the application indicates packet loss between the routers.

3 NNM iSPI Performance for Traffic reveals competing traffic from an unauthorized traffic source.



4 NA user (Network Engineer) runs a **Batch Insert ACL Line** to modify multiple ACLs to multiple devices to block unauthorized traffic. As part of initial setup, the **ACL handles** need to be configured—grouping of similar functionality ACLs.

5 **Interface utilization** exception automatically clears in NNMi as a result of traffic returning to normal, and the incident closes in NNMi.



Benefits

1 Increased service levels as a result of proactive management of network utilization issues before it becomes a problem for mission critical applications

2 Faster Mean Time to Repair (MTTR), with tools to triage the cause of network utilization issues

3 Efficient network configuration, including remediation of network configuration issues that affect critical services across the entire network

Index