HP Automated Network Management

Solution Version: 9.20

Configuration Guide

Document Release Date: May 2013
Software Release Date: May 2013

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 2010–2013 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 ANM Requirements

This chapter describes the hardware and software prerequisites for ANM.

Supported Product Versions

Table 1 lists the software products and versions that comprise ANM 9.20. Table 2 lists the additional software products and versions enabled by the purchase of ANM Advanced 9.20.

Table 1 ANM Products

Product Name	Product Abbreviation	Version
HP Network Node Manager i Software	NNMi	9.23
HP Network Automation	NA	9.22
HP Network Node Manager iSPI Performance for Quality Assurance Software	NNM iSPI Performance for QA	9.22
NNM iSPI Network Engineering Toolset Software	NNM iSPI NET	9.20
HP Network Node Manager iSPI Performance for Metrics Software	NNM iSPI Performance for Metrics	9.20 patch 3
HP Network Node Manager iSPI Performance for Traffic Software	NNM iSPI Performance for Traffic	9.21

Table 2 ANM Advanced Optional Additional Integrated Products

Product Name	Product Abbreviation	Version
HP Network Node Manager iSPI for MPLS Software	NNM iSPI for MPLS	9.21
HP Network Node Manager iSPI for IP Multicast Software	NNM iSPI for IP Multicast	9.21
HP Network Node Manager iSPI for IP Telephony Software	NNM iSPI for IP Telephony	9.21

Note the following:

- The ANM Advanced license also enables the NNMi Advanced functionality.
- The HP NNMi—HP NA integration cannot distinguish among duplicate IP addresses. For this reason, the integration is not supported in overlapping address domain (OAD) environments.

Example Deployment Architecture

This section describes several example deployment architectures:

Basic ANM Deployment

Figure 1 on page 9 shows the example deployment architecture for ANM. The left side of the drawing shows the distribution of the ANM components across six servers. The right side of the drawing shows the distribution of the ANM Advanced components across six servers. Follow the diagram that matches your ANM license. Each box in the diagram represents a server.

The instructions in this document support this example deployment architecture. The procedures described in Chapter 2, Configuring ANM reference the server names listed in Table 3 on page 10. The example deployment architecture is based on the following assumptions:

- Each product that requires a database uses the embedded database available with that product.
- All servers are on the same network segment without firewalls between servers. Having a firewall between the solution servers affects product performance.
- The network includes supported network devices.
- The network includes devices running a supported flow technology and devices with embedded IP SLA capabilities.

Figure 1 Example ANM Deployment Architecture

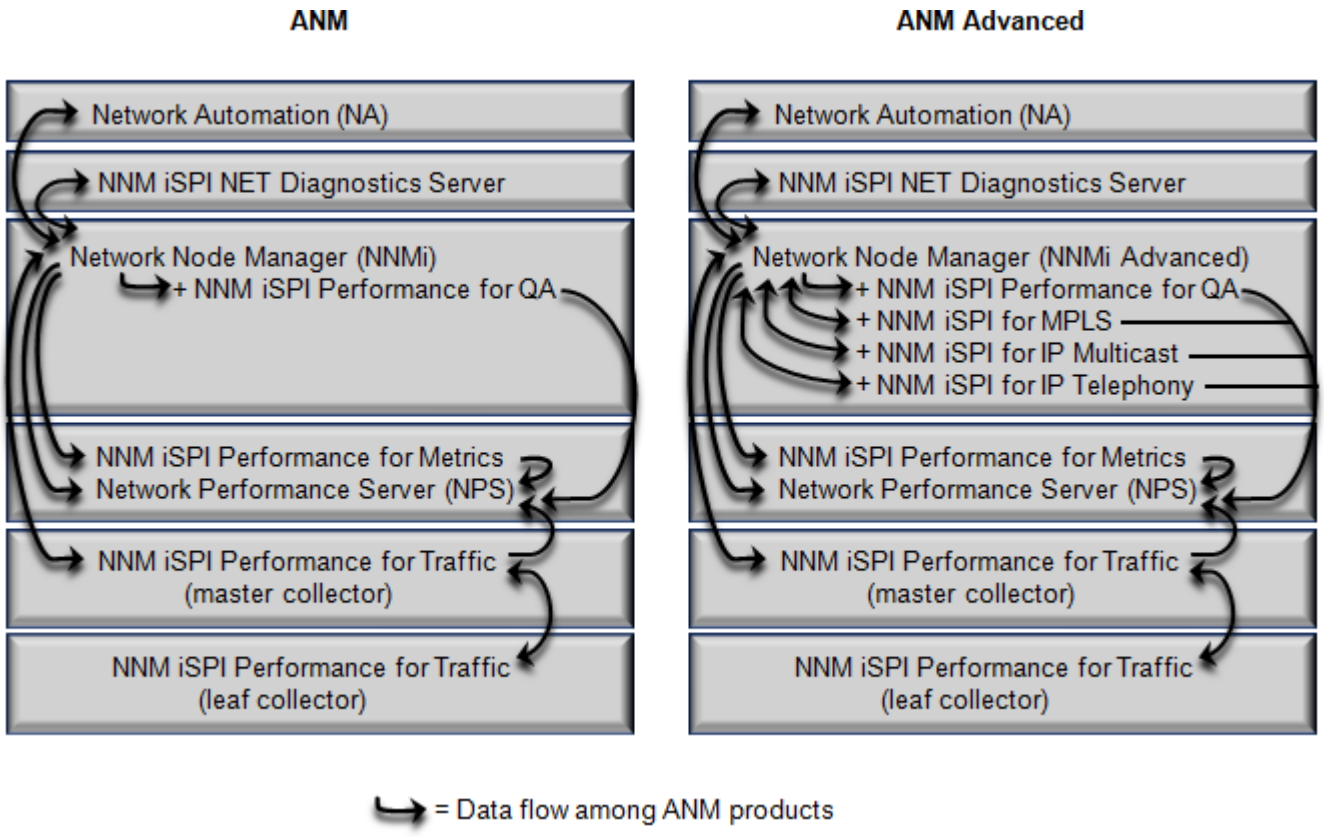


Table 3 presents another view of which products are installed to each server in the example ANM deployment architecture.

Table 3 Example Deployment Servers

Server	Installed Software
NNMi Management Server	• NNMi • NNM iSPI Performance for QA • NNM iSPI Performance for Traffic extensions • ANM Advanced optional integrated products: — NNM iSPI for MPLS — NNM iSPI for IP Multicast — NNM iSPI for IP Telephony
NA Server	• NA
NPS Server	• Network Performance Server (NPS) used by all of the NNM Performance iSPIs • NNM iSPI Performance for Metrics
Traffic Master Server	• NNM iSPI Performance for Traffic master collector
Traffic Leaf Server	• NNM iSPI Performance for Traffic leaf collector
NNM iSPI NET Diagnostics Server	• NNM iSPI NET

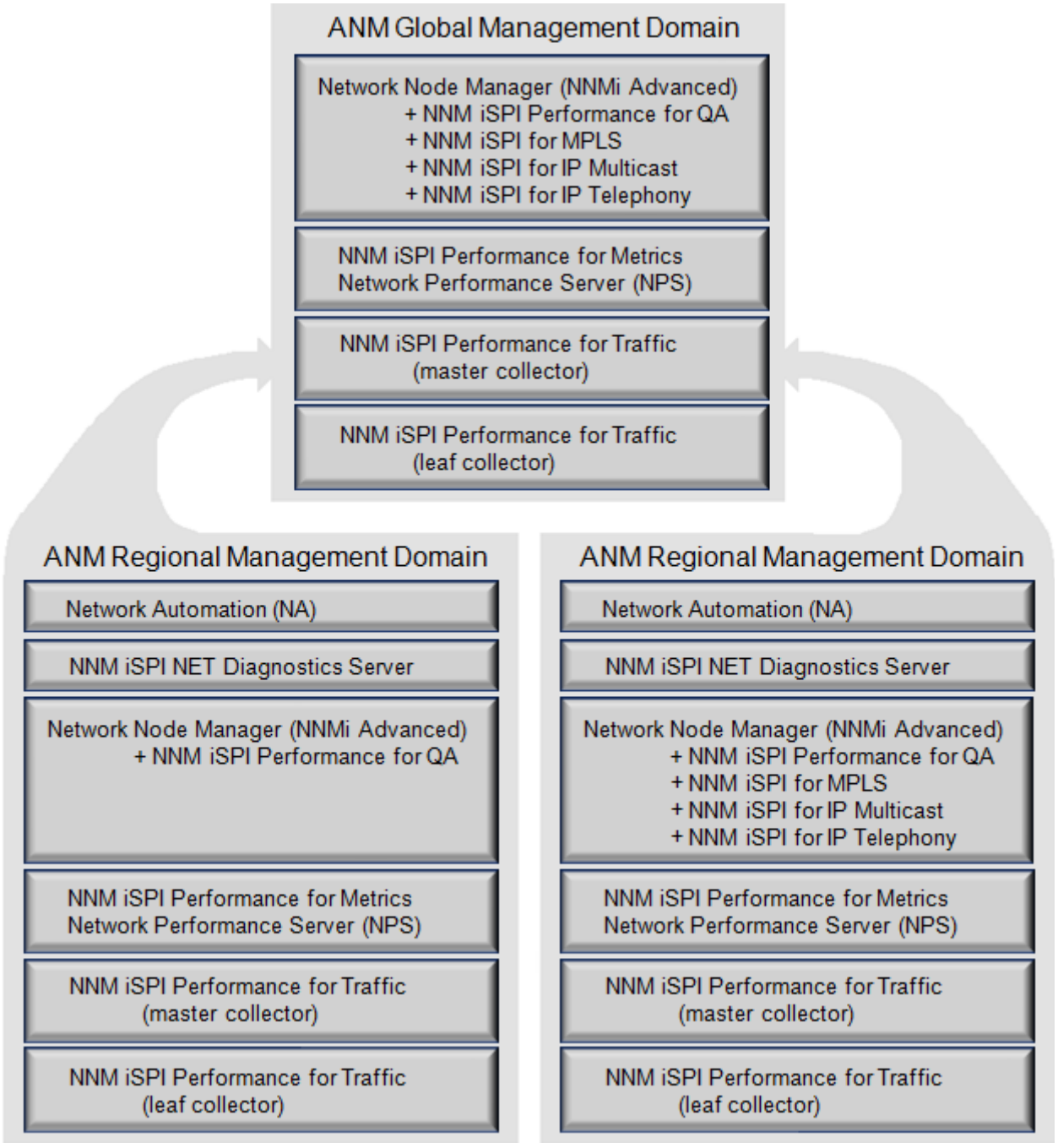
NNMi Global Network Management with Multiple NA Cores

Figure 2 on page 11 shows an example deployment architecture for distributed ANM, which is built on the NNMi Global Network Management feature. The NNMi global manager must have the NNMi Advanced license, so the ANM global management domain has the ANM Advanced license. The NNMi regional managers can have either the NNMi or the NNMi Advanced license, which maps to either the ANM or the ANM Advanced license. The NNM Performance iSPIs can consolidate data in the ANM global management domain. When the ANM regional management domain has the ANM Advanced license, NNM iSPI for MPLS, NNM iSPI for IP Multicast, and NNM iSPI for IP Telephony can also consolidate data in the ANM global management domain.

NA and NNM iSPI NET are not supported in the ANM global management domain.

If NA is configured for Horizontal Scalability, only one of the NA cores can participate in ANM.

Figure 2 Example Architecture for Distributed ANM



NNMi Global Network Management with One NA Core

Figure 3 on page 13 shows an example deployment architecture for distributed NNMi with one NA connected to each NNMi regional management domain. In this architecture, the NA core responds to requests from the NNMi regional management servers but does not initiate communication with the NNMi regional management servers. See Table 4 on page 12.

The HP NNMi–HP NA integration cannot distinguish among duplicate IP addresses. For this reason, all nodes synchronized from the NNMi regional management servers to the NA core must have unique IP addresses.

NA and NNM iSPI NET are not supported in the ANM global management domain.

In a multi-tenancy environment, some limitations apply. See Table 4 on page 12.

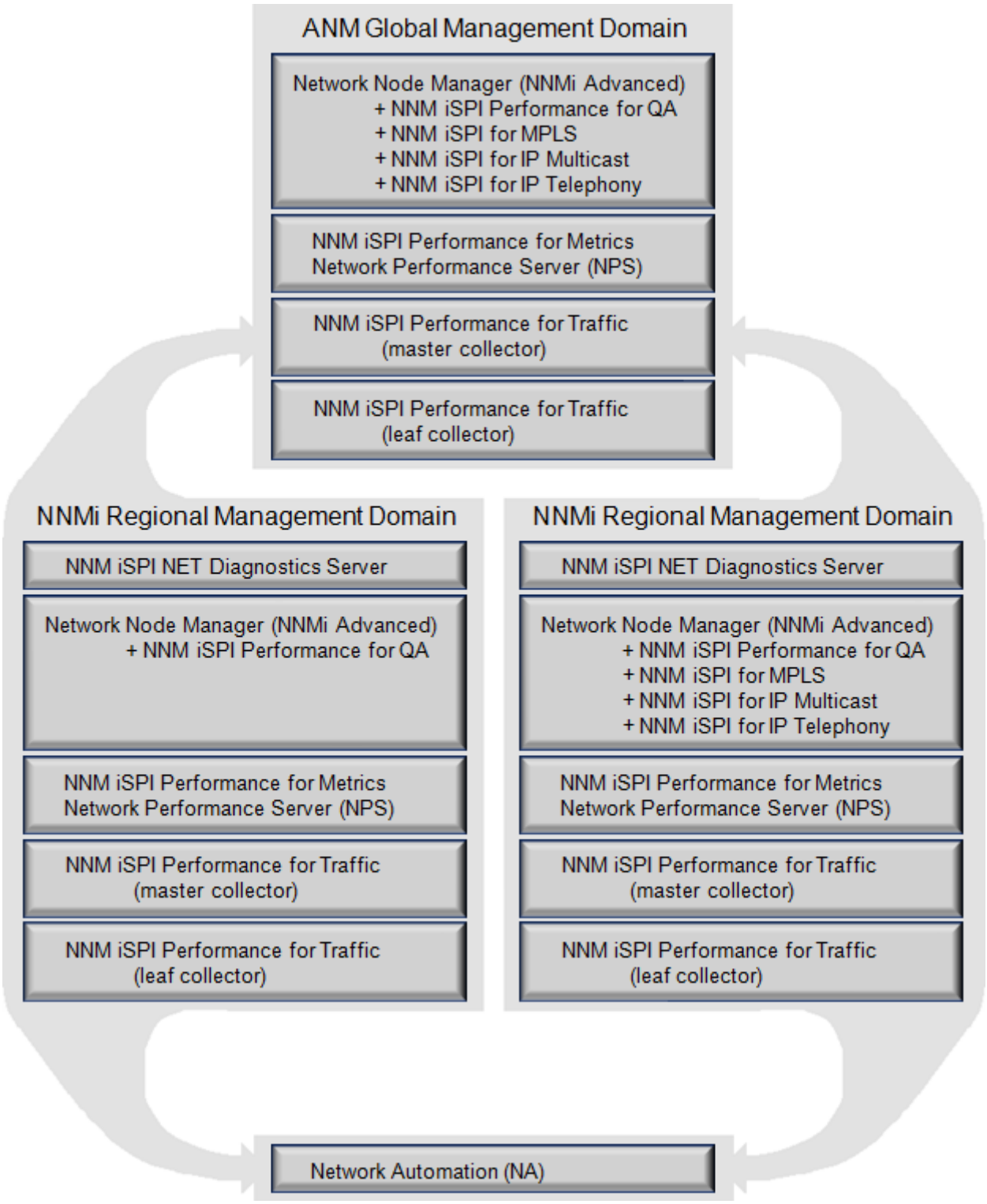
Table 4 Integration Functionality Limitations

Integration Feature	One NNMi to One NA	Multiple NNMis to One NA
Synchronize the NNMi topology into the NA inventory	X	X
Synchronize the NA inventory into the NNMi topology (Not available in a multi-tenancy environment)	X	
Deleting a node in NNMi unmanages that device in NA	X	X
Deleting a device in NA deletes that node in NNMi	X	
Launch NA pages from the NNMi console	X	X
View NA data in the NNMi analysis pane (with permission)	X	X
From NNMi, trigger NA diagnostics	X	X
Identify layer 2 connections with mismatched states	X	
Send device configuration change notifications from NA to NNMi	X	
Disable network management during device configuration	X	
Propagate device community string changes	X	
Single sign-on from NNMi to NA	X	X
Use an SSL connection from NNMi to NA	X	X
Use an SSL connection from NA to NNMi	X	

If NA is configured for Horizontal Scalability, only one of the NA cores can participate in ANM.

The architecture of Figure 3 is built on the NNMi Global Network Management feature. The NNMi global manager must have the NNMi Advanced license, so the ANM global management domain has the ANM Advanced license. The NNMi regional managers can have either the NNMi or the NNMi Advanced license, which maps to either the ANM or the ANM Advanced license. The NNM Performance iSPIs can consolidate data in the ANM global management domain. When the ANM regional management domain has the ANM Advanced license, NNM iSPI for MPLS, NNM iSPI for IP Multicast, and NNM iSPI for IP Telephony can also consolidate data in the ANM global management domain.

Figure 3 Example Architecture with Distributed NNMi and one NA



Hardware and Software Requirements

This section describes the hardware and software requirements for the basic ANM deployment of Figure 1 on page 9. It consolidates the information from the product support matrices for a medium-sized network with the following parameters:

- 3,000 to 8,000 managed devices
- Up to 60,000 performance polled interfaces polled at five minute intervals
- 30,000 configured QA probes
- 600,000 flow records per minute sent to the NNM iSPI Performance for Traffic master collector
- 300,000 flow records per minute sent to the NNM iSPI Performance for Traffic leaf collector

The stated requirements are for physical systems. For additional information, including requirements for virtual systems, non-embedded databases, and different environment sizes, see the product support matrices, which are available from the HP manuals web site as described in Product Documentation on page 23.

If there are discrepancies between the requirements listed in this chapter and those listed in the individual product support matrices, follow the information in the product support matrices.

The ANM servers need not be homogenous. With a few exceptions noted in this chapter, each server may be any of the supported types for that software.

Red Hat 5.5 or later is required for CPU chips with more than 4 cores on a single chip. (Do not confuse this number with the total number of cores; this number is just the cores per chip.).

This section describes the requirements for the following systems:

Web Browser and Software Requirements

Table 5 lists the web browser requirements and additional software required to use certain ANM features.

Table 5 Web Browser and Software Requirements for Using ANM

Purpose	Requirements
Run the NNMi console, the NA console, and the NPS console	One of: • Microsoft Internet Explorer (32-bit and 64-bit) version 8 (not running in Compatibility View mode) • Microsoft Internet Explorer (32-bit and 64-bit) version 9 (not running in Compatibility View mode) • Mozilla Firefox 10.x ESR or 17.x ESR on Microsoft Windows® or Linux The Firefox ESR (Extended Support Release) browser is available from: **http://www.mozilla.org/en-US/firefox/organizations/all.html** Disable automatic updating in the Firefox **Options** dialog box (**Advanced > Update**).
View NNMi graphs, the NNMi MIB browser and the NA device selector	• Adobe Flash Player Plug-in version 10.2 (or later minor version) or version 11.1 (or later minor version). • For 64-bit Internet Explorer, version 11.1 or later is required
View NA summary reports	• Microsoft Excel 2000 or later
View exported map files	One of: • Microsoft Visio 2007 • Microsoft Visio 2010

Each web browser that will be used to run any of the ANM consoles must be configured as follows:

- Disable all pop-up window blockers.
- Enable cookies.
- Enable JavaScript.
- Set Internet Explorer to enable VML.
- Set Firefox to open new windows as separate windows, not tabs.
- Set the display resolution to at least 1024 x 768.

NNMi Management Server

Table 6 lists the combined requirements for the following software to be installed on the NNMi management server:

- NNMi
- NNM iSPI Performance for QA
- NNM iSPI Performance for Traffic extension

Table 6 NNMi Management Server Requirements

Area	Minimum Requirements
Hardware	**NOTE**: The NNM iSPI Performance for QA Intelligent Response Agent (iRA) runs on Windows and Linux operating systems only. • System: — Windows or Linux: Intel® 64-bit (x86-64) or AMD 64-bit (AMD64) x 10 CPU cores — HP-UX: Intel Itanium® Processor Family x 10 CPU cores — Solaris: Oracle SPARC64 VI or later x 10 CPU cores • RAM: 24GB for NNMi and NNM iSPI Performance for QA combined • Virtual Memory: Double the amount of RAM • Disk space for installation and operation: 355MB for NNMi and NNM iSPI Performance for QA combined Recommended that free space be on a different drive than the operating system. **NOTE**: The NNM iSPI for IP Multicast, NNM iSPI for IP Telephony, and NNM iSPI for MPLS must be co-resident with NNMi. If you plan to install any of these NNM iSPIs, increase the NNMi management server requirements as follows: 1 From the support matrix of each additional NNM iSPI, determine the following values: — Number of CPU cores — RAM — Disk space for installation and runtime 2 Add these values to the values listed in Table 6. The available virtual memory should be double the total RAM requirement for all installed products. For information about downloading the product support matrices, see Product Documentation on page 23.

Table 6 NNMi Management Server Requirements (Continued)

Area	Minimum Requirements
Operating System	**NOTE**: If the NNMi management server runs on a Windows operating system, the NPS server also *must* run on a Windows operating system. • Windows: — Windows Server 2008 x64 Datacenter Edition with Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition with Service Pack 1 — Windows Server 2008 x64 Enterprise Edition with Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition with Service Pack 1 — Windows Server 2008 x64 Standard Edition with Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition with Service Pack 1 • HP-UX: HP-UX 11i v3 • Linux: — Red Hat Enterprise Linux Server 6.0 (or later minor version through 6.x) — Red Hat Enterprise Linux Server 5.4 (or later minor version through 5.x) • Solaris: Oracle Solaris 10 SPARC

NA Server

Table 7 lists the requirements for NA to be installed on the NA server.

Table 7 NA Server Requirements

Area	Minimum Requirements
Hardware	• System: Windows or Linux: — Intel® 64-bit (x86-64) x 6 CPU cores — AMD 64-bit (AMD64) x 6 CPU cores • Solaris: — Oracle SPARC64 VI or later (M-Series) x 6 CPU cores — Oracle SPARC T4 or later (T-Series) x 6 CPU cores • RAM: 16GB • Disk space for installation and operation: 512GB Recommended that free space be on a different drive than the operating system.
Operating System	• Windows: — Windows Server 2008: x64 Datacenter Edition, Service Pack 2 — Windows Server 2008: R2 x64 Datacenter Edition, Service Pack 1 — Windows Server 2008: x64 Enterprise Edition, Service Pack 2 — Windows Server 2008: R2 x64 Enterprise Edition, Service Pack 1 — Windows Server 2008: x64 Standard Edition, Service Pack 2 — Windows Server 2008: R2 x64 Standard Edition, Service Pack 1 • Linux: — Red Hat Enterprise Linux Server AS 4.0 or later minor version — Red Hat Enterprise Linux Server 5.4 or later through 5.9 — Red Hat Enterprise Linux Server 6.0 or later through 6.2 — SUSE Linux Enterprise Server 9 — SUSE Linux Enterprise Server 11 Service Pack 1 • Solaris: Oracle Solaris 10 SPARC
Perl	• To use the Perl SDK: — Windows: ActivePerl 5.8.x — Linux or Solaris: Perl 5.8.x • To use the NA connect module with SSH: Perl Net::SSH::Expect module • **NOTE**: SSH connections to the NA Perl API require the Net::SSH::Expect module. Due to limitations of ActiveState ActivePerl on Windows, the NA Perl API does not support SSH connections from Windows systems. As a workaround, install the NA client on a supported Linux or Solaris system, and run the NA Perl API from that system.

NPS Server

Table 8 lists the combined requirements for the following software to be installed on the NPS server:

- NPS
- NNM iSPI Performance for Metrics report pack
- NNM iSPI Performance for QA report pack
- NNM iSPI Performance for Traffic report pack

Table 8 NPS Server Requirements

Area	Minimum Requirements
Hardware	• System: — Windows or Linux: Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 28 CPU cores • RAM: 88GB for NPS, NNM iSPI Performance for Metrics, NNM iSPI Performance for QA, and NNM iSPI Performance for Traffic combined • Virtual Memory: Double the amount of RAM • Disk space for installation and operation: 6.5TB for NPS, NNM iSPI Performance for Metrics, NNM iSPI Performance for QA, and NNM iSPI Performance for Traffic combined Recommended that free space be on a different drive than the operating system. **NOTE**: This requirement is for the minimum retention period. For longer retention periods, increase the operational disk space. **NOTE**: The NNM iSPI for IP Multicast, NNM iSPI for IP Telephony, and NNM iSPI for MPLS must be co-resident with NNMi. If you plan to install any of these NNM iSPIs, increase the NPS server requirements as follows: 1 From the support matrix of each additional NNM iSPI, determine the disk space requirement for report data. 2 Add this values to the disk space value listed in Table 8. The available virtual memory should be double the total RAM requirement for all installed products. For information about downloading the product support matrices, see Product Documentation on page 23.
Operating System	**NOTE**: If the NNMi management server runs on a Windows operating system, the NPS server also *must* run on a Windows operating system. • Windows: — Windows Server 2008 x64 Datacenter Edition with Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition with Service Pack 1 — Windows Server 2008 x64 Enterprise Edition with Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition with Service Pack 1 — Windows Server 2008 x64 Standard Edition with Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition with Service Pack 1 • Linux: — Red Hat Enterprise Linux Server 6.0 (or later minor version through 6.x) — Red Hat Enterprise Linux Server 5.4 (or later minor version through 5.x)

Traffic Master Server

Table 9 lists the requirements for the NNM iSPI Performance for Traffic master collector to be installed on the Traffic Master server.

Table 9 Traffic Master Server Requirements

Area	Minimum Requirements
Hardware	• System: — Windows or Linux: Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 8 CPU cores • RAM: 16GB • Virtual Memory: Double the amount of RAM • Disk space for installation and operation: 800MB Recommended that free space be on a different drive than the operating system.
Operating System	**NOTE**: Recommended that the NNM iSPI Performance for Traffic master collector and the NNM iSPI Performance for Traffic leaf collector run on the same operating system. • Windows: — Windows Server 2008 x64 Datacenter Edition with Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition with Service Pack 1 — Windows Server 2008 x64 Enterprise Edition with Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition with Service Pack 1 — Windows Server 2008 x64 Standard Edition with Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition with Service Pack 1 • Linux: — Red Hat Enterprise Linux Server 6.0 (or later minor version through 6.x) — Red Hat Enterprise Linux Server 5.4 (or later minor version through 5.x)

Traffic Leaf Server

Table 10 lists the requirements for the NNM iSPI Performance for Traffic leaf collector to be installed on the Traffic Leaf server.

Table 10 Traffic Leaf Server Requirements

Area	Minimum Requirements
Hardware	• System: — Windows or Linux: Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 4 CPU cores • RAM: 16GB • Virtual Memory: Double the amount of RAM • Disk space for installation and operation: 800MB Recommended that free space be on a different drive than the operating system.
Operating System	**NOTE**: Recommended that the NNM iSPI Performance for Traffic master collector and the NNM iSPI Performance for Traffic leaf collector run on the same operating system. • Windows: — Windows Server 2008 x64 Standard Edition with Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition with Service Pack 1 — Windows Server 2008 x64 Datacenter Edition with Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition with Service Pack 1 — Windows Server 2008 x64 Enterprise Edition with Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition with Service Pack 1 — • Linux: — Red Hat Enterprise Server AS 5.2 (or later minor version through 5.x) — Red Hat Enterprise Server ES 5.2 (or later minor version through 5.x)

NNM iSPI NET Diagnostics Server

Table 11 lists the requirements for NNM iSPI NET to be installed on the NNM iSPI NET Diagnostics server.

Table 11 NNM iSPI NET Diagnostics Server Requirements

Area	Minimum Requirements
Hardware	• System: — Windows: Intel 64-bit (x86-64) or AMD 64-bit (AMD64) • RAM: 2GB • Disk space for installation and operation: 2GB Recommended that free space be on a different drive than the operating system.
Operating System	• Windows: — Windows Server 2008 x64 Datacenter Edition with Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition with Service Pack 1 — Windows Server 2008 x64 Enterprise Edition with Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition with Service Pack 1 — Windows Server 2008 x64 Standard Edition with Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition with Service Pack 1

Product Documentation

As a convenience, the Automated Network Management Suite category on the HP Product Manuals web site includes the `ANM_Product_Docs.zip` file, which contains the product documents referenced by this document, the *ANM Configuration Guide*. The product documents are revised as needed. The `ANM_Product_Docs.zip` file is updated periodically to include the revised documents.

The complete, most current documentation set for each ANM product is available on the HP Product Manuals web site. Table 12 on page 24 lists the search category for each ANM product. To locate documentation for a given product, choose the product name from Table 12, choose product version **`9.20`**, and then choose the operating system. Select the version of the document that matches the software version (for example, 9.20) you are using.

Access the HP Product Manuals web site at:

h20230.www2.hp.com/selfsolve/manuals

Use your HP Passport account to access this site, or register a new HP Passport identifier.

Enable Linking between ANM and Product Documentation

The ANM documentation and its associated product documentation (for example, Network Automation Software and Network Node Manager i Software) include markers that enable navigation from this document to specific sections or chapters in the associated product documentation.

Each link that navigates to another PDF is identified with orange text as shown in Figure 4.

Figure 4 Format of a Link to an External PDF

This navigation strategy requires a specific name for each product documentation PDF file. Table 12 lists the expected names. Where possible, the files in the `ANM_Product_Docs.zip` file have the correct names. In some cases, you must make minor changes to the file names to enable linking.

If you do not follow the steps described in this section, links to specific sections or chapters in the associated product documentation will not work. You can manually navigate to each section or chapter identified in the ANM documentation.

To enable linking between the ANM documentation and its associated product documentation, follow these steps:

1. Create a directory for the ANM documentation and the associated product documentation. For example:

   `anm_docs`

2. Connect to the HP Product Manuals web site at:

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

3 From the Automated Network Management Suite category, download the following files to the directory created in step 1:

- *Automated Network Management Concepts Guide*
- *Automated Network Management Configuration Guide*
- `ANM_Product_Docs.zip`

4 Unzip the `ANM_Product_Docs.zip` file to the directory created in step 1.

5 Verify the file names against the values in the **Save As File Name** column of Table 12. Rename files as necessary:

- Remove the operating system identifiers from the file names. For example, rename `iSPI_Metrics_Install_Linux.pdf` to `iSPI_Metrics_Install.pdf`.
- Remove the localized language identifiers from the file names. For example, rename `NA_Install_ko.pdf` to `NA_Install.pdf`.

The file name, including capitalization, must match the name specified.

6 *Optional*. For a product document that is newer than the `ANM_Product_Docs.zip` file, download that file from the product search category on the HP Product Manuals web site, and then rename the file according to the **Save As File Name** column of Table 12.

Table 12 Product Documentation Linked from the ANM Documentation

Product Search Category	Referenced Documents	Save As File Name
network automation	*HP Network Automation Installation and Upgrade Guide*	`NA_Install.pdf`
	HP Network Automation User Guide	`NA_User.pdf`
network node manager	*HP Network Node Manager i Software System and Device Support Matrix*	`NNMi_SupportMatrix.pdf`
	HP Network Node Manager i Software Help for Administrators	`NNMi_HelpAdmin.pdf`
	HP Network Node Manager i Software Deployment Reference	`NNMi_Deploy.pdf`
	HP Network Node Manager i Software - HP Network Automation Integration Guide	`NNMi_NA_Integrate.pdf`
	HP Network Node Manager i Software Upgrade Reference	`NNMi_Upgrade.pdf`
network node manager iSPI for NET	*HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*	`iSPI_NET_Install.pdf`
	HP NNM iSPI Network Engineering Toolset Software Release Notes	`iSPI_NET_ReleaseNotes.pdf`
network node manager iSPI Performance for Metrics	*HP Network Node Manager iSPI Performance for Metrics Software Installation Guide*	`iSPI_Metrics_Install.pdf`

Table 12 Product Documentation Linked from the ANM Documentation (Continued)

Product Search Category	Referenced Documents	Save As File Name
network node manager iSPI Performance for QA	*HP Network Node Manager iSPI Performance for Quality Assurance Software Installation Guide*	`iSPI_QA_Install.pdf`
	HP Network Node Manager iSPI Performance for Quality Assurance Software Intelligent Response Agent Installation Guide	`iSPI_QA_iRA_Install.pdf`
	HP Network Node Manager iSPI Performance for Quality Assurance Help for Administrators	`iSPI_QA_HelpAdmin.pdf`
network node manager iSPI Performance for Traffic	*HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*	`iSPI_Traffic_Install.pdf`
	HP Network Node Manager iSPI Performance for Traffic Online Help	`iSPI_Traffic_Help.pdf`
network node manager SPI for IP Multicast	*HP Network Node Manager iSPI for IP Multicast Software Installation Guide*	`iSPI_Mcast_Install.pdf`
network node manager SPI for IP Telephony	*HP Network Node Manager iSPI for IP Telephony Software Installation Guide*	`iSPI_IPT_Install.pdf`
network node manager SPI for MPLS VPN	*HP Network Node Manager iSPI for MPLS Software Installation Guide*	`iSPI_MPLS_Install.pdf`

2 Configuring ANM

This chapter outlines the process for installing and configuring ANM.

For a new installation, complete all procedures in the following sections:

- Install and Configure ANM on page 27
- Verify the HP NNMi–HP NA Integration on page 34
- License ANM on page 35

For an upgrade from ANM 9.00 or 9.10 to ANM 9.20, complete all procedures in the following sections:

- Upgrade from ANM 9.10 to ANM 9.20 on page 36
- Verify the HP NNMi–HP NA Integration on page 34

Install and Configure ANM

This section outlines the procedure for installing and configuring ANM for the example deployment architecture of Figure 1 on page 9. For additional information, see the product documentation, which is available from the HP manuals web site as described in Product Documentation on page 23.

Note the following:

- It is recommended to run ANM in a test lab before deploying the solution to production.
- For assistance configuring ANM for your specific environment, contact the HP Professional Services Organization.
- Perform all configuration steps using administrator access to the ANM products.
- Single sign-on among the ANM products provides for moving from one console to another without repeatedly logging on. During the ANM configuration process, the administrator must log on to NNMi and NA separately.
- Anti-virus and backup software can interfere with the products' operation if the software locks files while the products are running. Any application that locks files should be configured to exclude the installation and data directories (selected during the installation process).
- Windows 2008 includes the concept of User Access Control (UAC). Users who are part of the Administrator group may not have full Administrator privileges. All scripts and commands associated with the products detect and warn if the user is not enabled. Scripts and commands must be run with full Administrator access. To achieve full Administrator access, right-click the **Command Tool** icon, and then click **Run as Administrator**.

To install and configure ANM, complete the following tasks:

- Task 1: Prepare a Web Browser
- Task 2: Install and Configure NNMi
- Task 3: Install and Configure NPS and NNM iSPI Performance for Metrics
- Task 4: Install and Configure NNM iSPI Performance for QA
- Task 5: Install the NNM iSPI Performance for Traffic Master Collector
- Task 6: Install and Configure the NNM iSPI Performance for Traffic Leaf Collector
- Task 7: Install and Configure NNM iSPI NET
- Task 8: Install and Configure NA
- Task 9: Configure the HP NNMi—HP NA Integration

Task 1: Prepare a Web Browser

On a system that can access the ANM servers, configure a supported web browser as described in "Configuring a Web Browser to Access the NNMi Console" in the *HP Network Node Manager i Software Interactive Installation Guide*.

To take advantage of single sign-on among the ANM products, always start the NNMi console with a URL that includes the fully-qualified domain name of the NNMi management server.

Task 2: Install and Configure NNMi

Install NNMi before installing any of the other ANM products.

To install and configure NNMi, follow these steps:

1. Verify that the NNMi management server meets the requirements listed in Table 6 on page 16.
2. *UNIX NNMi management server only.* Prepare the NNMi management server as described in "Installation Prerequisites" for the server operating system type (HP-UX, Linux, or Solaris) in the *HP Network Node Manager i Software System and Device Support Matrix*.
3. On the NNMi management server, verify the server configuration as described in "Preparing the NNMi Management Server" in the *HP Network Node Manager i Software Interactive Installation Guide*.
4. On the NNMi management server, install NNMi as described in "Installing NNMi Manually" in the *HP Network Node Manager i Software Interactive Installation Guide*.
5. In the NNMi console, configure NNMi with the access credentials and appropriate timeout and retry values for different devices and areas of your network. For information, see "Configuring Communication Protocol" in the NNMi Help for Administrators.
6. In the NNMi console, configure NNMi discovery. For information, see "Configure Discovery" in the NNMi Help for Administrators.
7. On the NNMi management server, enable single sign-on for NNMi as described in "Enabling SSO for a Single Domain" in the *HP Network Node Manager i Software Deployment Reference*.

8 In the NNMi console, create two NNMi users with the Web Service Client role:

- One NNMi user for NNM iSPI Performance for QA.
- One NNMi user for NNM iSPI Performance for Traffic.

For information, see "Configuring Security" in the NNMi Help for Administrators.

Task 3: Install and Configure NPS and NNM iSPI Performance for Metrics

Prerequisite: NNMi must be installed on the NNMi management server.

To install and configure NPS and NNM iSPI Performance for Metrics, follow these steps:

1 On the NNMi management server, run the NNM iSPI Performance for Metrics enablement script as described in "Enabling NPS on the NNMi Management Server" in the *HP Network Node Manager iSPI Performance for Metrics Software Installation Guide*.

2 Verify that the NPS server meets the requirements listed in Table 8 on page 19.

3 On the NPS server, install NPS as described in "Installing NPS" in the *HP Network Node Manager iSPI Performance for Metrics Software Installation Guide*.

The installation runs for about one hour without interaction.

During the installation, select to install NNM iSPI Performance for Metrics also.

4 On the NPS server, verify the installation as described in "Validate the Configuration File" in the *HP Network Node Manager iSPI Performance for Metrics Software Installation Guide*.

5 In the NNMi console, configure fault and performance polling. For information, see the following topics in the NNMi Help for Administrators:

- "Configure Baseline Settings for Interfaces"
- "Configure Baseline Settings for Node Components"
- "Configure Threshold Monitoring for Interfaces"
- "Configure Threshold Monitoring for Node Components"

Task 4: Install and Configure NNM iSPI Performance for QA

Prerequisites:

- NNMi must be installed on the NNMi management server.
- NPS must be installed on the NPS server.

To install and configure NNM iSPI Performance for QA, follow these steps:

1. On the NNMi management server, install NNM iSPI Performance for QA as described in "Installing on the NNMi Management Server" in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Installation Guide*.
2. *Optional*. On the NNMi management server, install the NNM iSPI Performance for QA Intelligent Response Agent (iRA) as described in "Installing the iRA on a Windows System" or "Installing the iRA on a Linux System" in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Intelligent Response Agent Installation Guide*.

   The iRA runs on Windows and Linux operating systems only.

3. On the NNMi management server, configure single sign-on between NNMi and NNM iSPI Performance for QA as described in "Enabling Single Sign-On" in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Help for Administrators*.

   This configuration enables NNMi users with the Administrator role to open the Quality Assurance Configuration console without entering logon credentials.

4. In the NNMi console, wait for NNMi to discover the existing QA probes.

   The discovered probes appear in the Probes table view of the Quality Assurance workspace.

   Alternatively, hasten the discovery process as described in "Discovering QA Probes Using nmsqadisco.ovpl Command" in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Help for Administrators*.

5. In the NNMi console, configure QA probes as described in "Launching the Probe Configuration Form" in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Help for Administrators*.

   Alternatively, use the command-line interface to configure QA probes as described in "Configuring QA Probes Using nmsqaprobeconfig.ovpl Command" in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Help for Administrators*.

6. In the NNMi console, set thresholds on QA probes as described in "Adding New Threshold Settings Using the Threshold Configuration Form" in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Help for Administrators*.

Task 5: Install the NNM iSPI Performance for Traffic Master Collector

Prerequisites:

- NNMi must be installed on the NNMi management server.
- NPS must be installed on the NPS server.

To install and configure the NNM iSPI Performance for Traffic master collector, follow these steps:

1. On the NNMi management server, install the NNM iSPI Performance for Traffic extension as described in "Installing the HP NNMi Extension for iSPI Performance for Traffic" of the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.
2. Verify that the Traffic Master server meets the requirements listed in Table 9 on page 20.
3. On the Traffic Master server, install the NNM iSPI Performance for Traffic master collector as described in "Installing the Master Collector" of the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.

Task 6: Install and Configure the NNM iSPI Performance for Traffic Leaf Collector

Prerequisites:

- NNMi must be installed on the NNMi management server.
- NPS must be installed on the NPS server.
- The NNM iSPI Performance for Traffic master collector must be installed on the Traffic Master server.

To install and configure the NNM iSPI Performance for Traffic leaf collector, follow these steps:

1. Verify that the Traffic Leaf server meets the requirements listed in Table 10 on page 21.
2. On the Traffic Leaf server, install the NNM iSPI Performance for Traffic leaf collector as described in "Installing the Leaf Collector" of the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.
3. On the Traffic Master and Traffic Leaf servers, complete the steps described in "Post-Installation Tasks" in the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.
4. In the NNMi console, configure the NNM iSPI Performance for Traffic leaf collector systems and instances. Also configure the NNM iSPI Performance for Traffic master collector. For information, see "Configuring the NNM iSPI Performance for Traffic" in the NNM iSPI Performance for Traffic help.
5. For flow-enabled interfaces, enable the flow protocol to send flow records to the NNM iSPI Performance for Traffic leaf collector.

Task 7: Install and Configure NNM iSPI NET

Prerequisite: NNMi must be installed on the NNMi management server.

To install and configure NNM iSPI NET, follow these steps:

1. Verify that the NNM iSPI NET Diagnostics server meets the requirements listed in Table 11 on page 22.
2. On the NNM iSPI NET Diagnostics server, install NNM iSPI NET as described in "Installing the NNM iSPI NET Diagnostics Server and Diagnostic Flows" in the *HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*.

   The installation runs for about one hour without interaction.

3. In the NNMi console, specify device credentials for running diagnostic flows as described in "NNMi Management Server Preparation" in the *HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*.
4. In the NNMi console, configure NNM iSPI NET diagnostics on one or more NNMi incidents. For information, see "NNM iSPI NET Diagnostics" in the *HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*.

Task 8: Install and Configure NA

To install and configure NA, follow these steps:

1. Verify that the NA server meets the requirements listed in Table 7 on page 18.
2. On the NA server, install NA as described in "Installing NA" in the *HP Network Automation Installation and Upgrade Guide*.
3. On the NA server, install the most recent driver pack as described in "Installing the Latest NA Driver Pack" in the *HP Network Automation Installation and Upgrade Guide*.
4. Configure NA device password rules. For information, see "Creating Device Password Rules" in the *HP Network Automation User Guide*.
5. Configure NA device configurations. For information, see "Managing Device Configurations" in the *HP Network Automation User Guide*.
6. Configure NA device policies. For information, see "Managing Policy Assurance" in the *HP Network Automation User Guide*.

Task 9: Configure the HP NNMi—HP NA Integration

Prerequisites:

- NNMi must be installed on the NNMi management server.
- NA must be installed on the NA server.

To configure the HP NNMi—HP NA integration, follow these steps:

1. In the NNMi console, configure the HP NNMi—HP NA integration as described in "New Integration Configuration" in the *HP Network Node Manager i Software—HP Network Automation Integration Guide*.
   - On the HP NNMi–HP NA Integration Configuration form, make the following selections:
     - Leave **Topology Filter Node Group** unset so the integration will synchronize the entire NNMi topology with the NA inventory.
     - Set **Topology Synchronization Interval (hrs)** to a non-zero value.
     - Select the **Discover Device Drivers in NA** check box.
     - Set **NA Connection Check Interval (hrs)** to a non-zero value.
     - Set **Minimum NNMi Role for Analysis Pane Data** to one of the NNMi role levels (*not* to None), as appropriate to your environment.
   - For secure socket layer (SSL) communications between NNMi and NA, be sure to exchange certificates between the two products.
2. Configure single-sign on between NNMi and NA as described in "Configuring Single Sign-On Between NNMi and HP NA" in the *HP Network Node Manager i Software—HP Network Automation Integration Guide*.

Verify the HP NNMi–HP NA Integration

To verify that the HP NNMi–HP NA integration is correctly enabled, follow these steps:

1. Log on to the NNMi console as a user with the Administrator role.
2. In the NNMi console, verify that the NA SNMP trap incident configurations are in place:
   a. Open the SNMP Trap Configurations view (**Configuration > Incidents > SNMP Trap Configurations**).
   b. Locate the trap definitions for named **NASnmpTrapv1** and **NASnmpTrapv2**.
3. Log on to NA as a user with administrator privileges.
4. In the NA console, verify that the NA inventory matches the NNMi topology:
   a. In the menu at the top of the Home page, select **Devices > Inventory**.
   b. Confirm that all devices listed in NNMi were imported to NA.

   If you specified a node group for the **Topology Filter Node Group** setting, only the devices in that node group should be imported to NA.
5. In the NA console, click **Admin > 3rd Party Integrations > NNM Integration Connection Test**.

   A success message appears.

   If an error message appears, confirm that you configured the integration correctly or contact your support representative.

License ANM

The permanent license keys for NNMi and the NNM iSPIs are tied to the IP address of the NNMi management server.

The permanent license key for NA is tied to the IP address of the NA server.

To license ANM, follow these steps:

1. On the NNMi management server, install the following license keys on the NNMi management server:
   - One or more NNMi license keys as needed to enable management of all nodes in your network. For instructions, see "Licensing NNMi" in the *HP Network Node Manager i Software Interactive Installation Guide*.
   - One NNM iSPI NET license key. For instructions, see "License NNM iSPI NET" in the *HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*.
   - One or more NNM iSPI Performance for Metrics license keys as needed to enable performance reporting of all nodes in your network. For instructions, see "Licensing for NNM iSPI Performance" in the *HP Network Node Manager iSPI Performance for Metrics Software Installation Guide*.
   - One or more iSPI Points license key; this license key applies to all of the NNM iSPIs except for NNM iSPI NET and NNM iSPI Performance for Metrics. Ensure that you have enough iSPI points for your use of these NNM iSPIs. For information about how iSPI points accumulate and instructions on installing the license keys, see the following documentation:
     - "License-Related Information" in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Installation Guide*.
     - "Licensing" in the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.
     - "License-related Information" in the *HP Network Node Manager iSPI for IP Multicast Software Installation Guide*.
     - "License Information" in the *HP Network Node Manager iSPI for IP Telephony Software Installation Guide*.
     - "License-Related Information" in the *HP Network Node Manager iSPI for MPLS Software Installation Guide*.
   - One Collector Connection Software LTU license key for each NNM iSPI Performance for Traffic leaf collector. For instructions, see "Licensing" in the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.
2. On the NA server, install one NA license key. For instructions, see "Obtain and Deploy an NA License" in the *HP Network Automation Installation and Upgrade Guide*.

Upgrade from ANM 9.10 to ANM 9.20

This section outlines the procedure for upgrading ANM for the example deployment architecture of Figure 1 on page 9. For additional information, see the product documentation, which is available from the HP manuals web site as described in Product Documentation on page 23.

To prevent data loss, observe the following:

- NNM iSPI Performance for QA and NNM iSPI Performance for Traffic must be at version 9.11 (9.1x Patch 1) before completing this procedure.
- If the NNM iSPI Performance for Traffic master or leaf is installed on the NNMi management server, NNMi must be at 9.1x Patch 3 (or later) *and* NNM iSPI Performance for Traffic must be at 9.1x Patch 2 (or later) before completing this procedure.

If any of NPS, NNM iSPI Performance for Metrics, or the NNM iSPI Performance for Traffic master or leaf is installed on the NNMi management server, the upgrade procedure includes additional steps. Follow the upgrade procedures in those product documents.

To upgrade from ANM 9.10 to ANM 9.20, follow these steps:

1. On the NPS server, back up all NPS data by running the following command:
   - *Windows*:

     %NPSInstallDir%\bin\backup.ovpl -b <*dir*>
   - *UNIX*:

     /opt/OV/NNMPerformanceSPI/bin/backup.ovpl -b <*dir*>

   If you created Report Views for scheduled reports, the views will be saved during the upgrade. Schedules, jobs, and queries made using Query Studio will also be saved. Shortcuts and other object types, however, will not be saved. Check the log entries in the `Migration.log` file, which can be found in the log directory, to see the results of the upgrade.
2. On the NPS server, stop the NPS processes by running the following command:
   - *Windows*:

     %NPSInstallDir%\bin\stopALL.ovpl
   - *UNIX*:

     /opt/OV/NNMPerformanceSPI/bin/stopALL.ovpl
3. On the Traffic Leaf server, stop the leaf collector by running the following command:
   - *Windows*:

     %TrafficInstallDir%\nonOV\traffic-leaf\bin\nmstrafficleafstop.ovpl
   - *UNIX*:

     /opt/OV/traffic-leaf/nonOV/bin/nmstrafficleafstop.ovpl

4 On the Traffic Master server, stop the master collector by running the following command:

- *Windows*:

  ```
  %TrafficInstallDir%\nonOV\traffic-master\bin\
  nmstrafficmasterstop.ovpl
  ```

- *UNIX*:

  ```
  /opt/OV/traffic-master/nonOV/bin/nmstrafficmasterstop.ovpl
  ```

5 Upgrade NNMi as described in "Upgrading from NNMi 9.0x or 9.1x" in the *HP Network Node Manager i Software Upgrade Reference*.

6 Upgrade NPS and NNM iSPI Performance for Metrics as described in "Upgrading NPS on the Dedicated Server" in the *HP Network Node Manager iSPI Performance for Metrics Software Installation Guide*.

When the NPS Configuration Utility window appears, click **Exit** to cancel.

7 Upgrade NNM iSPI Performance for QA as described in "Upgrading the NNM iSPI Performance for QA" in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Installation Guide*.

8 Upgrade NNM iSPI Performance for Traffic as described in "Upgrade the NNM iSPI Performance for Traffic" in the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.

9 On the NPS server, start the NPS processes by running the following command:

- *Windows*:

  ```
  %NPSInstallDir%\bin\startALL.ovpl
  ```

- *UNIX*:

  ```
  /opt/OV/NNMPerformanceSPI/bin/startALL.ovpl
  ```

10 Upgrade NNM iSPI NET as described in "Upgrading from NNM iSPI NET diagnostics server version 9.10" the *HP NNM iSPI Network Engineering Toolset Software Release Notes*.

11 Upgrade NA as described in "Upgrading to NA 9.20 from a Different System" or "Upgrading to NA 9.20 on the Same System" in the *HP Network Automation Installation and Upgrade Guide*.

12 In the NNMi console, upgrade the HP NNMi—HP NA integration as described in "Integration Configuration Upgraded from NNMi 9.1x to NNMi 9.20" in the *HP Network Node Manager i Software—HP Network Automation Integration Guide*.

For secure socket layer (SSL) communications between NNMi and NA, be sure to exchange certificates between the two products.

3 Configuring the ANM Example Scenarios

This chapter outlines the process for configuring the ANM example scenarios. It assumes that ANM is configured as described in Chapter 2, Configuring ANM.

It contains the following topics:

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.

Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- Configure the Device to Send syslog Messages to NA on page 40.
- An NA device configuration policy must be applied to the device.
- The ANM operator must have permission in NA to view and modify the device configuration.
- Customize the NA SNMP Trap Incidents on page 40.
- Set NA to Run the Check Policy Compliance Task When a Device Configuration Changes on page 41.
- Configure NA to Send SNMP Traps to NNMi When a Policy Compliance Check Fails on page 41.

Configure the Device to Send syslog Messages to NA

1. In the NA console, click **Tasks > New Task > Configure Syslog**.
2. On the New Task/Template –Configure Syslog page, do the following:
   a. Set *Applies to* to the device.
   b. Under Scheduling Options, set Recurring Options to Periodically, and then specify an appropriate interval.
   c. Click **Save**.

Customize the NA SNMP Trap Incidents

In the NNMi console, the NASnmpTrapv1 and NASnmpTrapv2 incident configurations convert the SNMP traps sent by NA into incidents that NNMi can display and process.

If you want all traps sent by NA to NNMi to appear in the key incident views in the NNMi console, set the NASnmpTrapv1 and NASnmpTrapv2 incident configurations to be root cause.

This action sets all NA traps to be root cause regardless of content.

In the NNMi console, edit the NASnmpTrapv1 and NASnmpTrapv2 incident configurations to be root cause. This change sets all traps sent by the NA to NNMi to appear in the key incident views in the NNMi console.

Follow these steps:

1. In the NNMi console, in the Configuration workspace, click **Incidents > SNMP Trap Configurations**.
2. Edit each of the NASnmpTrapv1 and NASnmpTrapv2 incident configurations to select the **Root Cause** check box.

Set NA to Run the Check Policy Compliance Task When a Device Configuration Changes

In the NA console, on the Event Notification & Response Rules page, create a new rule that checks for policy compliance whenever a device's configuration changes.

1. In the NA console, click **Admin > Event Notification & Response Rules**.
2. On the Event Notification & Response Rules page, click the **New Event Notification & Response Rules** link at the top of the page.
3. On the New Event Notification & Response Rule page, do the following:
   a. Enter a rule name.
   b. Set *To take this action* to **Run Task**.
   c. Set *When the following events occur* to **Device Configuration Change**.
   d. Set *And then run this task* to **Check Policy Compliance**.
4. On the New Task/Template – Check Policy Compliance page, click **Done**.
5. On the Edit Event Notification & Response Rule page, click **Save**.

Configure NA to Send SNMP Traps to NNMi When a Policy Compliance Check Fails

In the NA console, on the Event Notification & Response Rules page, update the NA/NNM Integration via SNMP Traps rule to send SNMP traps when policy non-compliance events occur.

1. In the NA console, click **Admin > Event Notification & Response Rules**.
2. On the Event Notification & Response Rules page, locate the NA/NNM Integration via SNMP Traps rule, and then click the **Edit** link in this row.
3. On the Edit Event Notification & Response Rule page, do the following:
   a. In the *When the following events occur* list, verify that **Policy Non-Compliance** is selected.
   b. If necessary, **Ctrl-click** this row to add it to the selection list.
   c. Note the value set for SNMP Version, and change this value if appropriate.
   d. Click **Save**.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

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, in the analysis pane, open the **History of Node Configuration** tab, and then click **Compare to previous** for the most recent row to see a comparison of the current device configuration with the previous device configuration.

4 In the NA console, 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.

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.

Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- The device must be configured to send traps to the NNMi management server.
- OSPF traps must be enabled on the device.
- The ANM operator must have permission in NA to view and modify the device configuration.

Enable the OSPFNbrStateChange Incident

In the NNMi console, enable the OSPFNbrStateChange incident configuration.

1. In the NNMi console, in the Configuration workspace, click **Incidents > SNMP Trap Configurations**.
2. Open the OSPFNbrStateChange incident configuration.
3. Select the **Enabled** check box.
4. Save the configuration.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

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 the NA console, view the diagnostic report of the OSPF neighbor router and observe the ACL configuration error.
5. In the NA console, 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.

Scenario 3: Verify traffic flow through the network after a device configuration change

As part of completing an approved device configuration change, a network engineer wants proof that the change has the correct impact on application traffic. ANM can display graphs of the traffic between two network devices. A network engineer can view these graphs before and after a device configuration change to validate the effectiveness of that change.

Scenario Prerequisites

- The devices must be in the NNMi topology.
- The NetFlow or sFlow protocol must be enabled on at least one device in the area of the network.

  Alternatively, you can use a traffic flow export. The NetFlow protocol must be configured to send the NetFlow export to the NNM iSPI Performance for Traffic leaf collector server.

No additional configuration is needed to enable this scenario.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

1. In the NNMi console, open the traffic path view (**Actions > Traffic Maps > Traffic Path View**) representing the source and destination nodes for the traffic flow in the area of the network to be re-engineered.
2. Select the NetFlow-enabled interface, and then, in the analysis pane, open the **Performance** tab.

   For comparison purposes, take a screen capture of the traffic graphs.
3. Change the network configuration in a way that impacts traffic routing.
4. To verify that traffic has reconverged after the network change, wait 10 minutes, and then refresh the **Performance** tab to see the updated traffic graphs.

Scenario 4: 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.

Scenario Prerequisites

- The area of the network to be re-addressed must be in the NNMi topology and the NA inventory.
- Prepare a list of available IPv6 addresses.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

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.
5. In the NNMi console, export the IP Addresses inventory view to CSV format.
6. Compare the configured IPv6 addresses to the planned IPv6 addresses.

Scenario 5: 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.

Scenario Prerequisites

- The devices must be in the NNMi topology and the NA inventory.
- Performance monitoring and interface utilization thresholds must be enabled and configured in NNMi for the interfaces.
- The NetFlow or sFlow protocol must be enabled on at least one device in the area of the network.

  Alternatively, you can use a traffic flow export. The NetFlow protocol must be configured to send the NetFlow export to the NNM iSPI Performance for Traffic leaf collector server.
- Enable the InterfaceInputUtilizationHigh and InterfaceInputUtilizationLow Incidents on page 46.

Enable the InterfaceInputUtilizationHigh and InterfaceInputUtilizationLow Incidents

In the NNMi console, enable the InterfaceInputUtilizationHigh and InterfaceInputUtilizationLow incident configurations.

1. In the NNMi console, in the Configuration workspace, click **Incidents > Management Event Configurations**.
2. Open the InterfaceInputUtilizationHigh incident configuration.
3. Select the **Enabled** check box.
4. Save the configuration.
5. Repeat step 2 through step 4 for the InterfaceInputUtilizationLow incident configuration.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

1. NNMi generates a management event incident to indicate that interface utilization is beyond acceptable boundaries for an important network interface.
2. In the traffic inventory, locate the source interface of the NNMi incident and, in the analysis pane, view the **Top Apps-In** tab.

   This tab displays a pie chart of the applications generating the most traffic. The chart 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.

Scenario 6: 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.

Scenario Prerequisites

- The edge router must be in the NNMi topology.
- IP SLA tests must be configured on the edge router.
- The IP SLA tests must be in the NNM iSPI Performance for QA inventory.
- Thresholds must be configured for the metrics of the IP SLA tests.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

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. From the NNMi incident, in the analysis pane, open the **Performance** tab to view the QA graph to show recent values of the IP SLA test.
3. Notify the ISP of the problem.

Scenario 7: 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.

Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- An NNM iSPI Performance for Traffic site must be defined to for the IP addresses of the web site locations.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

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. NNM iSPI Performance for Traffic generates a management incident to indicate a high volume of data regards to HTTP traffic toward a NNM iSPI Performance for Traffic site that represents the web site locations.
3. From the NNM iSPI Performance for Traffic incident, in the analysis pane, open the **Top Apps - In** tab for the interface identified in the incident.

   This tab displays a pie chart of the applications generating the most traffic.
4. From the Traffic Reporting Interfaces table in the Traffic Analysis workspace, open the interface mentioned in the NNM iSPI Performance for Traffic incident.

   The **Top 5 Sources** and **Top 5 Destinations** tabs show that the high interface utilization comes from a few hosts.
5. Determine that the web site URL is being loaded with many HTTP requests. The requests seem to be an attack on the web site.
6. In the NA console, modify the ACLs on the device hosting the web server to deny traffic from the sources of the attack.
7. Network traffic across the interface returns to acceptable levels, and the interface utilization incident automatically closes in the NNMi console.

Scenario 8: 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.

Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- Performance monitoring and thresholds must be enabled and configured in NNMi for the interface.
- Enable the InterfaceInputErrorRateHigh and InterfaceInputUtilizationHigh Incidents on page 50.

Enable the InterfaceInputErrorRateHigh and InterfaceInputUtilizationHigh Incidents

In the NNMi console, enable the InterfaceInputErrorRateHigh and InterfaceInputUtilizationHigh incident configurations.

1. In the NNMi console, in the Configuration workspace, click **Incidents > Management Event Configurations**.
2. Open the InterfaceInputErrorRateHigh incident configuration.
3. Select the **Enabled** check box.
4. Save the configuration.
5. Repeat step 2 through step 4 for the InterfaceInputUtilizationHigh incident configuration.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

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 the NA console, 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.

Scenario 9: Prevent incidents from devices undergoing maintenance

When a device becomes unavailable, the network monitoring solution creates alarms regarding that device's unavailability. Network operators then spend time identifying the cause of the alarms. ANM can automate the process of identifying devices that are undergoing maintenance and prevent unnecessary incidents regarding the status of those devices.

Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- Configure NA to Send Out-of-Service Events on page 52.
- The ANM operator must have permission in NA to view and modify the device configuration.

Configure NA to Send Out-of-Service Events

1. In the NA console, click **Admin > Administrative Settings > 3rd Party Integrations**.
2. On the Administrative Settings–3rd Party Integrations page, do the following:
   a. Verify that *NNMi-NA Integration Level* is set to either **Complete** or **Partial**.
   b. In the *Tasks that Place Device Out-of-Service* list, select the NA tasks that should cause NNMi to change the management mode to NOT MANAGED.
   c. *Optional*. Change the default settings for the other options under NNMi Integration Out-of-Service Settings.
   d. Click **Save**.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

1. From the NA console, initiate a device maintenance task. As NA starts the task, NA sends an out-of-service event to NNMi.
2. NNMi sets the management mode of the node to OUT OF SERVICE. NNMi does not generate incidents for this node while it is out of service.
3. After the device maintenance task completes, NA waits for the out-of-service completion delay time. Then, NA sends an in-service event to NNMi.
4. NNMi returns the management mode of the node to the original state.

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 9.20, May 2013

Document title: *ANM Configuration Guide*

Feedback: