HP Network Node Manager i Software

NNMi Network Bandwidth Utilization
(Standalone and Global Network Management Environments)

Release 9.00

This document provides examples of network bandwidth utilization for NNMi 9.00 in both standalone environments (one NNMi management server) and Global Network Management environments (multiple NNMi management servers). Measurements were averaged from multiple samples of live environments. Performance in your network environment may vary.

The large majority of traffic generated by NNMi is SNMP and ICMP. In addition, NNMi's Global Network Management feature uses TCP for communication between Regional Managers and Global Managers. Even though other network traffic (for example, ARP, RARP, etc.) is likely to increase by using NNMi or any other network management software, the scenarios in this document only measure traffic generated directly by NNMi.

If you have questions about the NNMi features described in this document (Communication configuration settings, Discovery configuration settings, Monitoring configuration settings, Incident configuration settings, Global Network Management, and Node Groups), see the NNMi online Help for details. A PDF version of the NNMi online Help is available at: http://h20230.www2.hp.com/selfsolve/manuals

CONTENTS

Introduction

This white paper documents the amount of network traffic generated by NNMi during different periods of common use. Use this information to extrapolate how much network traffic may be generated by NNMi in your network environment. NNMi is used in many different ways, and each network is different (performance in your network environment may vary).

The first section (Standalone NNMi Network Utilization) documents the network utilization of one NNMi management server. The second section (Global Network Management Utilization) documents the amount of network traffic generated for the Global Network Management feature. The Global Network Management feature of NNMi allows a Global Manager (NNMi management server) to display data from several Regional Managers (NNMi management servers). The Regional Managers forward the data to the Global Manager.

Standalone NNMi Network Utilization

Standalone System – Initial Discovery

This scenario measured the volume of SNMP traffic generated on one NNMi management server during the initial discovery cycle. The time required for this initial discovery cycle depends on your network speed, the number and type of devices in your network, and the hardware on which NNMi is installed. The NNMi management server was configured as described in the following table.

Configuration settings on the NNMi management server:

Configuration Workspace	Specific Settings	Objects
Communication Configuration	Communication Region (one defined): ICMP Settings: (1) ☐ **Enable ICMP Communication** (2) **ICMP Timeout** set to 5 seconds Default SNMPv1/v2 Community Strings: (1) Only one Community String configured	
Discovery Configuration	Ping Sweep: none Auto-Discovery Rules: none Subnet Connection Rules: none Excluded IP Addresses: none Excluded Interfaces: none **Discovery Seeds**: 1500	1500 Nodes
Monitoring Configuration	Disable all current polling configurations: **Enable State Polling:** ☐	
Incident Configuration	SNMP Traps: (none)	

This scenario measured the SNMP traffic generated by NNMi during the initial discovery of 1500 seeded nodes.

- No traps were received or generated by NNMi during this scenario.
- All NNMi Monitoring (SNMP and ICMP polling) was disabled to ensure that this scenario measured only discovery traffic.

Results: Averages of 521.421 SNMP packets per second and 1.136 Megabits per second.

Standalone System – Rediscovery

This scenario measured the volume of SNMP traffic generated on one NNMi management server during the rediscovery cycle. The time required for this rediscovery cycle depends on your network speed, the number and type of devices in your network, and the hardware on which NNMi is installed.

The NNMi management server was configured as described in the following table.

Configuration settings on the NNMi management server:

Configuration Workspace	Specific Settings	Objects
Communication Configuration	Communication Region (one defined): ICMP Settings: (1) ☐ **Enable ICMP Communication** (2) **ICMP Timeout** set to 5 seconds Default SNMPv1/v2 Community Strings: (1) Only one Community String configured	
Discovery Configuration	Ping Sweep: none Auto-Discovery Rules: none Subnet Connection Rules: none Excluded IP Addresses: none Excluded Interfaces: none **Discovery Seeds**: 1500	1500 Nodes
Monitoring Configuration	Disable all current polling configurations: **Enable State Polling:** ☐	
Incident Configuration	SNMP Traps: (none)	

This scenario measured the SNMP traffic during the rediscovery of 1500 seeded nodes. This measurement was taken during the first rediscovery cycle which will typically use the most bandwidth. Over time, rediscovery spreads out over your configured rediscovery period and average bandwidth for rediscovery decreases.

Results: Averages of 526.925 SNMP packets per second and 1.237 Megabits per second.

Standalone System – SNMP Status Polling

This scenario measured the volume of SNMP traffic generated on one NNMi management server during the device status polling cycle. The NNMi management server was configured as described in the following table.

Configuration settings on the NNMi management server:

Configuration Workspace	Specific Settings	Objects
Communication Configuration	Region: ICMP Settings: (1) ☐ **Enable ICMP Communication** (2) **ICMP Timeout** set to 5 seconds Default SNMPv1/v2 Community Strings: (1) Only one Community String configured	
Discovery Configuration	**Rediscovery Interval** set to 10 days (to prevent rediscovery cycles during the scenario)	
Monitoring Configuration	Default Fault Monitoring: (1) ☐ **Enable ICMP Management Address Polling**	

	(2) ☐ **Enable ICMP Fault Polling** (3) ☑ **Enable SNMP Interface Fault Polling** (4) ☐ **Enable Card Fault Polling** (5) ☐ **Enable Node Component Fault Polling** (6) **Fault Polling Interval** set to 5 minutes	11,000 Interfaces
	Default Performance Monitoring: (1) ☐ Enable SNMP Interface Performance Polling (2) **Performance Polling Interval** set to 5 minutes	
Incident Configuration	SNMP Traps: none	

This scenario measured the SNMP traffic generated by NNMi during the status polling segment of the Monitoring cycle for 11,000 polled interface objects.

- No traps were received or generated by NNMi during this scenario.
- All ICMP polling was disabled.

Results: Averages of 27.054 SNMP packets per second and 0.006 Megabits per second.

Standalone System – Performance Polling

This scenario measured the volume of SNMP traffic generated on one NNMi management server during the device performance polling cycle. The NNMi management server was configured as described in the following table.

Configuration settings on the NNMi management server:

Configuration Workspace	Specific Settings	Objects
Communication Configuration	Region: ICMP Settings: (1) ☐ **Enable ICMP Communication** (2) **ICMP Timeout** set to 5 seconds Default SNMPv1/v2 Community Strings: (1) Only one Community String configured	
Discovery Configuration	**Rediscovery Interval** set to 10 days (to prevent rediscovery cycles during the test)	
Monitoring Configuration	Default Fault Monitoring: (1) ☐ **Enable ICMP Management Address Polling** (2) ☐ **Enable ICMP Fault Polling** (3) ☐ **Enable SNMP Interface Fault Polling** (4) ☐ **Enable Card Fault Polling** (5) ☐ **Enable Node Component Fault Polling** (6) **Fault Polling Interval** set to 5 minutes	
	Default Performance Monitoring: (1) ☑ Enable SNMP Interface Performance Polling (2) **Performance Polling Interval** set to 5 minutes	11,000 Interfaces
Incident Configuration	SNMP Traps: none	

This scenario measured the SNMP traffic generated by NNMi during the performance polling segment of the Monitoring cycle for 11,000 polled interface objects (same interfaces from previous scenario).

- No traps were received or generated by NNMi during this scenario.
- All ICMP polling was disabled.

Results: Averages of 100.113 SNMP packets per second and 0.0371 Megabits per second.

Standalone System – ICMP Status Polling

This scenario measured the volume of ICMP traffic generated on one NNMi management server during the ICMP fault polling cycle. The NNMi management server was configured as described in the following table.

Configuration settings on the NNMi management server:

Configuration Workspace	Specific Settings	Objects
Communication Configuration	Region: ICMP Settings: (1) ☑ **Enable ICMP Communication** (2) **ICMP Timeout** set to 5 seconds Default SNMPv1/v2 Community Strings: (1) Only one Community String configured	1808 addresses
Discovery Configuration	**Rediscovery Interval** set to 10 days (to prevent rediscovery cycles during the test)	
Monitoring Configuration	Default Fault Monitoring: (1) ☐ **Enable ICMP Management Address Polling** (2) ☑ **Enable ICMP Fault Polling** (3) ☐ **Enable SNMP Interface Fault Polling** (4) ☐ **Enable Card Fault Polling** (5) ☐ **Enable Node Component Fault Polling** (6) **Fault Polling Interval** set to 5 minutes	1808 addresses
	Default Performance Monitoring: (1) ☐ Enable SNMP Interface Performance Polling (2) **Performance Polling Interval** set to 5 minutes	
Incident Configuration	SNMP Traps: none	

This scenario measured the ICMP traffic generated by NNMi during ICMP fault polling segment of the Monitoring cycle for 1808 polled addresses.

- No traps were received or generated by NNMi during this scenario.
- All SNMP polling was disabled.

Results: Averages of 12.207 ICMP packets per second and 0.001 Megabits per second.

Standalone System – Traps

This scenario measured the volume of SNMP traffic generated on one NNMi management server by a steady-state trap load. The NNMi management server was configured as described in the following table.

Configuration settings on the NNMi management server:

Configuration Workspace	Specific Settings	Object
Communication Configuration	Region: ICMP Settings: (1) ☐ **Enable ICMP Communication** (2) **ICMP Timeout** set to 5 seconds Default SNMPv1/v2 Community Strings: (1) Only one Community String configured	
Discovery Configuration	**Rediscovery Interval** set to 10 days (to prevent rediscovery cycles during the test)	1500 nodes
Monitoring Configuration	Default Fault Monitoring:	

	(1) ☐ **Enable ICMP Management Address Polling** (2) ☑ **Enable ICMP Fault Polling** (3) ☑ **Enable SNMP Interface Fault Polling** (4) ☐ **Enable Card Fault Polling** (5) ☐ **Enable Node Component Fault Polling** (6) **Fault Polling Interval** set to 5 minutes	1,808 IP addresses 11,000 Interfaces
	Default Performance Monitoring: (1) ☐ Enable SNMP Interface Performance Polling (2) **Performance Polling Interval** set to 5 minutes	
Incident Configuration	SNMP Traps: (1) SNMP link up (2) SNMP link down (3) Cisco link up (4) Cisco link down	

This scenario measured the SNMP traffic generated by NNMi under a steady state trap load. Our test tools generated a link down/up trap at a rate of 10 per second. These 10 traps per second were randomly sent to NNMi from various SNMP agents in the discovered environment.

- Link up/down traps cause the following NNMi actions (*) which result in additional ICMP and SNMP traffic:
  - Rediscovery of each node that sent a link down trap
  - Immediate status poll of each interface that sent a trap
- Some trap deduplication occurred using NNMi default configurations, so not every trap caused the secondary NNMi actions described in the previous bullet(*). (See the NNMi online help for information about the deduplication feature.)

Results: Averages of 36.777 SNMP packets per second and 0.008 Megabits per second.

Standalone System – Custom Polling

This scenario measured the volume of SNMP traffic generated on one NNMi management server during a custom poller cycle. The NNMi management server was configured as described in the following table.

Configuration settings on the NNMi management server:

Configuration Workspace	Specific Settings	Object
Communication Configuration	Region: ICMP Settings: (1) ☐ **Enable ICMP Communication** (2) **ICMP Timeout** set to 5 seconds Default SNMPv1/v2 Community Strings: (1) Only one Community String configured	
Discovery Configuration	**Rediscovery Interval** set to 10 days so that no discovery would occur	1500 nodes
Monitoring Configuration	Default Fault Monitoring: (1) ☐ **Enable ICMP Management Address Polling** (2) ☐ **Enable ICMP Fault Polling** (3) ☐ **Enable SNMP Interface Fault Polling** (4) ☐ **Enable Card Fault Polling** (5) ☐ **Enable Node Component Fault Polling** (6) **Fault Polling Interval** set to 5 minutes	
	Default Performance Monitoring:	

	(1) ☐ Enable SNMP Interface Performance Polling (2) **Performance Polling Interval** set to 5 minutes	
Incident Configuration	SNMP Traps: none	
Custom Poller Configuration	☑ Enable Custom Poller One Custom Poller Collection defined for if%util	11000 interfaces

This scenario measured the SNMP traffic generated by NNMi during the Custom Polling cycle for 11,000 polled interfaces (SNMP if%util was configured as the Custom Poll).

- No traps were received or generated by NNMi during this scenario.
- All SNMP and ICMP polling other than Custom Polling was disabled.

Results: Averages of 15.647 SNMP packets per second and 0.005 Megabits per second.

Global Network Management Utilization

Configuration

The Global Network Management feature of NNMi allows a Global Manager (NNMi management server) to display data from up to 10 Regional Managers (NNMi management servers).

To enable Global Network Management:

The NNMi administrator for the Global Manager does the following:

(1) In the Configuration workspace, open the Global Network Management form.
(2) On the Regional Manager Connection tab, establish settings for each Regional Manager.
(3) *Optional*. Configure special Incident Configuration settings above and beyond the default configurations provided by NNMi. For this scenario only default Incident Configuration settings were used.

The NNMi Administrator for each Regional Manager has the *option* of limiting data that is forwarded to the Global Manager by assigning *one Node Group* as the Forwarding Filter (Configuration workspace, Global Network Management form, Forwarding Filter tab). For this scenario, traffic from Regional Managers was not limited to any particular Node Groups.

Traffic Measured for the Global Network Management Scenarios:

- Traffic was measured on the Global Manager. The Global Manager was not responsible for discovering or monitoring any nodes (only responsible for displaying data received from the Regional Managers).

- Six Regional Managers (each managing from 6,000 to 25,000 nodes) forwarded data to the Global Manager.

- The Global Manager's database included a cumulative 65,000 nodes (combined from all Regional Managers).

Global Network Management Discovery Scenario

This scenario measured the volume of traffic generated during the period directly after configuring one Regional Manager to forward data to the Global Manager. This is the traffic badwidth required to send all of the topology information for 25,000 nodes from the Regional Manager to the Global Manager. The time required for this initial discovery cycle depends on your network speed, the number and type of devices in your network, and the hardware on which NNMi is installed.

Configuration Settings on the Global Manager (NNMi management server)

Configuration Workspace	Specific Settings	Objects
Global Network Management	Regional Manager Connections (one configured)	1 Regional Manager
Incident Configuration	SNMP Traps: none	

Initial discovery on the Regional Manager was completed prior to this scenario. No other Regional Managers were configured to report to the Global Manager during this scenario.

Results: Combined traffic forwarded to the Global Manager averaged 241 TCP packets per second and 1.46 megabits per second.

Global Network Management Steady-State Scenario

This scenario measured the TCP traffic volume received by the Global Manager from the six Regional Managers. The six Regional Managers were configured as described in the following table.

Configuration Settings on the Six Regional Managers (NNMi management servers)

Configuration Workspace	Specific Settings on Regional Managers (each with these settings)	Cumulative Object Count forwarded Global Manager
Discovery Configuration	**Rediscovery Interval** on all Regional Managers was set to 24 hours	65,000 nodes
Monitoring Configuration	Default Fault Monitoring: (1) ☑ **Enable ICMP Management Address Polling** (2) ☑ **Enable ICMP Fault Polling** (3) ☑ **Enable SNMP Interface Fault Polling** (4) ☑ **Enable Card Fault Polling** (5) ☑ **Enable Node Component Fault Polling** (6) **Fault Polling Interval** set to 5 minutes	30,000 IP addresses -and- 420,000 Interfaces -and- 500,000 Node Components
	Default Performance Monitoring: (1) ☑ Enable SNMP Interface Performance Polling (2) **Performance Polling Interval** set to 5 minutes	420,000 Interfaces
Incident Configuration	SNMP Traps: none	

During this scenario the Global Manager had already received all the topology data from the 6 Regional Managers. TCP traffic was only generated for updates from the 6 Regional Managers.

Results: Combined traffic forwarded to the Global Manager averaged 99 TCP packets per second and 1.15 megabits per second.

Global Network Management Heavy-Load Scenario

This scenario measured the TCP traffic volume received by the Global Manager from the six Regional Managers:

- One of the Regional Managers was configured to generate heavy traffic (1 minute polling interval).
- Five of the Regional Managers were configured for normal traffic (5 minute polling interval)

All the Regional Manager configuration settings are described in the following tables. The only differences in the Regional Manager settings are the interval settings noted in red.

HEAVY TRAFFIC CONFIGURATION SETTINGS:
Configuration Settings on *One* of the Regional Managers (NNMi management server)

Configuration Workspace	**Specific Settings on Regional Managers (each with these settings)**	**Cumulative Object Count forwarded Global Manager**
Discovery Configuration	**Rediscovery Interval** was set to 24 hours	10,000 Nodes
Monitoring Configuration	Default Fault Monitoring: (1) **Enable ICMP Management Address Polling** (2) ☑ **Enable ICMP Fault Polling** (3) ☑ **Enable SNMP Interface Fault Polling** (4) ☑ **Enable Card Fault Polling** (5) ☑ **Enable Node Component Fault Polling** (6) **Fault Polling Interval** set to 1 minute	5,000 IP addresses -and- 80,000 Interfaces -and- 50,000 Node Components
	Default Performance Monitoring: (1) ☑ Enable SNMP Interface Performance Polling (2) **Performance Polling Interval** set to 1 minute	80,000 Interfaces
Incident Configuration	SNMP Traps: none	

NORMAL TRAFFIC CONFIGURATION SETTINGS:
Configuration Settings on *Five* of the Regional Managers (NNMi management servers)

Configuration Workspace	**Specific Settings on Regional Managers (each with these settings)**	**Cumulative Object Count forwarded Global Manager**
Discovery Configuration	**Rediscovery Interval** on all Regional Managers was set to 24 hours	55,000 Nodes
Monitoring Configuration	Default Fault Monitoring: (1) **Enable ICMP Management Address Polling** (2) ☑ **Enable ICMP Fault Polling** (3) ☑ **Enable SNMP Interface Fault Polling** (4) ☑ **Enable Card Fault Polling** (5) ☑ **Enable Node Component Fault Polling** (6) **Fault Polling Interval** set to 5 minutes	25,000 IP addresses -and- 340,000 Interfaces -and- 450,000 Node Components
	Default Performance Monitoring: (1) ☑ Enable SNMP Interface Performance Polling	340,000 Interfaces

	(2) **Performance Polling Interval** set to 5 minutes	
Incident Configuration	SNMP Traps: none	

During this scenario, traffic was measured on the Global Manager. (TCP traffic was only generated for updates from the 6 Regional Managers.) During this scenario:

- Heavy Traffic = 80,000 interfaces were fault and performance polled every minute.
- Normal Traffic = 340,000 interfaces were fault and performance polled every 5 minutes.

Results: Combined traffic forwarded to the Global Manager averaged 135 TCP packets per second and 1.66 megabits per second.