



**Hewlett Packard**  
Enterprise

# **HPE Network Node Manager i Software 10.20**

Guidelines to be followed for Network  
Bandwidth Utilization for Standalone and  
Global Network Management  
Environments

# Contents

Network Bandwidth Utilization for NNMi Standalone and Global Network Management Environments.....	3
Introduction.....	3
Standalone NNMi Network Utilization.....	3
Standalone System – Initial Discovery .....	3
Standalone System – Rediscovery.....	4
Standalone System – SNMP Status Polling .....	5
Standalone System – Performance Polling .....	6
Standalone System – ICMP Status Polling.....	6
Standalone System – Traps .....	7
Standalone System – Custom Polling .....	8
NNMi Application Failover Configuration .....	10
Application Failover – Discovery.....	10
Application Failover - Steady State SNMP Polling.....	10
Application Failover - Database Synchronization .....	10
Global Network Management (GNM) Network Utilization Configuration .....	10
GNM - Discovery Scenario .....	11
GNM – Steady State SNMP Polling.....	11
GNM - Heavy Load Fault and Performance Polling.....	12
GNM - Resynchronization Scenario .....	12
We appreciate your feedback! .....	14

# Network Bandwidth Utilization for NNMi Standalone and Global Network Management Environments

This document provides examples of the expected network utilization for the NNMi release 10.0 standalone and Global Network Management environments. When using this document, note the following:

- Use this document as a guideline only.
- The majority of NNMi traffic is SNMP and ICMP.
- The Global Network Management traffic is TCP.
- The scenarios included in this document only measure traffic generated directly by NNMi.
- Other network traffic is likely to increase (for example, ARP and RARP) by using NNMi or any other network management software.

## Introduction

This document describes the amount of network traffic generated by NNMi during different periods of common use. Use this document to determine in general how much network traffic might be used by NNMi in your network. NNMi is used in many ways, and each network is different (performance in your network environment might vary).

The first section (Standalone NNMi Network Utilization) documents network utilization of one NNMi management server. The second section (Global Network Management Network Utilization) documents the amount of network traffic generated in the Global Network Management environment. The third section documents Application Failover scenarios.

## 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.

This test measured utilization during initial discovery of 1,500 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 messaged only discovery traffic.

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: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Communication</b></li> <li>• <b>ICMP Timeout</b> set to 5 seconds</li> </ul> Default SNMPv1/v2 Community Strings: <ul style="list-style-type: none"> <li>• Only one Community String configured</li> </ul>									
Discovery Configuration	<table border="1"> <thead> <tr> <th colspan="2">Schedule Settings</th> </tr> </thead> <tbody> <tr> <td>Ping Sweep</td> <td>none</td> </tr> <tr> <td>Rediscovery Interval</td> <td>10 days</td> </tr> <tr> <td>Auto-Discovery Rules</td> <td>none</td> </tr> </tbody> </table>	Schedule Settings		Ping Sweep	none	Rediscovery Interval	10 days	Auto-Discovery Rules	none	1500 Nodes
Schedule Settings										
Ping Sweep	none									
Rediscovery Interval	10 days									
Auto-Discovery Rules	none									

	Subnet Connection Rules	none
	Excluded IP Addresses	none
	Excluded Interfaces	none
	Discovery Seeds	1500
Monitoring Configuration	Disable all current polling configurations Enable State Polling	
Incident Configuration	SNMP Traps: (none)	

**Results:** Up to 960 packets per second or 2.55 Megabits per second with a total transfer of 192 MB when discovering nodes at a rate of 1500 nodes per 10 minutes. Environments with higher latency will see longer discovery times and lower peak bandwidth but roughly comparable total transfer.

### 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 types of devices on your network, and the hardware on which NNMi is installed.

All polling was disabled during the rediscovery of the 1,500 nodes. This rediscovery scenario measured the utilization of a rediscovery cycle. This measurement was taken during the first rediscovery cycle, which typically uses the most bandwidth. Over time, rediscovery extends over your configured rediscovery period and average bandwidth for rediscovery decreases.

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: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Communication</b></li> <li>• <b>ICMP Timeout</b> set to 5 seconds</li> </ul> Default SNMPv1/v2 Community Strings: <ul style="list-style-type: none"> <li>• Only one Community String configured</li> </ul>	
Discovery Configuration	<b>Schedule Settings</b>	1500 Nodes
	Ping Sweep	none
	Auto-Discovery Rules	none
	Subnet Connection Rules	none
	Excluded IP Addresses	none
	Excluded Interfaces	none
	Discovery Seeds	1500

Monitoring Configuration	Disable all current polling configurations Enable State Polling
Incident Configuration	SNMP Traps: (none)

**Results:** Up to 1378 packets per second or 3.67 Megabits per second with a total transfer of 138 MB when re-discovering nodes at a rate of 1500 nodes per 5 minutes. Environments with higher latency will see longer re-discovery times and lower peak bandwidth but roughly comparable total transfer.

### 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.

This scenario measured utilization during status polling on ~12k polled interface objects.

- No traps were being received by NNMi during this time.
- All polling except SNMP status polling was turned off.
- Discovery was turned off during this period.

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: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Communication</b></li> <li>• <b>ICMP Timeout</b> set to 5 seconds</li> </ul> Default SNMPv1/v2 Community Strings: <ul style="list-style-type: none"> <li>• Only one Community String configured</li> </ul>	
Discovery Configuration	<b>Rediscovery Interval set to 10 days</b> (to prevent rediscovery cycles during the scenario)	1800 Interfaces
Monitoring Configuration	Default Fault Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Management Address Polling</b></li> <li>• Enable <b>ICMP Fault Polling</b></li> <li>• Enable <b>SNMP Interface Fault Polling</b></li> <li>• Enable <b>Card Fault Polling</b></li> <li>• Enable <b>Node Component Fault Polling</b></li> <li>• <b>Fault Polling Interval</b> set to 5 minutes</li> </ul> Default Performance Monitoring: <ul style="list-style-type: none"> <li>• Enable SNMP Interface Performance Polling</li> <li>• Performance Polling Interval set to 5 minutes</li> </ul>	Disable all current polling configurations Enable State Polling
Incident Configuration		SNMP Traps: (none)

**Results:** Up to 30 packets per second or 0.039 Megabits per second with a total transfer of 1.46 MB when SNMP Status polling on ~12k polled interface objects per 5 minutes. It might increase as per customer environment.

### Standalone System – Performance Polling

This scenario measured the volume of SNMP traffic generated on one NNMi management server during the device performance polling cycle.

Utilization was measured during performance polling for the same ~12k interface objects polled during status polling scenario.

- No traps were being received by NNMi during this time.
- All polling except SNMP performance polling was turned off.

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: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Communication</b></li> <li>• <b>ICMP Timeout</b> set to 5 seconds</li> </ul> Default SNMPv1/v2 Community Strings: <ul style="list-style-type: none"> <li>• Only one Community String configured</li> </ul>	
Discovery Configuration	<b>Rediscovery Interval set to 10 days</b> (to prevent rediscovery cycles during the scenario)	1800 Interfaces
Monitoring Configuration	<b>Default Fault Monitoring:</b> <ul style="list-style-type: none"> <li>• Enable ICMP Management Address Polling</li> </ul>	
Incident Configuration		SNMP Traps: (none)

**Results:** Up to 243 packets per second or 0.773 Megabits per second with a total transfer of 29 MB when Performance Polling on ~12k polled interface objects per 5 minutes. It might increase as per customer environment.

### Standalone System – ICMP Status Polling

This scenario measure the volume of ICMP traffic generated on one NNMi management server during the ICMP fault polling cycle.

Utilization was measured during ICMP polling on 1,800 polled addresses.

- Only ICMP traffic was measured—all other traffic was excluded.

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: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Communication</b></li> <li>• <b>ICMP Timeout</b> set to 5 seconds</li> </ul>	

	Default SNMPv1/v2 Community Strings: <ul style="list-style-type: none"> <li>• Only one Community String configured</li> </ul>	
Discovery Configuration	<b>Rediscovery Interval set to 10 days</b> (to prevent rediscovery cycles during the scenario)	1800 addresses
Monitoring Configuration	<b>Default Fault Monitoring:</b> <ul style="list-style-type: none"> <li>• Enable <b>ICMP Management Address Polling</b></li> <li>• Enable <b>ICMP Fault Polling</b></li> <li>• Enable <b>SNMP Interface Fault Polling</b></li> </ul> <ul style="list-style-type: none"> <li>• Enable <b>Card Fault Polling</b></li> <li>• Enable <b>Node Component Fault Polling</b></li> <li>• <b>Fault Polling Interval</b> set to 5 minutes</li> </ul> <b>Default Performance Monitoring:</b> <ul style="list-style-type: none"> <li>• Enable SNMP Interface Performance Polling</li> <li>• <b>Performance Polling Interval</b> set to 5 minutes</li> </ul>	
Incident Configuration		SNMP Traps: (none)

**Results:** Up to 12 packets per second or 0.005 Megabits per second with a total transfer of .19 MB when ICMP Status polling on 1800 polled addresses per 5 minutes. It might increase as per customer environment.

### Standalone System – Traps

This scenario measured the volume of SNMP traffic generated on one NNMi management server under a steady-state trap load. A Cisco Link Down/Cisco Link Up trap was sent at a rate of 10 per second.

- Only Cisco Link Up/Cisco Link Down traps were sent from interface 1 (which was polled by NNMi), and were randomly sent from all 1,500 nodes at rate 10 traps/sec.
- Cisco Link Up/Cisco Link Down traps caused the following NNMi actions that resulted 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 de-duplication was occurring so not every trap caused the secondary NNMi actions.

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: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Communication</b></li> <li>• <b>ICMP Timeout</b> set to 5 seconds</li> </ul> Default SNMPv1/v2 Community Strings: <ul style="list-style-type: none"> <li>• Only one Community String configured</li> </ul>	

Discovery Configuration	<b>Rediscovery Interval set to 10 days</b> (to prevent rediscovery cycles during the scenario)	1500 nodes
Monitoring Configuration	Default Fault Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Management Address Polling</b></li> <li>• Enable <b>ICMP Fault Polling</b></li> <li>• Enable <b>SNMP Interface</b></li> </ul> Fault Polling <ul style="list-style-type: none"> <li>• Enable <b>Card Fault Polling</b></li> <li>• Enable <b>Node Component Fault Polling</b></li> <li>• <b>Fault Polling Interval</b> set to 5 minutes</li> </ul> Default Performance Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>SNMP Interface Performance Polling</b></li> <li>• <b>Performance Polling Interval</b> set to 5 minutes</li> </ul>	1800 IP addresses 11646 Interfaces
Incident Configuration		SNMP Traps: <ul style="list-style-type: none"> <li>• Cisco Link Up</li> <li>• Cisco Link Down</li> </ul>

**Results:** Up to 216 packets per second or 0.405 Megabits per second with a total transfer of 61 MB when traps sent at 10 traps/sec from 1500 nodes per 20 minutes. It might increase as per customer environment.

### Standalone System – Custom Polling

This scenario measured the volume of SNMP traffic generated on one NNMi management server during a Custom Polling cycle. Utilization was measured during custom polling of 11500 interfaces (if%util was polled).

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: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Communication</b></li> <li>• <b>ICMP Timeout</b> set to 5 seconds</li> </ul> Default SNMPv1/v2 Community Strings: <ul style="list-style-type: none"> <li>• Only one Community String configured</li> </ul>	
Discovery Configuration	<b>Rediscovery Interval set to 10 days</b> so that no discovery would occur	1500 nodes
Monitoring Configuration	Default Fault Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Management Address Polling</b></li> <li>• Enable <b>ICMP Fault Polling</b></li> <li>• Enable <b>SNMP Interface</b></li> </ul> Fault Polling <ul style="list-style-type: none"> <li>• Enable <b>Card Fault Polling</b></li> </ul>	1800 IP addresses 11646 Interfaces



- 
- Enable **Node Component Fault Polling**

- **Fault Polling Interval** set to 5 minutes

Default Performance Monitoring:

- Enable **SNMP Interface Performance Polling**
- **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

11500 interfaces

---

**Results:** Up to 13 packets per second or 0.042 Megabits per second with a total transfer of 1.6 MB when Custom polling on 11500 interfaces per 5 minutes. It might increase as per customer environment.

## NNMi Application Failover Configuration

NNMi's Application Failover functionality replicates the Postgres database from the Active server to the Standby server on port 5432 and sends transaction logs and database .zip files on port 7810. The following scenarios measured the TCP traffic on these two ports.

For these scenarios, NNMi was scaled to the upper end of the Extra High single-system tier: 30,000 nodes, 90,000 polled objects (performance and fault polling), and 210,000 Custom Polled objects. All objects were polled at the default interval.

The NNMi Active Server configuration that applies to each scenario is described in the following table:

Configuration settings on Extra high Single-System Tier (NNMi management servers): Configuration Workspace	Specific Settings on Active machine	Objects
Discovery Configuration	<b>Rediscovery Interval</b> on all Regional Managers was set to 24 hours	30,000 nodes
Monitoring Configuration	Default Fault Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Management Address Polling</b></li> <li>• Enable <b>ICMP Fault Polling</b></li> <li>• Enable <b>SNMP Interface</b></li> </ul> Fault Polling <ul style="list-style-type: none"> <li>• Enable <b>Card Fault Polling</b></li> <li>• Enable <b>Node Component Fault Polling</b></li> <li>• <b>Fault Polling Interval</b> set to 5 minutes</li> </ul> Default Performance Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>SNMP Interface Performance Polling</b></li> <li>• <b>Performance Polling Interval</b> set to 5 minutes</li> </ul>	32,908 Interfaces 90,000 Node Components
Incident Configuration		SNMP Traps: (none)

### Application Failover – Discovery

This scenario measured the TCP traffic volume received on the Application Failover ports during initial discovery on the Active server.

**Results:** Up to 2457 packets per second or 36 Megabits per second with a total transfer of 4050 MB when discovery of 30K nodes per 15 minutes. It might increase as per customer environment.

### Application Failover - Steady State SNMP Polling

This scenario measured traffic after discovery had completed and all polling was set to the 5 minutes default interval. No resynchronization, heavy rediscovery, outages or other events that would cause heavy load on the system were occurring.

**Results:** Up to 27 packets per second or 0.53 Megabits per second with a total transfer of 60 MB when status poll of 30K nodes per 15 minutes. It might increase as per customer environment.

### Application Failover - Database Synchronization

Periodically, Application Failover does full database synchronization from the Active server to the Standby server. Network traffic was measured during this period of increased traffic between the Active and Standby servers.

**Results:** Up to 1312 packets per second or 20 Megabits per second with a total transfer of 2279 MB when DB Synchronization happens for 30K nodes per 15 minutes. It might increase as per customer environment.

## Global Network Management (GNM) Network Utilization Configuration

The Global Network Management (GNM) feature of NNMi allows for central collection of several remote network management stations. The GNM scenario described in this section included one Global Manager and three Regional Managers.

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. It was only responsible for displaying data received from the three Regional Managers.
- The Global Manager’s database contained a total of 65,000 nodes.
- Three Regional Managers (each managing from 15000 to 30,000 nodes) forwarded data to the Global Manager.
- Across the three Regional Managers was a total of 408,961 fault and performance polled interfaces, 534,581 node components (sometimes referred to as node health components) and 126,681 IP addresses.

**GNM - 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 bandwidth required to send all of the topology information for 30,000 nodes from the Regional Manager to the Global Manager. Initial discovery on the Regional Manager was completed. No other Regional Managers were connected to the Global Manager during this period.

Configuration settings on Extra high Single-System Tier (NNMi management servers): Configuration Workspace	Specific Settings	Objects
Global Network Management	Regional Manager Connections (one configured)	1 Regional Manager
Incident Configuration		SNMP Traps: (none)

**Results:** Up to 145 packets per second or .8 Megabits per second with a total transfer of 90 MB of TCP traffic during forwarding the 30K nodes to GNM per 15 minutes. It might increase as per customer environment.

**GNM – Steady State SNMP Polling**

This scenario measured the TCP traffic volume received by the Global Manager from the three Regional Managers.

During this scenario all of the polled objects mentioned in the Configuration section above were polled at the default interval of 5 minutes. The Global Manager had completed discovering (transferring) all the topology data from the three Regional Managers.

The three Regional Managers were configured as described in the following table:

Configuration settings on the three Regional Managers (NNMi management servers) Configuration Workspace	Specific Settings on Regional Managers (each with these settings)	Cumulative Object Count forwarded Global Manager
Discovery Configuration	<b>Rediscovery Interval</b> on all Regional Managers was <b>set to 24 hours</b>	65,000 nodes
Monitoring Configuration	Default Fault Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Management Address Polling</b></li> <li>• Enable <b>ICMP Fault Polling</b></li> <li>• Enable <b>SNMP Interface</b></li> </ul> Fault Polling <ul style="list-style-type: none"> <li>• Enable <b>Card Fault Polling</b></li> <li>• Enable <b>Node Component Fault Polling</b></li> <li>• <b>Fault Polling Interval</b> set to 5 minutes</li> </ul> Default Performance Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>SNMP Interface Performance Polling</b></li> </ul>	126681 IP addresses 408961 Interfaces 534581 Node Components

- **Performance Polling Interval** set to 5 minutes

Incident Configuration

SNMP Traps: (none)

**Results:** Up to 155 packets per second or .63 Megabits per second with a total transfer of 95 MB of TCP traffic during SNMP status polling on 65K nodes per 20 minutes. It might increase as per customer environment.

### GNM - Heavy Load Fault and Performance Polling

This scenario measured the TCP traffic volume received by the Global Manager from the three Regional Managers. During this scenario 117,500 of the 408,961 interfaces were fault and performance polled every minute. The remaining interfaces were fault and performance polled every 5 minutes.

Each of the Regional Manager configuration settings are described in the following tables. The only difference in the Regional Manager settings is the interval settings noted in red.

Configuration settings on the three Regional Managers (NNMi management servers) Configuration Workspace	Specific Settings on Regional Managers (each with these settings)	Cumulative Object Count forwarded Global Manager
---	---	--

Discovery Configuration	<b>Rediscovery Interval</b> was set to 24 hours	14,626 Nodes
-------------------------	---	--------------

Monitoring Configuration	Default Fault Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Management Address Polling</b></li> <li>• Enable <b>ICMP Fault Polling</b></li> <li>• Enable <b>SNMP Interface Fault Polling</b></li> <li>• Enable <b>Card Fault Polling</b></li> <li>• Enable <b>Node Component Fault Polling</b></li> <li>• <b>Fault Polling Interval</b> set to 1 minute</li> </ul> Default Performance Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>SNMP Interface Performance Polling</b></li> <li>• <b>Performance Polling Interval</b> set to 1 minute</li> </ul>	16,360 IP addresses 117,500 Interfaces 100,922 Node Components
--------------------------	--	--

Incident Configuration

SNMP Traps: (none)

**Results:** Up to 122 packets per second or .47 Megabits per second with a total transfer of 71 MB of TCP traffic during fault and performance polling on 65K nodes per 20 minutes. It might increase as per customer environment.

### GNM - Resynchronization Scenario

This scenario measures the TCP traffic volume received by the Global Manager from the three Regional Managers during a resynchronization of the NNMi database. GNM resynchronization happens when all state and status is recalculated and sent from the Regional Managers to the Global Manager. A resynchronization is automatically performed after major events such as:

1. A management station application failover,
2. Restore from backup, or
3. Upgrading from NNMi 9.10 to the current version.

Network traffic was measured on the Global Manager during a resynchronization.

Configuration settings on 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	<b>Rediscovery Interval</b> on all Regional Managers was set to 24 hours.	65,000 Nodes
-------------------------	---	--------------

Monitoring Configuration	Default Fault Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>ICMP Management Address Polling</b></li> <li>• Enable <b>ICMP Fault Polling</b></li> <li>• Enable <b>SNMP Interface</b></li> </ul> Fault Polling <ul style="list-style-type: none"> <li>• Enable <b>Card Fault Polling</b></li> <li>• Enable <b>Node Component Fault Polling</b></li> <li>• <b>Fault Polling Interval</b> set to 5 minutes</li> </ul> Default Performance Monitoring: <ul style="list-style-type: none"> <li>• Enable <b>SNMP Interface Performance Polling</b></li> <li>• <b>Performance Polling Interval</b> set to 5 minutes</li> </ul>	126,681 IP addresses 408,961 Interfaces 534,581 Node Components
--------------------------	---	---

Incident Configuration	SNMP Traps: (none)
------------------------	--------------------

**Results:** Up to 133 packets per second or .52 Megabits per second with a total transfer of 59 MB of TCP traffic during resynchronization of 65K nodes per 15 minutes. It might increase as per customer environment.

## **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 **network-management-doc-feedback@hpe.com**.

**Product name and version:** NNMi 10.20

**Document title:** Guidelines to be followed for Network Bandwidth Utilization for Standalone and Global Network Management Environments

**Feedback:**

---

© Copyright 2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.