iMaster NCE
V100R021C00
SNMP NBI User Guide

Issue	09
Date	2022-10-14

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Reading Guide

This reading guide provides recommended chapters for different readers.

NOTE

The Simple Network Management Protocol (SNMP) northbound interface (NBI) supports three formats of management information bases (MIBs): MIB1, MIB2, and MIB3.

- Both **HW-IMAPV1NORTHBOUND-TRAP-MIB.mib** and **HW-IMAPV2NORTHBOUND-TRAP-MIB.mib** refer to the MIB1, which is used to manage transport, access, and datacom devices, or cross-domain devices. V1 and V2 indicate the Structure of Management Information (SMI) versions of **HW-IMAPV1NORTHBOUND-TRAP-MIB.mib** and **HW-IMAPV2NORTHBOUND-TRAP-MIB.mib** respectively. The OSS selects a version based on its supported SMI version. SMI versions differ in syntax. For details, see RFC 1155 and RFC 1902.
- Both **IMAP_NORTHBOUND_MIB-V1.mib** and **IMAP_NORTHBOUND_MIB-V2.mib** refer to the MIB2, which is used to support upgrades of Agile Controller-WAN. V1 and V2 indicate the SMI versions of **IMAP_NORTHBOUND_MIB-V1.mib** and **IMAP_NORTHBOUND_MIB-V2.mib** respectively. The OSS selects a version based on its supported SMI version. SMI versions differ in syntax. For details, see RFC 1155 and RFC 1902.
- **T2000-NETMANAGEMENT-MIB.mib** refers to the MIB3 and complies with SMIv2, which supports upgrades of original transport network management systems (NMSs) and can manage only transport devices.
- MIB1 refers to the original U2000 MIB, and MIB3 refers to the original U2000-T MIB.

Intended Audience	Purpose	Recommended Chapter
Network planning engineer	Design, plan, and optimize networks. They need to know working principles, network positions, and interface parameters (such as IP address and ports) of the SNMP NBI.	2 Overview, 2.8 SNMP Introduction, 5 Checking the License, 6.2 Configuration Parameters, and 11 Service Port Description.

Intended Audience	Purpose	Recommended Chapter
Application developer	Develop OSS and programs for interconnecting with the SNMP NBI. They need to know basic principles, functions, MIB structures, and parameter definitions of the SNMP NBI.	**2 Overview**, **2.8 SNMP Introduction**, **6 Configuring the SNMP NBI**, **8 Configuring the SNMP NBI on the OSS**, **9 Calling the SNMP NBI**, **6.2 Configuration Parameters**, **12 MIB1**, **13 MIB2** and **14 MIB3**. Focus on **12 MIB1**, **13 MIB2**, and **14 MIB3**.
Installation and commissioning engineer Data configuration engineer	Configure the SNMP NBI and verify its connection with the OSS. They do not need to know basic concepts or principles of the SNMP NBI.	**6 Configuring the SNMP NBI**, **8 Configuring the SNMP NBI on the OSS**, **9 Calling the SNMP NBI**, **6.2 Configuration Parameters**, and **11 Service Port Description**. Focus on **6 Configuring the SNMP NBI**. Complete SNMP NBI deployment and configuration by referring to the flowchart and procedures.
System maintenance engineer	Maintain the SNMP NBI and diagnose SNMP NBI faults. They need to know working principles and parameters of the SNMP NBI.	**2 Overview**, **2.8 SNMP Introduction**, **10 Maintaining the SNMP NBI**, **6.2 Configuration Parameters**, and **11 Service Port Description**.

2 Overview

About This Chapter

iMaster NCE (referred to as NCE) provides the SNMP NBI for the OSS to manage alarms on NCE.

2.1 Introduction

2.2 Network Position
The SNMP NBI is configured between the OSS and NCE, and establishes transmission channels for alarm information between these two systems.

2.3 Devices Supported

2.4 Functions
The SNMP NBI supports three types of MIBs for different functions. Carriers can select an appropriate MIB to interconnect with the OSS for network O&M.

2.5 Standards Compliance
The SNMP NBI is developed based on the SNMP protocol. Currently there are three SNMP versions: SNMPv1, SNMPv2c, and SNMPv3, all of which are supported by the NCE SNMP NBI.

2.6 Security Mechanism
The security mechanism used by the SNMP NBI is also the security mechanism of the SNMP protocol. Any access to the SNMP NBI must be authenticated by the security mechanism of the specific SNMP version (SNMPv1, SNMPv2c, or SNMPv3).

2.7 Performance Indicators
The OSS manages alarms on NCE through the SNMP NBI. Performance indicators for the SNMP NBI include the maximum number of concurrent NMS connections, alarm reporting efficiency, and alarm reporting delay.

2.8 SNMP Introduction

2.1 Introduction

Oriented to carriers, NCE provides a large-scale management capability. NCE Lite is a lightweight version of NCE, which is a cost-effective miniaturized solution for enterprises.

Based on the unified service-oriented architecture of NCE, NCE Lite is capable of managing IP, transport, and access devices separately or together. NCE Lite provides basic apps and the Network Management app and has the same GUI and operation experience as NCE.

NOTE

NCE is used for both NCE and NCE Lite mentioned in the document.

The SNMP NBI is one of the NBIs provided by NCE. The OSS can access NCE through the SNMP NBI to monitor and manage alarms in Huawei device networks.

The SNMP protocol consists of a set of standards for network management and is one of the most widely used protocols in TCP/IP networks.

As one of the widely applied network management protocols in the TCP/IP network, SNMP aims to:

- Transmit the management information between two nodes.
- Help the manager search and modify the information, and locate faults on any node in the network.
- Help the manager diagnose faults, configure NEs, and generate reports.

The features of SNMP are as follows:

- Uses the polling mechanism and provides basic operation sets.
- Fits small, fast, and cost-effective networks.

Huawei developed the SNMP NBI for NCE in compliance with industry standards. With this NBI, the OSS can interconnect with NCE quickly and monitor and manage alarms on the network.

NOTE

OSSs are computer systems used by carriers to manage performance, inventories, services, and faults of network devices efficiently. By function, OSSs can be classified into the service assurance OSS, the service provisioning OSS, and the inventory management OSS.

In this document, OSSs cover upper-layer NMSs and third-party NMSs. The SNMP NBI can support alarm management only. Generally, the OSS indicates a service assurance OSS.

2.2 Network Position

The SNMP NBI is configured between the OSS and NCE, and establishes transmission channels for alarm information between these two systems.

After an alarm is generated on a device, the alarm is reported to NCE for processing. Then report the processed alarm to the OSS through the SNMP NBI in real time. The OSS queries, acknowledges, unacknowledges, or clears alarms on NCE through the SNMP NBI.

Figure 2-1 shows the position of the SNMP NBI on a network.

Figure 2-1 Position of the SNMP NBI on a network

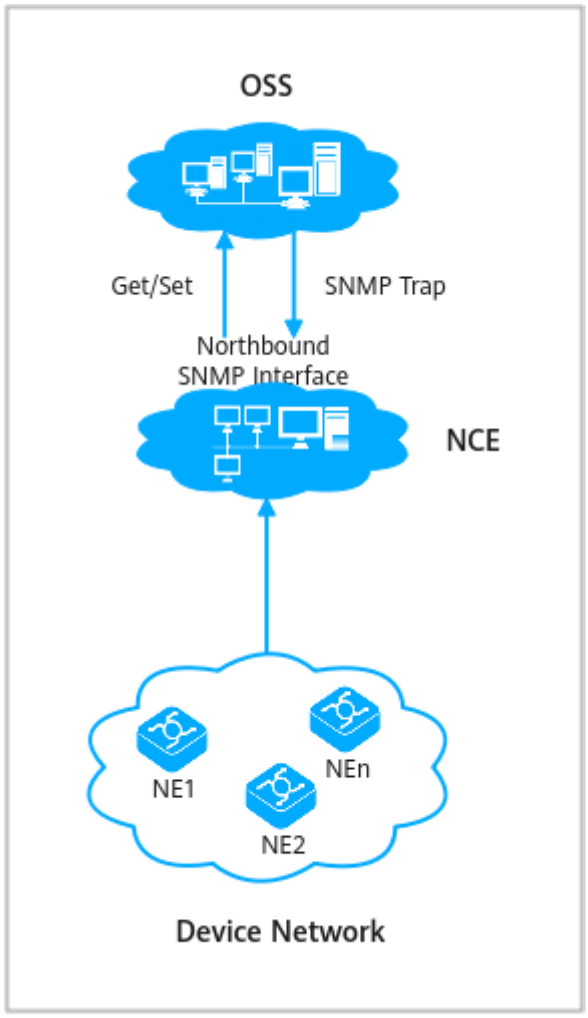


Table 2-1 SNMP NBI components

Component	Description
OSS	The SNMP NBI can support alarm management only. Generally, the OSS indicates a service assurance OSS.
NCE	iMaster NCE is positioned as a Huawei device management system. As a major future-oriented network management solution of Huawei, it possesses powerful element and network management functions.
NE	Network element.

2.3 Devices Supported

Transport Devices

Table 2-2 Transport devices supported by the SNMP NBI

Feature	MSTP	Hybrid MSTP	WDM	OTN	Hybrid RTN (TDM Feature)	TDM RTN	Packet RTN	PTN	Marine
Alarm	√	√	√	√	√	√	√	√	×

NOTE

Submarine devices or devices intended for North America are not supported.

Routers

Table 2-3 Routers supported by the SNMP NBI

Feature	NE Series	CX Series	Huawei Switch	BRAS	ATN	Security Series
Alarm	√	√	√	√	√	√

NOTE

The following devices are supported:

- NE series: NE40/40E/40E-4/40E-X3/40E-X8/40E-X16, NE80/80E, NE5000E, NE5000E-Multi
- CX series: CX600/600-4/600-8/600-16/600-X1/600-X2/600-X3/600-X4/600-X8/600-X16
- Switches: Quid Way S2300/3300/5300/9300
- BRASs: ME60/60-X3/-X8/60-X16
- ATN VRP series: ATN910/950/990
- Eudemon series
- eLog series

Access Devices

Table 2-4 Access devices supported by the SNMP NBI

Feature	MSAN/DSLAM		FTTx	
	Narrowband Port	Broadband Port	FTTH	FTTB/FTTC
Alarm	√	√	√	√

2.4 Functions

The SNMP NBI supports three types of MIBs for different functions. Carriers can select an appropriate MIB to interconnect with the OSS for network O&M.

2.4.1 MIB1

The MIB1 is used to manage transport, access, and datacom devices or manage multi-domain devices. When the MIB1 is loaded, the SNMP NBI supports automatic alarm reporting, synchronization (querying active alarms), clearance, acknowledgement/unacknowledgement, and alarm acknowledgement and clearance status reporting.

NCE

On the NCE side, the primary functions are:

- Reporting alarms
- Reporting heartbeats

NOTE

To enable automatic alarm reporting, set OSS parameters on NCE when configuring the SNMP NBI. Alarm information will be received at the preset port of the OSS server.

After receiving alarms from devices or NCE, the SNMP NBI reports these alarms to the OSS by means of standard SNMP trap messages.

The SNMP NBI sends heartbeat traps to the OSS periodically. Based on the heartbeats, the OSS determines whether the connection with the SNMP NBI is proper.

For details about traps, see **12.3 MIB1 Trap**.

Function	Description
Subscribing alarms	Subscribes alarms by alarm severity and category. You can set the severity and category when deploying the SNMP NBI. Sets the alarm field or variable binding (VB).

Function	Description
Reporting alarms	Reports alarms from NEs or NCE.
Reporting heartbeats	Reports heartbeats and sets the heartbeat period.
Reporting alarm acknowledgement status	Reports the alarm acknowledgement status.
Reporting alarm clearance status	Reports the alarm clearance status.

OSS

On the OSS side, the primary functions are:

- Synchronizing alarms (querying active alarms)
- Changing filter criteria in real time
- Acknowledging/Unacknowledging alarms
- Clearing alarms

NOTE

Ensure that the OSS is connected to the SNMP NBI properly before performing operations.

Function	Description
Synchronizing alarms (querying active alarms)	Queries active alarms (uncleared alarms) on NCE in the Set operation. The OSS uses the Set operation to query these alarms on NCE. To query active alarms on NCE, the OSS issues the query begin command in the Set operation. After receiving the command, the SNMP agent queries active alarms from NCE and reports the result to the OSS. If there are too many alarms and the query needs to be stopped, the OSS issues the query end command in the Set operation. After receiving the command, the SNMP agent stops querying alarms and does not report the result to the OSS. For details about alarm synchronization, see **9.1.3 Synchronizing Alarms**. For details about traps, see **MIB1 Trap**.

Function	Description
Querying alarms by criteria	Reports alarms by alarm severity and category. The filter criteria are specified during alarm subscription. You can change filter criteria in real time when loading the MIB1.
Changing filter criteria in real time	Changes filter criteria using the Set operation when the SNMP NBI is running. The filter criteria are specified during alarm subscription. The change will take effect without restarting the SNMP NBI.
Acknowledging/ Unacknowledging alarms	Acknowledges or unacknowledges current alarms on NCE based on alarm SNs.
Clearing alarms	Clears alarms on NCE based on alarm SNs.

2.4.2 MIB2

The MIB2 supports upgrades of Agile Controller-WAN. When the MIB2 is loaded, the SNMP NBI supports automatic alarm reporting, synchronization (querying active alarms), clearance, acknowledgement/unacknowledgement, and alarm acknowledgement and clearance status reporting.

NCE

On the NCE side, the primary functions are:

- Reporting alarms
- Reporting heartbeats

NOTE

To enable automatic alarm reporting, set OSS parameters on NCE when configuring the SNMP NBI. Alarm information will be received at the preset port of the OSS server.

After receiving alarms from devices or NCE, the SNMP NBI reports these alarms to the OSS by means of standard SNMP trap messages.

The SNMP NBI periodically reports heartbeats to the OSS. Based on the heartbeats, the OSS determines whether the connection with the SNMP NBI is proper.

For details about traps, see **13.3 MIB2 Trap**.

Function	Description
Subscribing alarms	Subscribes alarms by alarm severity and category. You can set the severity and category when deploying the SNMP NBI. Sets the alarm field or VB.
Reporting alarms	Reports alarms from NEs or NCE.
Reporting heartbeats	Reports heartbeats and obtains the heartbeat period.
Reporting alarm acknowledgement status	Reports the alarm acknowledgement status.
Reporting alarm clearance status	Reports the alarm clearance status.

OSS

On the OSS side, the primary functions are:

- Synchronizing alarms (querying active alarms)
- Obtaining the heartbeat period
- Acknowledging/Unacknowledging alarms
- Clearing alarms

NOTE

Ensure that the OSS is connected to the SNMP NBI properly before performing operations.

Function	Description
Synchronizing alarms (querying active alarms)	Queries active alarms (uncleared alarms) on NCE in the Set operation. The OSS uses the Set operation to query these alarms on NCE. To query active alarms on NCE, the OSS issues the query begin command in the Set operation. After receiving the command, the SNMP agent queries active alarms from NCE and reports the result to the OSS. If there are too many alarms and the query needs to be stopped, the OSS issues the query end command in the Set operation. After receiving the command, the SNMP agent stops querying alarms and does not report the result to the OSS. For details about alarm synchronization, see **9.2.3 Synchronizing Alarms**. For details about traps, see **13.3 MIB2 Trap**.

Function	Description
Obtaining the heartbeat period	The SNMP NBI allows the OSS to obtain the heartbeat period in real time. The MIB provides a leaf node about the heartbeat period so that the OSS can obtain the value of the heartbeat period in real time.
Acknowledging/ Unacknowledging alarms	Acknowledges or unacknowledges current alarms on NCE based on alarm SNs.
Clearing alarms	Clears alarms on NCE based on alarm SNs.

2.4.3 MIB3

The MIB3 is used to be compatible with upgrades of transport NMSs. It is used to manage only transport devices. When the MIB3 is loaded, the SNMP NBI supports automatic alarm reporting and synchronization (querying active alarms).

NCE

On the NCE side, the primary function is automatic alarm reporting.

NOTE

To enable automatic alarm reporting, set OSS parameters on NCE when configuring the SNMP NBI. Alarm information will be received at the preset port of the OSS server.

After receiving alarms from devices or NCE, the SNMP NBI reports these alarms to the OSS by means of standard SNMP trap messages. For details about traps, see **14.3 MIB3 Trap**.

Function	Description
Subscribing alarms	Subscribes alarms by alarm severity and category. You can set the severity and category when deploying the SNMP NBI.
Reporting alarms	Reports alarms from NEs or NCE.

OSS

On the OSS side, the primary function is querying active alarms (uncleared alarms) on NCE. The OSS uses the Set operation to query these alarms on NCE.

NOTE

Ensure that the OSS is connected to the SNMP NBI properly before performing operations.

To query active alarms on NCE, the OSS issues the query begin command (value: 1) in the Set operation. After receiving the command, the SNMP agent queries

active alarms from NCE and reports the result to the OSS. If there are too many alarms and the query needs to be stopped, the OSS issues the query end command (value: 0) in the Set operation. After receiving the command, the SNMP agent stops querying alarms and does not report the result to the OSS.

For details about alarm synchronization, see **9.3.2 Synchronizing Alarms**.

For details about traps, see **14.3 MIB3 Trap**.

Function	Description
Querying all active alarms	Reports all active alarms by default. You can stop alarm synchronization using the Set operation.
Querying alarms by criteria	Reports alarms by alarm severity and category. The filter criteria are specified during alarm subscription.

2.5 Standards Compliance

The SNMP NBI is developed based on the SNMP protocol. Currently there are three SNMP versions: SNMPv1, SNMPv2c, and SNMPv3, all of which are supported by the NCE SNMP NBI.

Currently, the NCE SNMP NBI complies with the following three SNMP protocol versions:

- SNMPv1: the first version. For details, see RFC 1157.
- SNMPv2c: the second version. Some data types and protocol applications are added. For details, see RFC 1902.
- SNMPv3: the latest version. The security mechanism is reinforced. For details, see RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575.

SNMPv1

- Mutual access to management information between the NMS (also called SNMP manager) and SNMP agent.
- Operations include:
  - Get
  - Set
  - Trap
- Protocol Data Unit (PDU)
  - GetRequest
  - GetNextRequest
  - GetResponse
  - SetRequest
  - Trap
- Community-based security model

NOTE

The OSS must get the community information from the NCE administrator.

SNMPv2c

SNMPv2c inherits all functions in SNMPv1 and provides the following new functions:

- Mutual access to management information between SNMP managers.
- Operations include:
  - GetBulk
  - Inform
  - Report
- The format of traps is modified to be the same as that of the Get and Set packets.
- SNMPv2c provides fractionalized error codes.

NOTE

The OSS must get the community information from the NCE administrator.

SNMPv3

SNMPv3 inherits all functions in SNMPv2c and provides the following new functions:

- User-based security model
- SNMPv3 supports all security levels as follows:
  - Not authenticated nor encrypted
  - Authenticated but not encrypted
  - Authenticated and encrypted

    Authentication supports MD5 and SHA algorithms, and encryption supports DES and AES algorithms.

NOTE

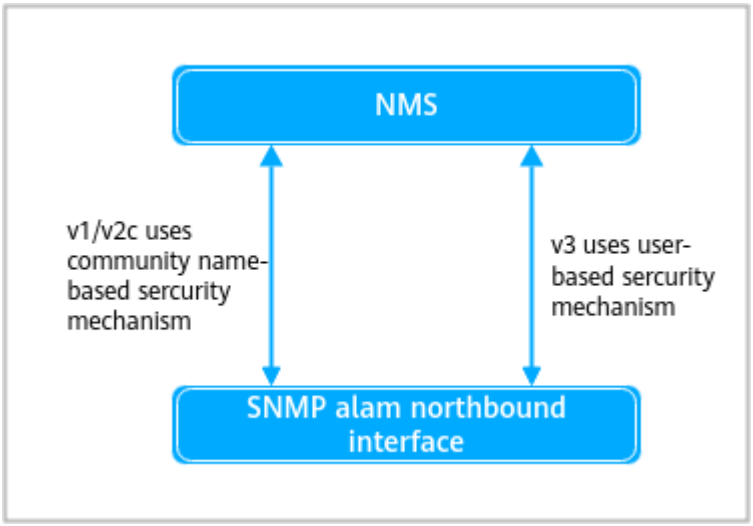
- The OSS must get the SNMPv3 information from the NCE administrator, including security levels, usernames, authentication passwords, and encryption passwords.
- MD5 and DES are insecure algorithms. Exercise caution when selecting them.

2.6 Security Mechanism

The security mechanism used by the SNMP NBI is also the security mechanism of the SNMP protocol. Any access to the SNMP NBI must be authenticated by the security mechanism of the specific SNMP version (SNMPv1, SNMPv2c, or SNMPv3).

As shown in **Figure 2-2**, SNMPv1 and SNMPv2c use a community-based security mechanism, whereas SNMPv3 uses a user-based security mechanism.

Figure 2-2 Security mechanism



SNMPv1 and SNMPv2c

The security mechanism of SNMPv1 and SNMPv2c is community-based. The NMS authenticates NEs based on the community name list and the agent does not check the validity of the community name. SNMP packets are transferred without encryption. Therefore, authentication security and confidentiality are not guaranteed.

- Before the **Get**, **Get Next**, or **Set** operation, the NMS must know the read and write community names configured for the agent.
- For trap and inform packets, the community name is the read community name configured for the agent.

NOTE

SNMPv1 does not support the inform mode.

SNMPv3

The security mechanism of SNMPv3 is user-based. In terms of security, SNMPv3 emphasizes data security and access control, and therefore offers a higher level of security than SNMPv1 and SNMPv2c.

In data security, SNMPv3 provides protection for SNMP packets in the following ways:

- Data integrity check

  The data cannot be modified in an unauthorized manner. Any changes in the data sequence are limited to the allowed extent.
- Data origin authentication

  SNMPv3 authenticates users from whom received packets are sent rather than applications that generate these packets. SNMPv3 ensures security on a user basis and authenticates messages generated by users instead of by applications.
- Data confidentiality check

When the NMS or agent receives a packet, it checks when the packet was generated. If the interval between the creation time and the system time exceeds the preset time range, this packet will be discarded. This check prevents packets from being maliciously modified and malicious packets from being received.

In access control, the NMS performs security checks on managed objects (MOs) based on SNMPv3.

Security Level

Table 2-5 lists security levels supported by the SNMP versions.

Table 2-5 Security level

Protocol Version	Security Level	Authentication	Data Encryption	Description
v1	Without authentication and encryption	Community	None	Uses only community names for access authentication.
v2c	Without authentication and encryption	Community	None	Uses only community names for access authentication.
v3	Without authentication and encryption	User name	None	Uses only usernames for access authentication.
v3	Authenticated but not encrypted	MD5 or SHA	None	Uses MD5 or SHA algorithms for authentication.
v3	Authenticated and encrypted	MD5 or SHA	AES or DES	Uses MD5 or SHA algorithms for authentication and AES or DES algorithms for data encryption.

NOTE

- For security purposes, from NCE V100R019C00, the SNMP NBI does not support the following insecure configuration items by default:
  - **Protocol version**: **SNMPv1** and **SNMPv2c**
  - **Security level**: **Not authenticated nor encrypted** and **Authenticated but not encrypted**
  - **Authentication protocol**: **MD5**, **SHA**, and **SHA2-224**
  - **Encryption protocol**: **DES**

    If you need insecure protocols, log in to the O&M plane, open the Security Management app, and choose **Configuration Compliance** > **Security Configuration** from the main menu. On the **Configuration Check** page, click **SNMP NBI-SNMP security configuration** and enable **SNMP Insecure Switch**. Then open the System Settings app, choose **System Settings** > **Northbound Interface** from the main menu, choose **SNMP NBI** > **Basic Settings** from the navigation pane, and configure protocols. If insecure protocols are not needed, disable **SNMP Insecure Switch**. A high-risk alert will be displayed if insecure protocols are enabled.
- The following rules are applicable to SNMPv3:
  - You can set a different username, authentication password, and encryption password from others.
  - You can select any of the listed security levels, authentication algorithms, and encryption algorithms.

2.7 Performance Indicators

The OSS manages alarms on NCE through the SNMP NBI. Performance indicators for the SNMP NBI include the maximum number of concurrent NMS connections, alarm reporting efficiency, and alarm reporting delay.

Table 2-6 lists the performance indicators for the SNMP NBI.

Table 2-6 Performance indicators for the SNMP NBI

Indicator	Description
Maximum number of third-party OSSs supported	10
Alarm reporting efficiency	60 or more alarms per second when three OSSs are connected
Alarm reporting delay	Shorter than 10 seconds when three OSSs are connected

2.8 SNMP Introduction

About This Section

This section describes the working principles of SNMP. For details about the SNMP protocol, see the relevant protocol documents.

2.8.1 Network Management Framework

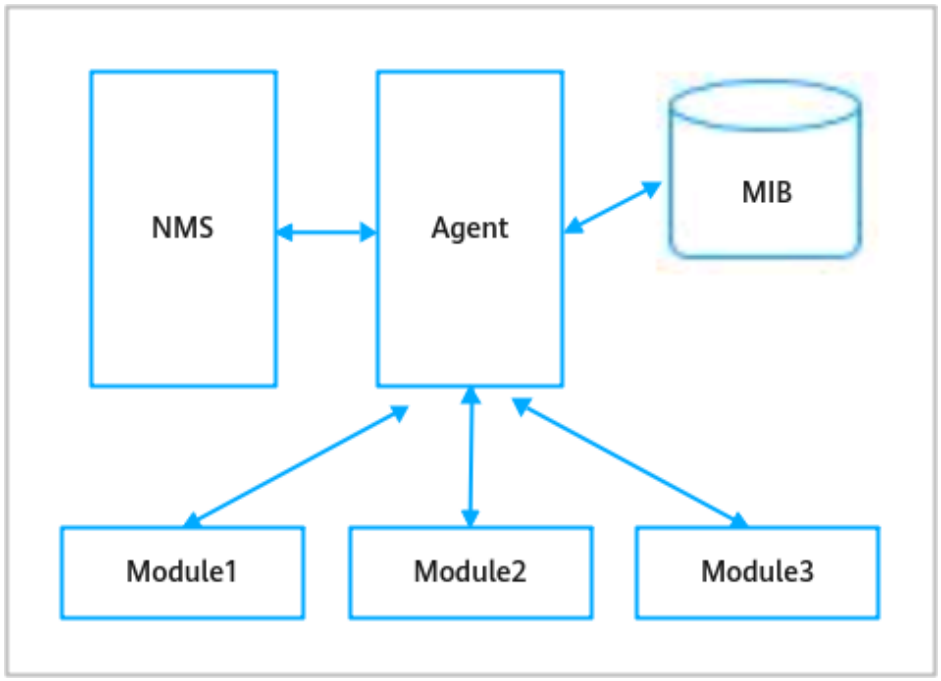
SNMP is a set of protocols and standards. It provides channels for the OSS to collect network management data from network devices and for network devices to report problems and errors to the OSS.

The SNMP network management framework consists of the NMS, Agent, MIB, and SNMP. **Figure 2-3** illustrates the relationships among them.

NOTE

In SNMPv3, both the NMS and the agent are called an entity.

Figure 2-3 Network management framework



- **NMS**

  An independent system that runs network management applications.

  Send query packets to NEs.

  Receive responses or traps from NEs.

- **SNMP agent**

  Processes that run on NEs.

  Receive, parse, and authenticate query packets from the NMS.

  Search the MIB tree, call other modules for operation, and obtain responses.

  Construct response packets and send them to the NMS.

  Send traps to the NMS if urgent.

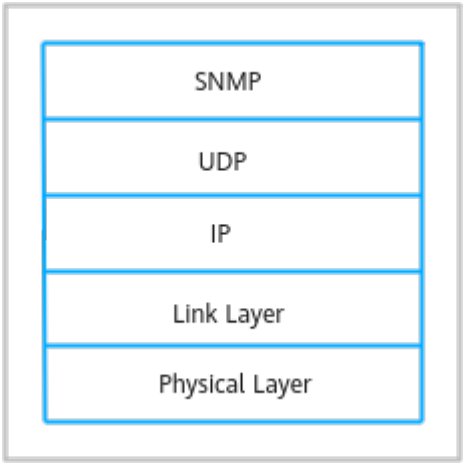
- **MIB**

  A type of database that stores NE management information and responds to management requests, such as the query and setting requests, issued from the NMS through the SNMP agent.

The agent queries the MIB for required operations.

- **SNMP Protocol**
  An application-layer protocol carried over UDP in the TCP/IP protocol stack. SNMP exchanges management information between the NMS and the agent.
  Figure 2-4 shows the position of SNMP in the TCP/IP protocol stack.

Figure 2-4 Position of SNMP



NOTE

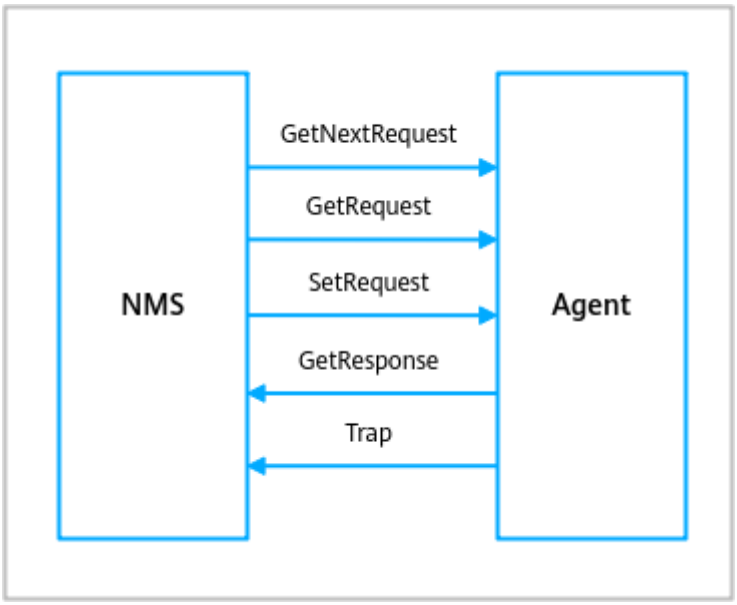
For the SNMP NBI, the agent runs on NCE and the NMS refers to the OSS. Currently three MIBs are supported: MIB1, MIB2, and MIB3. For details, see **12 MIB1**, **13 MIB2**, and **14 MIB3**.

2.8.2 Message Types

In SNMP, message types are also referred to as Protocol Data Units (PDUs).

As shown in **Figure 2-5**, SNMP provides five types of PDUs (SNMP packets) for communication between the NMS and the agent.

Figure 2-5 Message types



- GetRequest: The PDU that the NMS uses to visit the agent and obtain one or more parameter values.
- GetNextRequest: The PDU that the NMS uses to visit the agent and obtain the next parameter value.
- SetRequest: The PDU that the NMS uses to visit the agent and set one or more parameter values.
- GetResponse: The PDU that the agent uses to return one or more parameter values to the NMS as responses to GetRequest, GetNextRequest, and SetRequest packets.
- Trap: The PDU that the agent uses to send traps to inform the NMS of important events or state changes that occurred in NEs.

GetRequest, GetNextRequest, and SetRequest packets are sent from the NMS to agents, whereas GetResponse and trap packets are sent from agents to the NMS.

2.8.3 MIB

Management Information Base (MIB) is a key component of the SNMP network management framework.

NOTE

For NCE, MIB defines managed objects (MOs) that are used by all the function interfaces of the SNMP NBI. These definitions are important in that they determine what operations the OSS can perform and what network management information the OSS can obtain.

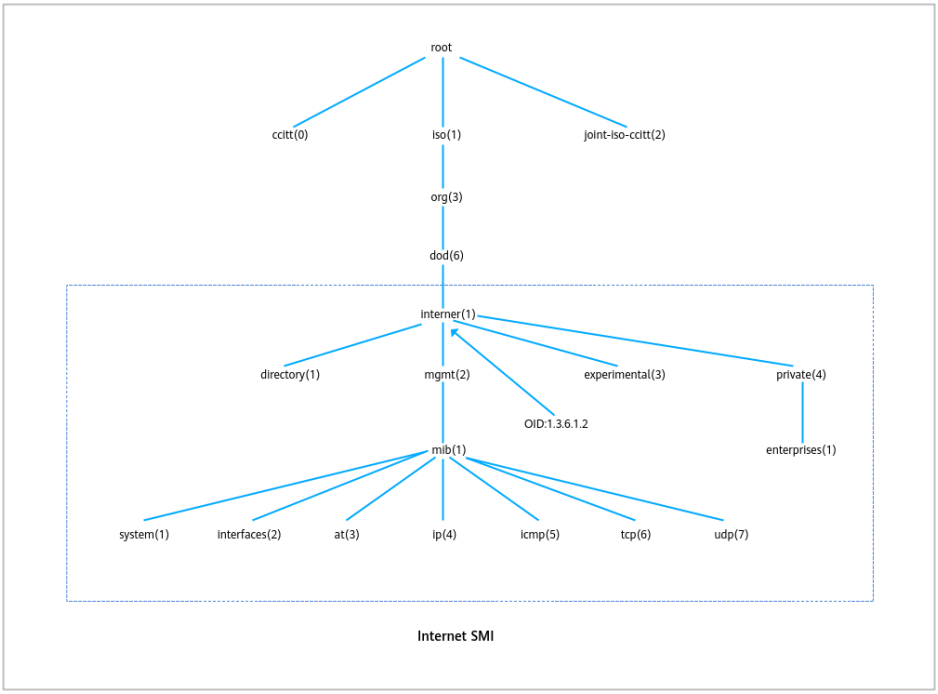
All MOs are collectively called the MIB. MIB represents a group of entities that are managed through SNMP. The MIB structure resembles a tree, and therefore it is also called a MIB tree. Each MO is mapped to a leaf node, also called an object or object identifier (OID). The MIB tree is static in that after the agent is started and the MIB is initialized, the NMS queries or modifies MOs based on the current MIB. The NMS manages the MIB in read and write mode.

In the MIB tree, each leaf node represents an MO, which can be identified by a unique path (also known as the OID) originating from the root node.

An OID consists of a set of integers greater than or equal to 0 and is used to identify an MO in the MIB tree. The SMI ensures that an MO is mapped to a unique OID.

Once the MIB file is released, OIDs are bound to related MOs and this binding cannot be modified. An MO in the MIB cannot be deleted, but can be set to **obsolete** indicating that this MO is no longer used.

Figure 2-6 MIB tree



In the preceding **Figure 2-6** MIB tree, the MO mgmt can be marked as { iso(1) org(3) dod(6) internet(1) mgmt(2) } or simply 1.3.6.1.2.

2.8.4 SNMP Packet Handling Process

This section uses SNMPv1 as an example to introduce the handling process of SNMP packets.

The agent on the managed node receives a request packet from the NMS through a UDP port. NCE uses port 9812 by default.

The agent handles the received packet as follows:

1. Decode the packet based on basic encoding rules of ASN.1 and represent it in an internal data structure. The agent discards the packet if some errors cause the decoding failure.
2. Check the SNMP version number contained in the packet. The agent fetches the version number from the packet and compares it with the version that it supports. If they are inconsistent, the agent discards the packet.

3. Check the community name contained in the packet. The community name is inserted by the NMS. If the community name is not the supported one, the agent discards the packet. A trap packet is returned to the NMS at the same time. SNMPv1 provides weak security measures, which are enhanced in SNMPv3.
4. Fetch the PDU from the authenticated ASN.1 object. If the operation fails, the agent discards the packet.
5. Handle the PDU. The agent handles the PDU according to its type. It searches the MIB to find the MO matching the variable, and then obtains the value of the variable from the module. Then, the agent generates the response packet, encodes it and returns it to the NMS.
6. The NMS performs the same operations as the agent, and displays the final result.

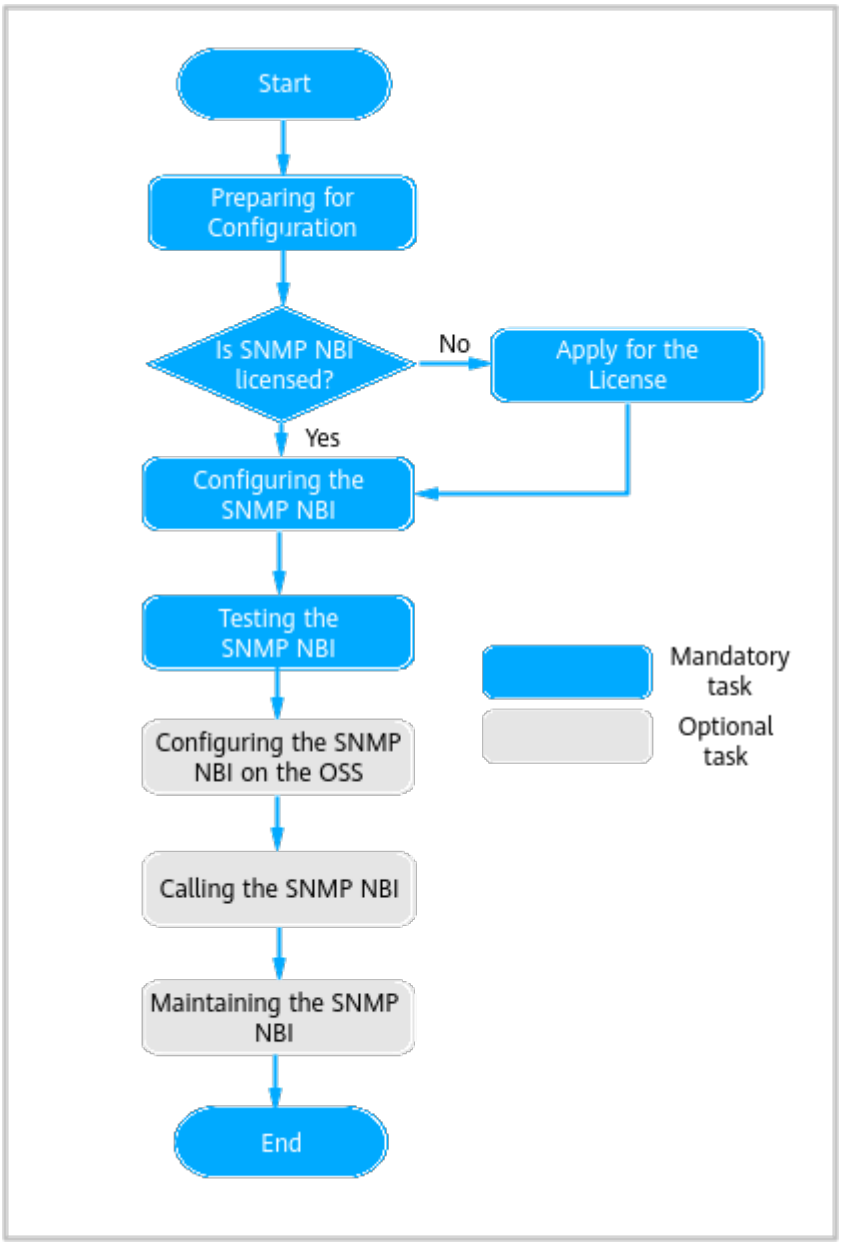
3 Configuration Process

The process of configuring the SNMP NBI includes checking the license, configuring the SNMP NBI, and verifying the SNMP NBI.

SNMP NBI Configuration Flowchart

Figure 3-1 shows the flowchart of configuring the SNMP NBI.

Figure 3-1 Flowchart of configuring the SNMP NBI



4 Preparing for Configuration

About This Chapter

Before configuring the SNMP NBI, you need to collect related configuration data. Modifying some configuration items as alarm field, encoding format, MIB frame, may require the restart of services. Therefore, to prevent service interruption, you need to apply for modifications in advance.

4.1 Precautions
This section describes the precautions for configuring the SNMP NBI.

4.2 Collecting Interconnection Parameters
Interconnection parameters must be collected from the OSS maintenance engineers and confirmed before the SNMP NBI is configured to ensure that the input parameters are correct. Otherwise, the OSS cannot receive alarms from or connect to NCE.

4.3 Viewing Operation Rights
The **admin** user has all the NCE NBI operation rights by default. For non-admin users, you should view and configure the operation rights of the corresponding NBI before you can configure the NBI.

4.1 Precautions

This section describes the precautions for configuring the SNMP NBI.

Configuring the SNMP NBI may affect OSS and other components of NCE. Modifying configuration items may also depend on NCE components. Therefore, confirm whether the configuration items to be modified will bring such type of impact and submit a request to the customer for approval before configuring the SNMP NBI.

Table 4-1 Basic configuration parameters

Item	Impact	Description
Alarm Field	The alarm fields will be changed if you modify this configuration item. The OSS may fail to parse the alarm.	Confirms the alarm fields and the detailed fields with the OSS, and then set this configuration item.
Encoding Format	The encoding format of alarms reported by the SNMP NBI will be changed if you modify this configuration item. The OSS may fail to parse the alarm.	Confirms the character set of the OSS, and then set this configuration item correctly. The character sets supported include UTF-8, GBK, and ISO-8859-1. The character sets of the SNMP NBI and OSS must be the same. If the character set of the SNMP NBI is different from that of the OSS, garbled characters may be displayed during the parsing.
MIB Frame	The OSS may fail to parse the alarm reported by the SNMP NBI if you modify this configuration item.	MIB1, MIB2, and MIB3 are supported. Check the MIB type that the OSS uses. ● If it is **T2000-NETMANAGEMENT-MIB.mib**, set this configuration item to **MIB3**. ● If it is **HW-IMAPV1NORTHBOUND-TRAP-MIB.mib** or **HW-IMAPV2NORTHBOUND-TRAP-MIB.mib**, set this configuration item to **MIB1**. ● If it is **IMAP_NORTHBOUND_MIB-V1.mib** or **IMAP_NORTHBOUND_MIB-V2.mib**, set this configuration item to **MIB2**.

Impact of Maintenance Operations on the NBIs

The NBI system is installed automatically during the installation of NCE. You need to configure NBI parameters manually to enable the functions.

- If the NCE server is configured with multiple NICs and they are in different network segments, set the IP address for connecting to the OSS as the IP address selected by the NCE SNMP NBI for alarm reporting (By default, the IP address is the northbound network communication IP address. If you manually change the IP address, you need to reconfigure the NBI synchronously.) is the IP address of the NIC for connecting to the OSS of the NCE server to ensure that the NCEserver and the OSS can communicate with each other. Otherwise, the OSS cannot interconnect with the NBI.
- You must configure the NBI again after the IP address of NCE is changed. By default, the northbound communication IP address specified during NCE installation is used as **Address for receiving requests** and **Address for sending traps**. If the northbound communication IP address is changed, you

need to manually update **Address for receiving requests** and **Address for sending traps** as follows:

a. Management plane: Choose **Maintenance** > **Network Configuration** > **Configure IP Address** or **Configure Floating IP Address** from the main menu. Select **Modify IP Address**.

b. O&M plane: Open the O&M plane app and choose **System Settings > Northbound Interface > SNMP NBI > Basic Settings** from the main menu and modify **Address for receiving requests** and **Address for sending traps** in the right pane.

4.2 Collecting Interconnection Parameters

Interconnection parameters must be collected from the OSS maintenance engineers and confirmed before the SNMP NBI is configured to ensure that the input parameters are correct. Otherwise, the OSS cannot receive alarms from or connect to NCE.

Table 4-2 and **Table 4-3** list the information to be collected.

For details about the parameter description, see **6.2 Configuration Parameters**.

Context

NOTICE

- Collect general parameters only and use default values for advanced parameters.
- For NCE upgrades, select the MIB structure carefully. For details, see **6.2.2 Advanced Settings**.
- For security purposes, from NCE V100R019C00, the SNMP NBI does not support the following insecure configuration items by default:
  - **Protocol version**: **SNMPv1** and **SNMPv2c**
  - **Security level**: **Not authenticated nor encrypted** and **Authenticated but not encrypted**
  - **Authentication protocol**: **MD5**, **SHA**, and **SHA2-224**
  - **Encryption protocol**: **DES**

    If you need insecure protocols, log in to the O&M plane, open the Security Management app, and choose **Configuration Compliance** > **Security Configuration** from the main menu. On the **Configuration Check** page, click **SNMP NBI-SNMP security configuration** and enable **SNMP Insecure Switch**. Then open the System Settings app, choose **System Settings** > **Northbound Interface** from the main menu, choose **SNMP NBI** > **Basic Settings** from the navigation pane, and configure protocols. If insecure protocols are not needed, disable **SNMP Insecure Switch**. A high-risk alert will be displayed if insecure protocols are enabled.
- SNMPv3 is recommended, because it is more secure than SNMPv1 and SNMPv2c.

Table 4-2 General parameters

Parameter	Description	Default Value
Address for receiving requests	IP address used by the SNMP agent to receive requests from the OSS. If there are multiple NICs, select an IP address that is able to communicate with the OSS.	IP address of NCE
Address for sending traps	IP address used to send traps and informs. If this parameter is set to an invalid value, the northbound communication IP address will be used. If there are multiple NICs, select an IP address that is able to communicate with the OSS.	IP address of NCE
Port for receiving requests	Port of the SNMP service. It is used to receive requests from the OSS. The default value is recommended.	9812
Port for sending traps	Port used to send traps and informs. The default value is recommended.	6666

Table 4-3 Advanced parameters

Parameter		Description	Default Value
SNMP Agent Settings	MIB type	Type of MIB structure to load. You are advised to use MIB2 to manage RAN and core network devices. • **MIB1**: supports the OIDs corresponding to **HW-IMAPV2NORTHBOUND-TRAP-MIB.mib**. • **MIB2**: supports the OIDs corresponding to **IMAP_NORTHBOUND_MIB-V2.mib**. • **MIB3**: supports the OIDs corresponding to **T2000-NETMANAGEMENT-MIB.mib**. It is used only for transport devices.	MIB1
	Alarm reporting interval (ms)	Interval for sending traps to the OSS. The value can range from 0 ms to 1000 ms.	0
	Time type	Type of the alarm reporting time.	UTC time

Parameter		Description	Default Value
	Time format	Format of the alarm reporting time. Currently, UTC time, local time without time zone, and local time with time zone are supported. For details, see **6.2.2 Advanced Settings**.	UTC time in the format of yyyy/MM/dd - hh:mm:ssZ
	Maximum length of reported alarm fields	Maximum length of a character string that in the VB.	4096
	Query active alarms	Whether to query active alarms. • **No**: Current alarms will be queried. • **Yes**: Active alarms will be queried.	Yes
	Alarm encoding format	Character set encoding format of the reported alarm traps. • UTF-8 • ISO-8859-1 • GBK	UTF-8
	Record PDU in logs	Whether to print PDU trace records in logs. • **No**: PDU trace records will not be printed in logs. • **Yes**: PDU trace records will be printed in logs.	No
	Filter correlative alarms	Whether to report correlative alarms. • **Yes**: Only common alarms and root alarms are reported. • **No**: Common alarms, root alarms, and correlative alarms are reported.	No
	Number of cached alarms	Cache size for real-time alarms. The value can range from 10000 to 50000.	10000
Inform/Trap Settings	Alarm reporting mode	• **Inform**: Alarms are reported in informs. • **Trap**: Alarms are reported in traps.	Trap

Parameter		Description	Default Value
	Timeout period (s)	This parameter is specified in the SNMP inform protocol. It determines the timeout period for sending inform packets. The value can range from 1 to 5 seconds.	5
	Number of retries	This parameter is specified in the SNMP inform protocol. It determines the maximum number of times that an inform packet can be retransmitted. The value can range from 0 to 5.	3
SNMPv3 Parameter Settings	Security level	Authenticated and encrypted.	Authenticated and encrypted
	Authentication protocol	Authentication protocol. ● SHA2-256 ● SHA2-384 ● SHA2-512	SHA2-512
	Encryption protocol	Encryption protocol. AES-128, AES-192, and AES-256 are supported.	AES-256
	RFC specifications	Whether the engine ID complies with the specifications of requests for comments (RFC). ● **Yes**: Converts the engine ID into a value that complies with the RFC specifications to report to the OSS. ● **No**: Directly reports the engine ID to the OSS.	Yes

Parameter		Description	Default Value
	Engine ID	Engine ID, which is the unique identifier of an SNMP entity. **NOTE** The value of **Engine ID** contains 5 to 32 characters. Only combinations of the following characters are allowed: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters =~!@#%^&*()-_+[{}]:./?,.	Engine ID automatically identified by the system. The default value is the IP address of the first NIC on the Common_Service node where CommonNBI service resides.
Heartbeat Period Settings	Report heartbeat notifications	Whether to send heartbeat traps. The options are as follows: • **Disable**: Heartbeat traps will not be sent. • **Enable**: Heartbeat traps will be sent.	Enable
	Heartbeat period (second)	Period for sending heartbeat traps. • The value of MIB1 ranges from 3 seconds to 300 seconds. • The value of MIB2 ranges from 3 seconds to 3600 seconds.	60
	Heartbeat ID	ID of a heartbeat trap.	SNMP Agent
SNMP NBI Advanced Parameter Settings	Parameter	Name of the configuration item of the SNMP interface.	-
	Value	Name of the configuration item of the SNMP interface.	-
MIB Alarm Reporting Settings		Name of the NE where an alarm is generated.	-

4.3 Viewing Operation Rights

The **admin** user has all the NCE NBI operation rights by default. For non-admin users, you should view and configure the operation rights of the corresponding NBI before you can configure the NBI.

Step 1 Log in to the O&M plane.

Step 2 Open the Security Management app and choose **User Management** from the main menu..

Step 3 On the **Users** tab, click the username, and view the roles that the user is bound to.

Step 4 On the **Roles** tab, click the role name, and view the operation rights of the role.

Table 4-4 Description of the SNMP NBI operation rights

Name of the Operation Right	Description
Modify SNMP interface configuration items	Provides permission to modify the interconnecting information of the third-party on O&M plane.
Query SNMP interface configuration items	Provides permission to query the interconnecting information of the third-party on O&M plane.

----End

5 Checking the License

NCE controls the functions and available resources of the SNMP NBI through a license. Before using the SNMP NBI, ensure that you have obtained its license and the SNMP NBI configurations in the license meet requirements.

Prerequisites

- NCE has been installed.
- The NCE license has been loaded.
- NCE has NE management licenses and functions properly.

Context

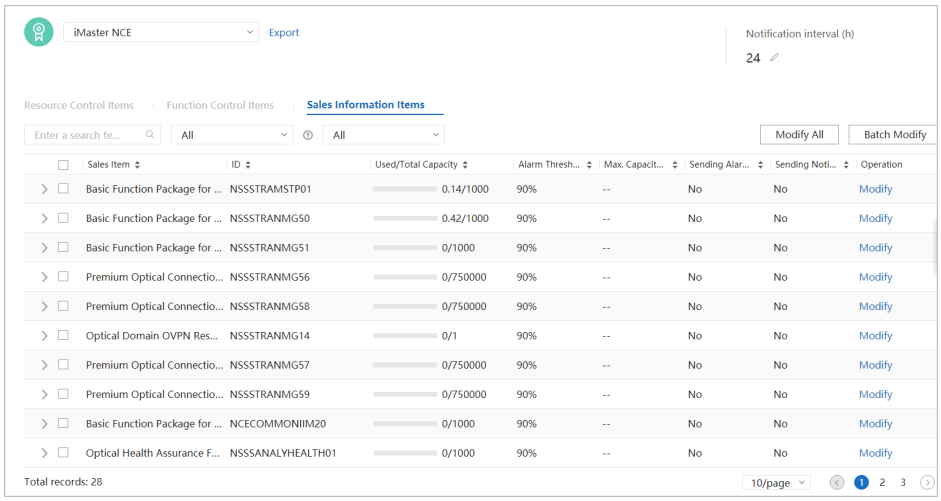
- When the NCE has a northbound license but the consumption reaches the alarm threshold, the system reports a northbound license threshold alarm. The alarm is reported successfully only when **Sending Alarms** is set to **Yes** in **System Settings** > **License Management** > **License Information** on the NCEO&M plane.
- In NCE capacity expansion, NBI licenses need to be expanded.

Procedure

Step 1 Log in to the NCE O&M plane.

Step 2 Open the System Settings app and choose **System Settings** > **License Management** from the main menu.

Step 3 On the **License Information** page, click the **Sales Information Items** tab of the current product.



Step 4 On the **Sales Information Items** tab page, check whether any resource name contains the license sale item corresponding to the NBI. If the results can be found, NCE has the permission to use the SNMP alarm interface. For details about the description of the license sale items, see **Table 5-1** and **Table 5-2**.

Table 5-1 License sale items for carriers

License Sale Item	Abbreviation	Value	Domain
NCE-FAN Unified Northbound API Suite (per Equivalence), Perpetual License	NSSS0FANAPI1	0–20000	NCE-FAN
NCE-FAN Unified Northbound API Suite (per 50 equivalent NEs), Perpetual License	NSSSCOMMON15	0–20000	NCE-FAN
Basic Northbound Interface for Manager (Includes SNMP, CORBA, XML, etc.), per 50 equivalent NEs, Perpetual License	NSSSTRANIPNBIPL01	0–20000	NCE-IP
NCE-T Basic Northbound Interface for Manager(Includes SNMP, CORBA, XML, etc.),per 50 equivalent NEs,Perpetual License	NSSSTRANOTNNBIPL01	0–20000	NCE-T
NCE-T Basic Northbound Interface for Manager(Includes SNMP, CORBA, XML, etc.),per 1 equivalent NEs,Perpetual License	NSSSTRANOTNNBIPLL01	0–20000	NCE-T
NCE-RTN Basic Northbound Interface for Manager(Includes SNMP, CORBA, XML, etc.),per 50 equivalent NEs,Perpetual License	NSSSTRANMWNBIPL01	0–20000	NCE-T

Table 5-2 License sale items for enterprises

License Sale Item	Abbreviation	Value	Domain
NCE-FAN Unified Northbound API Suite (per Equivalence), Perpetual License	NSSSEFANAPI1	0–20000	NCE-FAN
Access Network Unified Northbound API Suite (per 5 equivalent NEs), Perpetual License	NSSSANUNAS04	0–20000	NCE-FAN
Access Network Unified Northbound API Suite (per 20 equivalent NEs), Perpetual License	NSSSANUNAS01	0–20000	NCE-FAN
NCE-FAN Unified Northbound API Suite (per 50 equivalent NEs), Perpetual License	NSSSENUNAS01	0–20000	NCE-FAN
Basic Northbound Interface for Manager (Includes SNMP, CORBA, XML, etc.), per 5 equivalent NEs, Perpetual License	NSSSTENPNBIPLS07	0–20000	NCE-IP
Basic Northbound Interface for Manager(Includes SNMP, CORBA, XML, etc.),per 5 equivalent NEs,Perpetual License	NSSSTRANIPNBIPL71P5Eq	0–20000	NCE-IP
Basic Northbound Interface for Manager (Includes SNMP, CORBA, XML, etc.), per 20 equivalent NEs, Perpetual License	NSSSTRANSENPNBIPL07	0–20000	NCE-IP
Basic Northbound Interface for Manager (Includes SNMP, CORBA, XML, etc.), per 50 equivalent NEs, Perpetual License	NSSSTRANIPNBIPL71	0–20000	NCE-IP
Basic Northbound Interface for Manager (Includes SNMP, CORBA, XML, etc.), per 1 equivalent NE, Perpetual License	NSSSNORTH101	0–20000	NCE-T
NCE-NCE-T Basic Northbound Interface for Manager(Includes SNMP, CORBA, XML, etc.),per 5 equvalent NEs,Perpetual LicenseT Basic Northbound Interface for Manager(Includes SNMP, CORBA, XML, etc.),per 5 equvalent NEs,Perpetual License	NSSSTRANOTNNORTHL01	0–20000	NCE-T

License Sale Item	Abbreviation	Value	Domain
Transport domain Basic Northbound Interface for Manager (Includes SNMP, CORBA, XML, etc.), per 50 equivalent NEs, Perpetual License	NCEENTNORTH001	0–20000	NCE-T
NCE-RTN Basic Northbound Interface for Manager(Includes SNMP, CORBA, XML, etc.), per 5 equivalent NEs, Perpetual License	NSSSTRANMWNLITEL01	0–20000	NCE-T

Step 5 If the license does not contain the items for the required functions or resources, contact Huawei engineers to apply for a license. For details about the license introduction and how to apply for a license, see iMaster NCE License Instructions of the corresponding version.

----End

6 Configuring the SNMP NBI

About This Chapter

This chapter describes how to configure the SNMP NBI of NCE.

6.1 Configuration Operations
After NCE is installed, you need to configure the SNMP NBI parameters according to the NCE plan to enable the SNMP NBI.

6.2 Configuration Parameters
NCE can connect to the OSS after you correctly set general parameters on the NCE NBI configuration page. You can also set advanced parameters to customize the messages queried or reported through the SNMP NBI.

6.3 Configuring a Security Policy
Security settings allow you to configure the lockout policy for the login IP address after the SNMP NBI authentication fails. By default, if incorrect passwords are entered for consecutive three times within 60 minutes, the login IP address will be locked for 5 minutes.

6.4 Configuration Sample
This section describes how to configure the SNMP NBI by using a configuration sample.

6.1 Configuration Operations

After NCE is installed, you need to configure the SNMP NBI parameters according to the NCE plan to enable the SNMP NBI.

Prerequisites

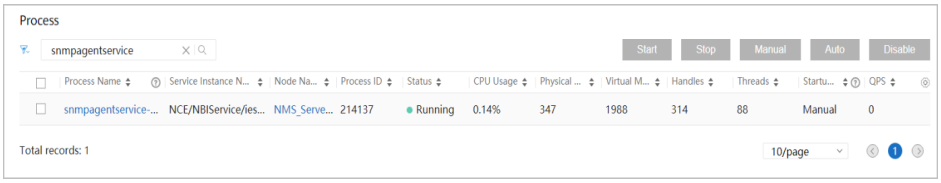
- The NCE license includes the SNMP NBI function.
- SNMP NBI processes are running.
  - In the single-site scenario, SNMP NBI processes are in the manual startup mode and stopped by default. To use the SNMP NBI, you need to start the SNMP NBI processes and change their startup modes to automatic. For details, see **10.4 Changing the Startup Modes of NBI Processes**.
  - In other scenarios, SNMP NBI processes are in the automatic startup mode and started by default. No manual operation is required.

FAQ

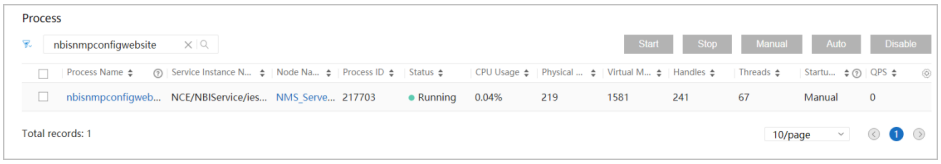
This section describes how to check whether the SNMP service is enabled.

Step 1 Log in to the NCE management plane and check the SNMP service status. If **Status** is **Running**, the SNMP NBI has been successfully started.

1. Log in to the NCE management plane.
2. Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.
3. In the navigation pane, choose **Service Monitoring**.
4. Click the **Process** tab and find the snmpagentservice process.
5. Check the status of the snmpagentservice process. (**Status** is **Running**.)



6. On the **Process** tab page, find the nbisnmpconfigwebsite process.
7. Check the status of the nbisnmpconfigwebsite process. (**Status** is **Running**.)



- If **Status** is **Not running**, refer to **10.6.1 SNMP NBI Processes Are Not Displayed**.
- If the SNMP NBI process fails to be started, refer to **10.6.2 SNMP Service Process Fails to Be Started**.

Step 2 Check whether heartbeat messages are received on the related OSS port. If no heartbeat message is received, refer to **10.6.4 OSS Cannot Receive Heartbeat Information**.

----End

NOTICE

- Set the MIB type to **MIB1** when loading the MIB1.
- Set the MIB type to **MIB2** when loading the MIB2.
- Set the MIB type to **MIB3** when loading the MIB3.
- When the MIB3 is loaded, the following advanced parameters are not supported:
  - Heartbeat Settings
- For security purposes, from NCE V100R019C00, the SNMP NBI does not support the following insecure configuration items by default:
  - **Protocol version**: **SNMPv1** and **SNMPv2c**
  - **Security level**: **Not authenticated nor encrypted** and **Authenticated but not encrypted**
  - **Authentication protocol**: **MD5**, **SHA**, and **SHA2-224**
  - **Encryption protocol**: **DES**

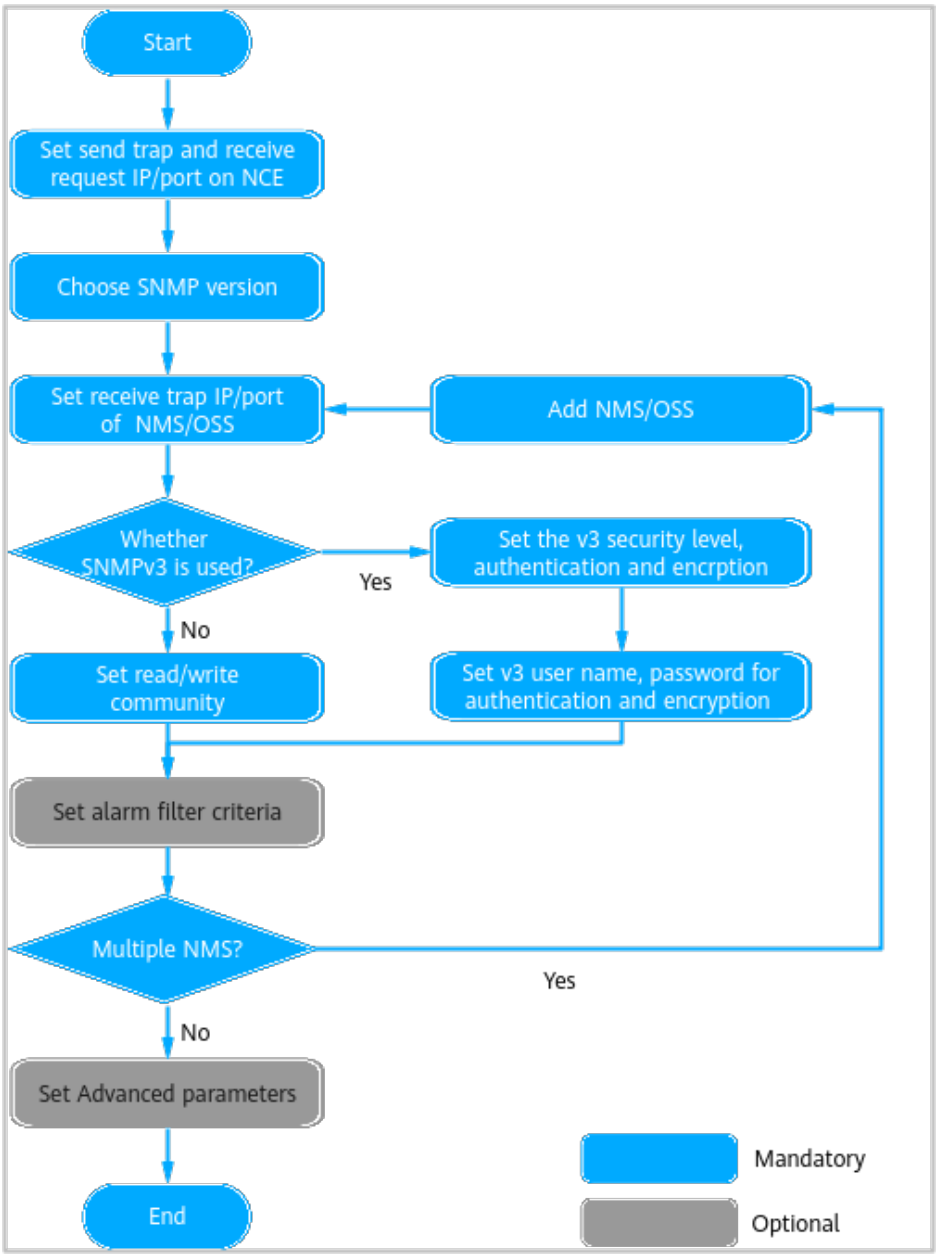
    If you need insecure protocols, log in to the O&M plane, open the Security Management app, and choose **Configuration Compliance** > **Security Configuration** from the main menu. On the **Configuration Check** page, click **SNMP NBI-SNMP security configuration** and enable **SNMP Insecure Switch**. Then open the System Settings app, choose **System Settings** > **Northbound Interface** from the main menu, choose **SNMP NBI** > **Basic Settings** from the navigation pane, and configure protocols. If insecure protocols are not needed, disable **SNMP Insecure Switch**. A high-risk alert will be displayed if insecure protocols are enabled.

Configuring the SNMP NBI

NCE provides the SNMP NBI configuration page to configure the interconnection parameters between NCE and the NMS. Select desired parameters based on customized requirements. Setting alarm filtering conditions and advanced parameters is optional and can be customized by operators.

Generally, advanced parameters are optional (default values are recommended). Advanced parameters are independent of each other and no configuration order is required.

Figure 6-1 Flowchart of configuring the SNMP NBI



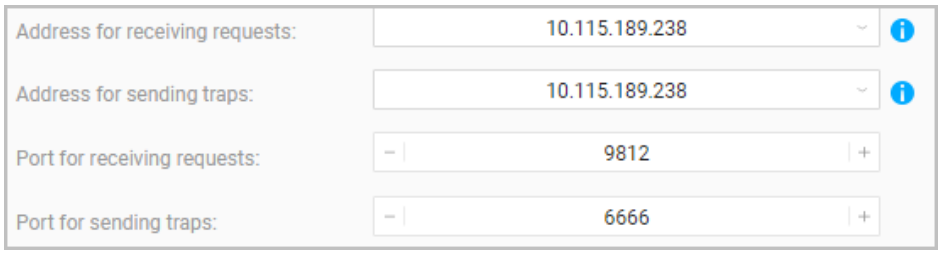
Procedure

Step 1 Log in to the NCEO&M plane as the **admin** user.

Step 2 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu..

Step 3 In the navigation pane, choose **SNMP NBI** > **Basic Settings**.

Step 4 On the **Basic Settings** page, set the IP addresses and port numbers for receiving requests and sending traps.



For details about SNMP agent parameters, see **6.2.1 General Parameters**.

1. Set the trap sending address/port and request receiving address/port.

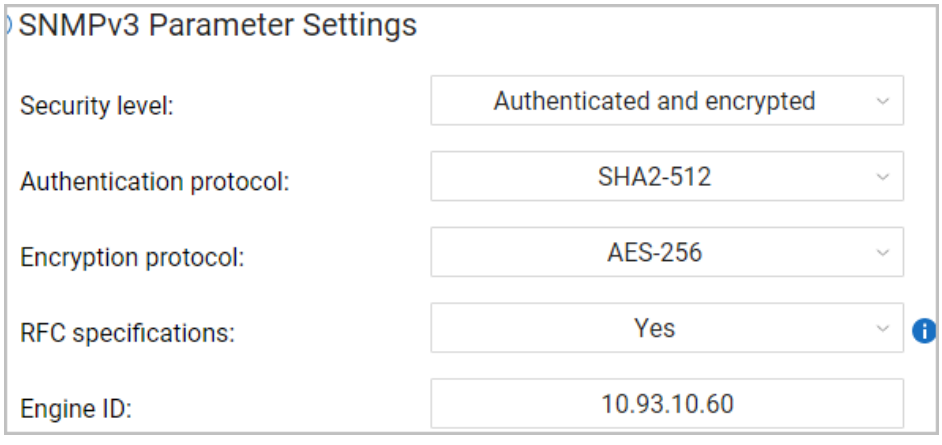
   By default, the trap sending port is **6666** and the request receiving port is **9812**.

NOTICE

- **Address for receiving requests** and **Address for sending traps** both are the IP address of the NCE server. (You are advised to use the default address, that is, the planned network communication IP address of the SNMP NBI. In Manager+Controller+Analyzer without IP address convergence, however, use the northbound floating IP address instead. If you select other IPv4 addresses, NCE may fail to communicate with third-party systems. The SNMP NBI supports both IPv4 and IPv6. If third-party system A requires IPv4 but third-party system B requires IPv6, you can select both IPv4 and IPv6 addresses for the two systems to communicate with NCE at the same time.) Ensure that this IP address can be used for successful communication between NCE and the OSS.
- When configuring ports for the SNMP NBI, refer to *iMaster NCE Communication Matrix* to prevent port conflicts.
- On NCE, the recommended port range is 1025–32767.

2. In the case of SNMPv3, set the security level, authentication protocol, and encryption protocol. By default, NCE supports SNMPv3.

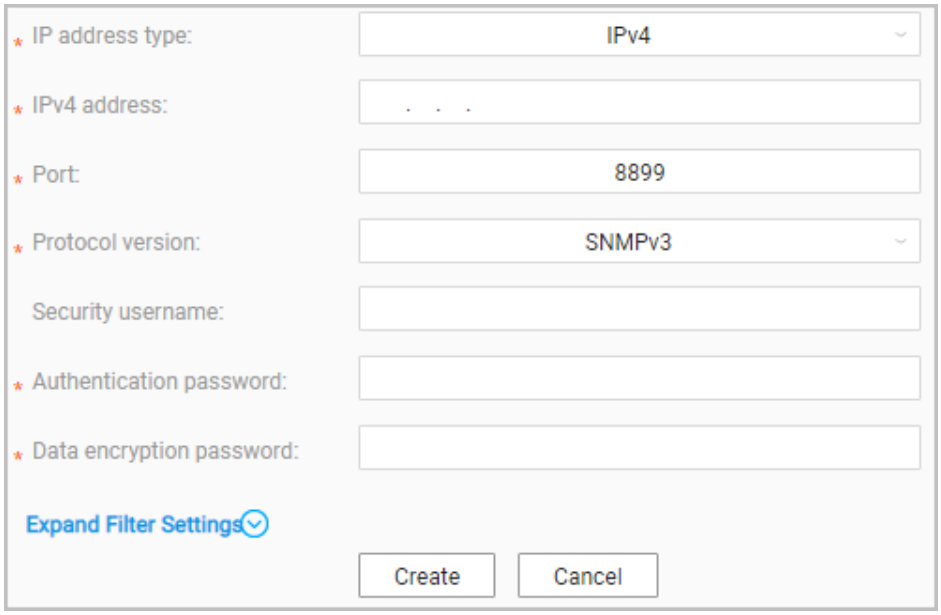
   In the **Advanced Settings** area, expand **SNMPv3 Parameter Settings**. For details about SNMPv3 parameters, see **SNMPv3 Parameter Settings**.



NOTICE

In the case of SNMPv3, it is recommended that the OSS use the more secure SHA and AES algorithms.

Step 5 In the navigation pane, choose **Third-party System Settings**. In the right pane, click **Create** and set OSS parameters.



For details about third-party NMS parameters, see **6.2.3 Third-Party NMS**.

1. Set the server parameters of the third-party NMS.

   IPv4 address is the IP address of the third-party NMS.

   NOTE

   - **IPv4 address** is not the IP address of the NCE server but the IP address of the third-party NMS. If the third-party NMS uses two servers to receive traps and send requests, the IP addresses for these two servers must be configured separately.
   - To configure multiple third-party system users, you are advised to set different read-write community names (v1 or v2) for them, use different user names (v3), or ensure not all user names are identical. If not all read-write community names (v1 or v2) are identical, duplicate user names (v3) exist, and the passwords for authentication and encryption are different, the interworking may fail for some users.
   - A maximum of 10 third-party NMSs are supported.

2. Set SNMP security parameters.

   The following are the default security parameters. Using SNMPv3 is recommended for security concern.

   - In the case of SNMPv1 and SNMPv2c, configure the read and write communities.
   - In the case of SNMPv3, set **V3 User Name**, **V3 Authentication Password**, and **V3 Privacy Password**. The default username is **admin**.

NOTICE

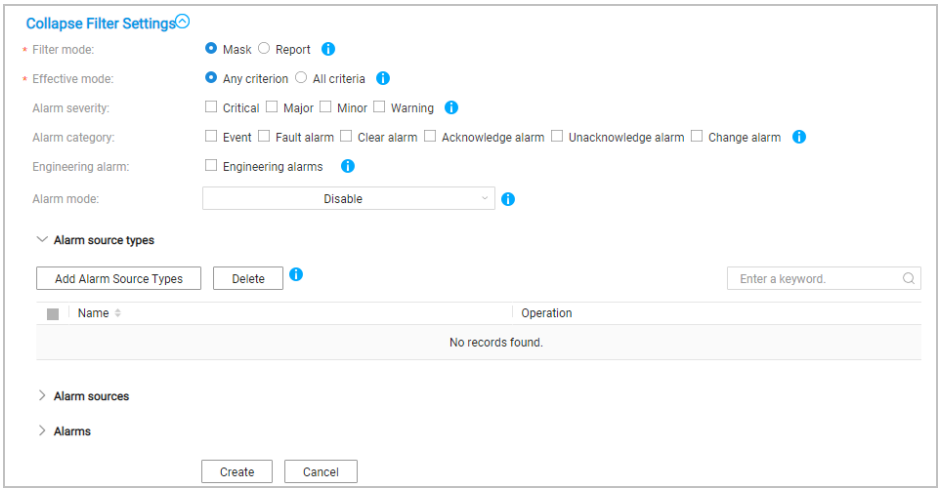
In the case of SNMPv3, the username cannot be left blank.

For security purposes, change the password regularly.

To prevent the password from being cracked, the password must meet the following requirements:

1. Contain 8 to 64 characters.
2. Not be the same as the username or the reverse of the username.
3. Not be repeated strings of any length, for example, aaaaaaaa, abababab, or abcdabcd.
4. Contain at least three of the following: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and special characters ~@#^*-_=+[{]};:./?.

3. On the page for creating an OSS, click Expand Filter Settings to set the alarm filter criteria.



NOTE

For details about how to set alarm/event northbound filtering rule settings, see "Setting Alarm/Event Northbound Filtering Rules" in iMaster NCE Online Help.

4. (Optional) Repeat the preceding substeps to add, modify, or delete the OSS.

Step 6 (Optional) On the **Basic Settings** page, set parameters in the **Advanced Settings** area.

1. Specify whether to enable the heartbeat reporting, and set the reporting period.

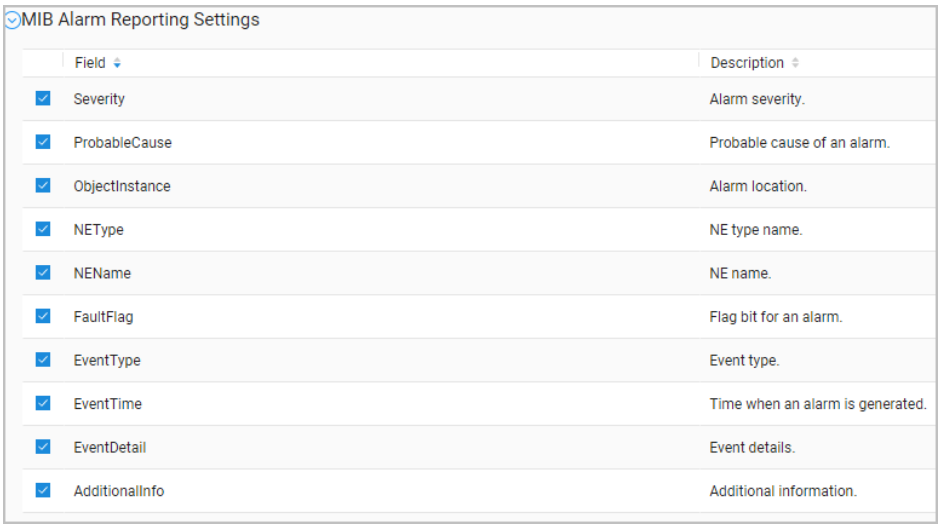
NOTE

The MIB3 does not support this function.

Parameter	Description	Default Value
Report heartbeat notifications	Whether to send heartbeat traps. **Disable**: Heartbeat traps will not be sent. **Enable**: Heartbeat traps will be sent.	Enable
Heartbeat period (second)	Period for sending heartbeat traps. The value of MIB1 ranges from 3 seconds to 300 seconds. The value of MIB2 ranges from 3 seconds to 3600 seconds. The default value is 60 seconds.	60
Heartbeat ID	ID of a heartbeat trap.	SNMP Agent

2. Set the alarm fields to be reported.

   In the **Advanced Settings** area of the **Basic Settings** page, expand **MIB Alarm Reporting Settings** and select the fields to be reported.



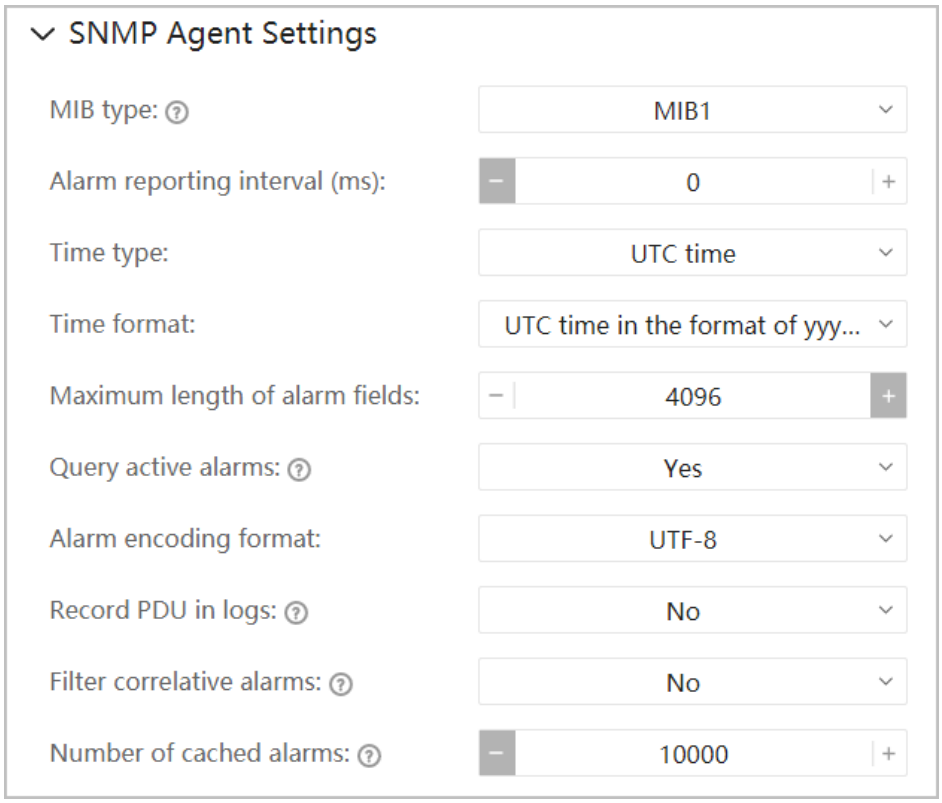
3. Set the reporting mode and other relevant parameters.

   Both SNMPv2c and SNMPv3 support the inform mode. The inform parameters include **Alarm reporting mode**, **Timeout period (s)** and **Number of retries**,

Parameter	Description	Default Value
Alarm reporting mode	– **Inform**: Alarms are reported in informs. – **Trap**: Alarms are reported in traps.	Trap
Timeout period (s)	This parameter is specified in the SNMP inform protocol. It determines the timeout period for sending inform packets. The unit is second. The default value is **5**, and the minimum value is **1**.	5
Number of retries	This parameter is specified in the SNMP inform protocol. It determines the maximum number of times that an inform packet can be retransmitted. The minimum value is **0**.	3

4. Set basic information about the SNMP agent.

   The SNMP agent parameters include **MIB type**, **Trap sending interval**, **Time type**, **Time format**, **Maximum length of reported alarm fields**, **Query active alarms**, **alarm encording format** ,**Record PDU in logs**, **Filter correlative alarms** and **Number of cached alarms**.



Parameter	Description	Default Value
Trap sending interval	Interval for sending traps to the OSS. The value can range from 0 ms to 1000 ms.	0
Time type	Type of the alarm reporting time. – UTC time – EMS time – NE system time	UTC time
Time format	Time format of the VB field that identifies alarm time. – UTC time in the format of yyyy/MM/dd - hh:mm:ssZ – Local time (without a time zone) in the format of yyyy/MM/dd - hh:mm:ss – Local time (without a time zone) in the format of yyyy-MM-dd,HH:mm:ss.0 – Local time (with a time zone) in the format of yyyy/MM/dd - hh:mm:ssTZ[DST] – Local time in the format of yyyy-MM-dd hh:mm:ss + hh:mm TZ + hh:mm DST – UTC time in the format of YYYY-MM-dd hh:mm:ss	UTC time in the format of yyyy/MM/dd - hh:mm:ssZ
Maximum length of reported alarm fields	Maximum length of a character string that in the VB.	4096
Query active alarms	Whether to query active alarms. **No**: Current alarms will be queried. **Yes**: Active alarms will be queried.	Yes
Alarm encoding format	Character set encoding format of the reported alarm traps. – UTF-8 – ISO-8859-1 – GBK **NOTICE** This character set defines the encoding format of alarm traps. After changing this configuration, OSS needs to be modified to the matching character set. Otherwise, the parsing may fail.	UTF-8

Parameter	Description	Default Value
Record PDU in logs	Whether to print PDU trace records in logs. – **No**: PDU trace records will not be printed in logs. – **Yes**: PDU trace records will be printed in logs.	No
MIB type	**MIB1**: The OSS uses the MIB file **HW-IMAPV1NORTHBOUND-TRAP-MIB.mib** or **HW-IMAPV2NORTHBOUND-TRAP-MIB.mib**. – For details about the supported alarm fields (VB), see **12.2 Alarm Fields Reported by MIB1**. – If cross-domain devices need to be managed, you are advised to set this parameter to **MIB1**. **MIB2**: The OSS uses the MIB file **IMAP_NORTHBOUND_MIB-V1.mib** or **IMAP_NORTHBOUND_MIB-V2.mib**. – For details about the supported alarm fields (VB), see **13.2 Alarm Fields Reported by MIB2**. – It is used for NCE-Super. **MIB3**: The OSS uses the MIB file **T2000-NETMANAGEMENT-MIB.mib**. – For details about the supported alarm fields (VB), see **14.2 Alarm Fields Reported by MIB3**. – It is used only for transport devices during the upgrades of certain scenarios.	MIB1
Filter correlative alarms	Whether to report correlative alarms. – **Yes**: Only common alarms and root alarms are reported. – **No**: Common alarms, root alarms, and correlative alarms are reported.	No
Number of cached alarms	Cache size for real-time alarms. The value can range from 10000 to 50000.	10000

NOTICE

The settings take effect only after you click **Save**.

5. Set advanced parameters about the SNMP interface.

   Advanced parameters are optional (default values are recommended). Select desired parameters based on customized requirements when interconnecting NCE with NMS.

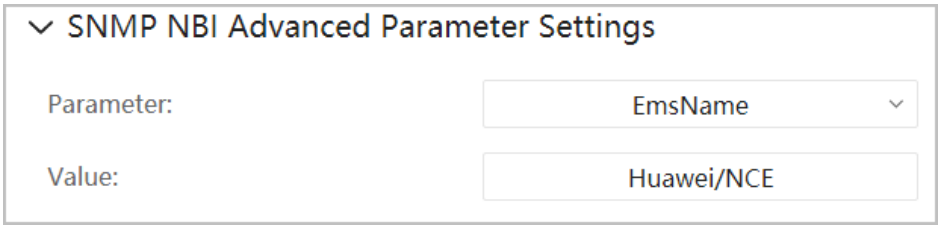


Table 6-1 MIB1 parameters

Parameter	Description	Default Value
EmsName	EMS name.	Huawei/NCE
Delimiter	Delimiter between character elements in the **ObjectInstance** and **ResourceIDs** fields. The default delimiter for **ObjectInstance** is space, and that for **ResourceIDs** is period (.). If the delimiter is longer than 1, the first letter of the delimiter is taken.	Space
ResIDFormat	Whether to display the resource information in FDN name-value format. **NOTE** This parameter applies only to HW-IMAPNORTHBOUND-TRAP-MIB and can be set to: – **0**: The **ResourceIDs** and **ObjectInstance** fields are represented as an FDN dotted notation, for example, **[3145731.-1.22.8.912.1.-1.-1]**. – **1**: The **ResourceIDs** and **ObjectInstance** fields are represented as an FDN name-value pair, for example, **[NE=312323,FR=1,S=1,CP=1,PP=4|1|2|]**. If an NBI compatibility ID has been set, NCE will adjust the EMS ID and FDN format based on the setting. For example, the EMS ID is changed from OSS to OMC and the FDN is changed from name-value format to dotted format.	0

Parameter	Description	Default Value
SupportX733Alarm	Whether the X733 standard is supported. This parameter can be set to: – **0**: The X733 standard is not supported. – **1**: The X733 standard is supported.	0
KeepAliveVBOID	Type of heartbeat VB OIDs. This parameter is set to **1.3.6.1.4.1.2011.2.15.1** by default. It can also be set to **1.3.6.1.4.1.2011.2.15.1.7.2.1**.	1.3.6.1.4.1.2011.2.15.1
NotifyOID	Trap OIDs for alarms (MIB1 configuration switch). This parameter can be set to: – **0**: The OID of the real-time alarm trap is 1.3.6.1.4.1.2011.2.15.1.7.1.0.1. – **1**: The OIDs of real-time alarm traps vary according to alarm severities. The OIDs of trap traps at different severities are as follows: **Critical**: 1.3.6.1.4.1.2011.2.15.1.7.1.0.3 **Major**: 1.3.6.1.4.1.2011.2.15.1.7.1.0.4 **Minor**: 1.3.6.1.4.1.2011.2.15.1.7.1.0.5 **Warning**: 1.3.6.1.4.1.2011.2.15.1.7.1.0.6 **Indeterminate**: 1.3.6.1.4.1.2011.2.15.1.7.1.0.7 **Unknown_Severity**: 1.3.6.1.4.1.2011.2.15.1.7.1.0.8	0
T2000Support	Whether to enable T2000 fields such as **ObjectInstance**, **ProbableCause**, **EventDetail**, **ProbableRepair**, and **EventName**.	1
SupportOldGroupID	Type of the MxU group ID. – **0**: new group ID – **1**: old group ID For example, for MA5616, the new group ID is **59**, and the old group ID is **71**.	0
severity_Critical	Alarm severity name.	Critical
severity_Major	Alarm severity name.	Major
severity_Minor	Alarm severity name.	Minor
severity_Warning	Alarm severity name.	Warning

Parameter	Description	Default Value
severity_Unreport	Alarm severity name.	Unknown_Severity
severity_Indeterminate	Alarm severity name.	Indeterminate
N2000Convert	Whether to convert fields such as **NEType**, **ProbableCause**, **EventDetail**, **ProbableRepair**, **EventName**, **ReasonID**, **FaultID**, and **DeviceType**. – **0**: Fields are not converted. – **1**: Fields are converted.	0
boardNameCompatibility	Content reported by the AdditionalVB1 field. – 0: Alarm object ID. – 1: Board type.	0

Table 6-2 MIB3 parameters

Parameter	Description	Default Value
EmsName	EMS name.	Huawei/NCE
ONEShelfTypeSupport	Value of the **ManagedObjectClass** field when an alarm on the WDM device under the optical NE is reported. – **0**: The optical NE type is reported. – **1**: The WDM NE type is reported.	0
oldPCSupport	Content of the **ProbableCause** field. – **0**: The content is consistent with the alarm cause on the client. – **1**: **ProbableCause** is compatible with earlier versions and its content complies with the TMF standard.	0

NOTICE

The settings take effect only after you click **Save**.

----End

6.2 Configuration Parameters

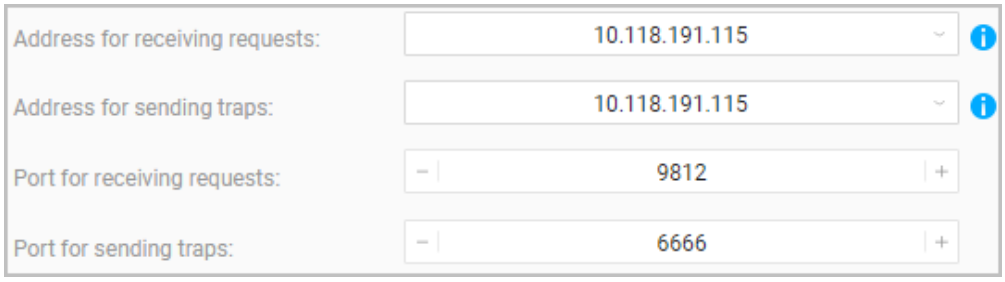
NCE can connect to the OSS after you correctly set general parameters on the NCE NBI configuration page. You can also set advanced parameters to customize the messages queried or reported through the SNMP NBI.

6.2.1 General Parameters

The SNMP NBI runs on NCE. It receives requests from the OSS, performs required operations on NCE, and reports alarms to the OSS in real time. General parameters for the SNMP NBI include the trap transmitting IP address or port, request receiving IP address or port, and SNMP version.

Navigation Path

On the NCE O&M plane, open the System Settings app, and choose **System Settings** > **Northbound Interface** > **SNMP NBI** > **Basic Settings**.



Parameter Description

NOTICE

Address for receiving requests and **Address for sending traps** both are the IP address of the NCE server. (You are advised to use the default address, that is, the planned network communication IP address of the SNMP NBI. In Manager +Controller+Analyzer without IP address convergence, use the northbound floating IP address instead. If you select other IPv4 addresses, NCE may fail to communicate with third-party systems. The SNMP NBI supports both IPv4 and IPv6. If third-party system A requires IPv4 but third-party system B requires IPv6, you can select both IPv4 and IPv6 addresses for the two systems to communicate with NCE at the same time.) Ensure that this IP address can be used for successful communication between NCE and the OSS.

When configuring ports for the SNMP NBI, refer to *iMaster NCE Communication Matrix* to prevent port conflicts.

On NCE, the recommended SNMP port range is 1025–32767.

Parameter	Description	Value
Address for sending traps	IP address on the SNMP agent for sending traps to the OSS. If there are multiple NICs, select an IP address that is able to communicate with the OSS. • In the Manager scenario, it is the northbound IP address of the NMS_Server node. • In the Manager+Controller +Analyzer scenario without IP address convergence, it is the northbound IP address of the Common_Service node. • In the Manager+Controller +Analyzer scenario with IP address convergence, it is the LVS-Northbound IP address of the GW node. The default IP address displayed on the page is the northbound IP address. To check whether the IP address is the same as the planned IP address, see **10.5 Checking the Northbound IP Address**.	IP addresses except 127.0.0.1 Default: IP address of the NCE server
Port for sending traps	Port used to send traps.	Port range: 1024–65535 Default: 6666

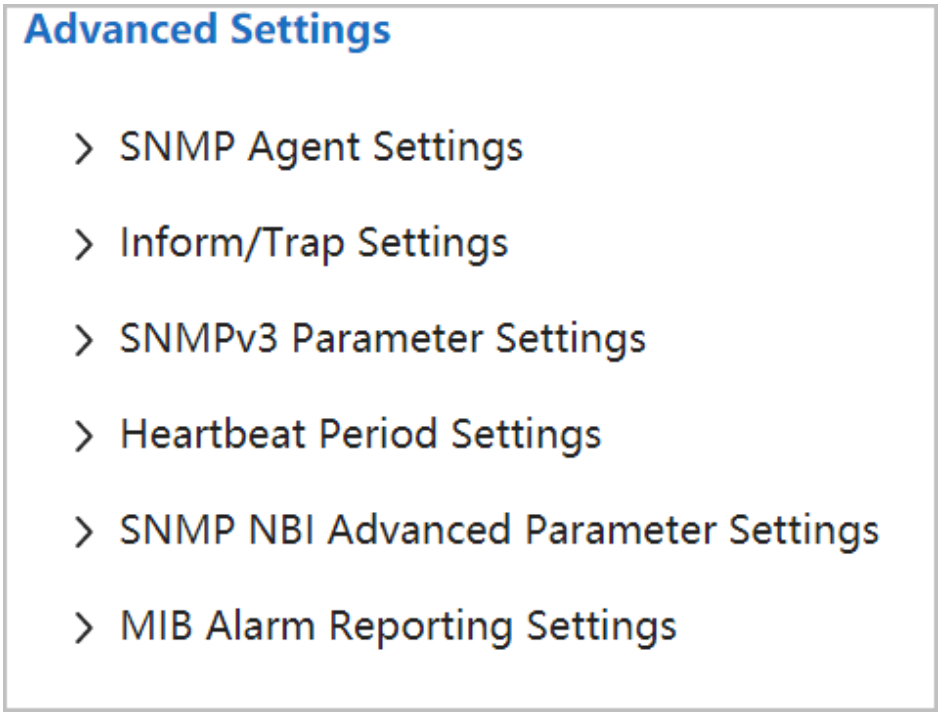
Parameter	Description	Value
Address for receiving requests	IP address used by the SNMP agent to receive requests from the OSS. If there are multiple NICs, select an IP address that is able to communicate with the OSS.	IP addresses except 127.0.0.1 Default: IP address of the NCE server
Port for receiving requests	Port used to receive requests from the OSS.	Port range: 1024–65535 Default: 9812

6.2.2 Advanced Settings

You can set the advanced parameters for the SNMP NBI on the SNMP NBI configuration page.

Navigation Path

1. Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu. on the O&M plane.
2. In the navigation pane, choose **SNMP NBI** > **Basic Settings**.
3. In the **Advanced Settings** area of the **Basic Settings** page, configure information as required.



SNMP Agent Settings

Parameter	Description	Default Value
MIB type	**MIB1**: The OSS uses the MIB file **HW-IMAPV1NORTHBOUND-TRAP-MIB.mib** or **HW-IMAPV2NORTHBOUND-TRAP-MIB.mib**. • For details about the supported alarm fields (VB), see **12.2 Alarm Fields Reported by MIB1**. • If cross-domain devices need to be managed, you are advised to set this parameter to **MIB1**. **MIB2**: The OSS uses the MIB file **IMAP_NORTHBOUND_MIB-V1.mib** or **IMAP_NORTHBOUND_MIB-V2.mib**. • For details about the supported alarm fields (VB), see **13.2 Alarm Fields Reported by MIB2**. **MIB3**: The OSS uses the MIB file **T2000-NETMANAGEMENT-MIB.mib**. • For details about the supported alarm fields (VB), see **14.2 Alarm Fields Reported by MIB3**. • It is used only for transport devices during the upgrades of certain scenarios.	MIB1
Alarm reporting interval (ms)	Interval for sending traps to the OSS. The value can range from 0 ms to 1000 ms.	0
Time type	• UTC time • EMS time • NE system time	UTC time

Parameter	Description	Default Value
Time format	Time format of the VB field that identifies alarm time. ● UTC time 1 in the format of yyyy/MM/dd - hh:mm:ssZ: uses local time without a time zone. ● Local time 3 (without a time zone) in the format of yyyy/MM/dd - hh:mm:ss: uses UTC time in a different format from that when this parameter is set to **0**. ● Local time (without a time zone) in the format of yyyy-MM-dd,HH:mm:ss.0 ● Local time (with a time zone) in the format of yyyy/MM/dd - hh:mm:ssTZ[DST] ● Local time in the format of yyyy-MM-dd hh:mm:ss + hh:mm TZ + hh:mm DST ● UTC time in the format of YYYY-MM-dd hh:mm:ss	UTC time in the format of yyyy/MM/dd - hh:mm:ssZ
Maximum length of reported alarm fields	255–4096	4096
Query active alarms	Whether to query active alarms. ● **Yes**: Active alarms will be queried. ● **No**: Current alarms will be queried. **NOTE** ● Active alarms refer to uncleared and unacknowledged alarms, and uncleared but acknowledged alarms. ● Current alarms refer to uncleared and unacknowledged alarms, cleared but unacknowledged alarms, and uncleared but acknowledged alarms.	Yes
Alarm encoding format	Character set encoding format of the reported alarm traps. ● UTF-8 ● ISO-8859-1 ● GBK	UTF-8
Record PDU in logs	Whether to print PDU trace records in logs. ● **No**: PDU trace records will not be printed in logs. ● **Yes**: PDU trace records will be printed in logs.	No

Parameter	Description	Default Value
Filter correlative alarms	Whether to report correlative alarms. • **Yes**: Only common alarms and root alarms are reported. • **No**: Common alarms, root alarms, and correlative alarms are reported.	No
Number of cached alarms	Cache size for real-time alarms. The value can range from 10000 to 50000.	10000

The correct MIB frame must be set when the SNMP NBI is configured. This ensures that the OSS connects to NCE for alarm management.

NOTICE

This setting has a direct impact on the successful communication between NCE and the OSS for alarm management. Confirm with the OSS when setting the MIB frame.

Three MIB files are supported by the SNMP NBI of NCE:

- T2000-NETMANAGEMENT-MIB.mib (MIB3)
- IMAP_NORTHBOUND_MIB-V1.mib and IMAP_NORTHBOUND_MIB-V2.mib (MIB2)
- HW-IMAPV1NORTHBOUND-TRAP-MIB.mib and HW-IMAPV2NORTHBOUND-TRAP-MIB.mib (MIB1)

Inform/Trap Settings

You can set the reporting mode and the relevant parameters.

NOTICE

- Trap mode: A received alarm is reported immediately regardless of whether the OSS returns a response to the previous alarm reporting.
- Inform mode: A received alarm is reported immediately after the OSS returns a response to the previous alarm reporting or the number of retry attempts is exceeded. In this mode, if the parameters configured for the OSS are incorrect, the SNMP agent tries connecting to the OSS for many times. This will occupy a large number of resources. As a result, the efficiency of the SNMP agent is reduced. Therefore, exercise caution when you set this parameter to **Inform**.
- The SNMPv1 supports the Trap mode only.

Parameter	Description	Default Value
Alarm reporting mode	• **Inform**: Alarms are reported in informs. • **Trap**: Alarms are reported in traps.	Trap
Timeout period (s)	This parameter is specified in the SNMP inform protocol. It determines the timeout period for sending inform packets. The unit is second. The default value is **5**, and the minimum value is **1**.	5
Number of retries	This parameter is specified in the SNMP inform protocol. It determines the maximum number of times that an inform packet can be retransmitted. The minimum value is **0**.	3

SNMPv3 Parameter Settings

NOTE

For security purposes, from NCE V100R019C00, the SNMP NBI does not support the following insecure configuration items by default:

- **Protocol version**: **SNMPv1** and **SNMPv2c**
- **Security level**: **Not authenticated nor encrypted** and **Authenticated but not encrypted**
- **Authentication protocol**: **MD5**, **SHA**, and **SHA2-224**
- **Encryption protocol**: **DES**

  If you need insecure protocols, log in to the O&M plane, open the Security Management app, and choose **Configuration Compliance** > **Security Configuration** from the main menu. On the **Configuration Check** page, click **SNMP NBI-SNMP security configuration** and enable **SNMP Insecure Switch**. Then open the System Settings app, choose **System Settings** > **Northbound Interface** from the main menu, choose **SNMP NBI** > **Basic Settings** from the navigation pane, and configure protocols. If insecure protocols are not needed, disable **SNMP Insecure Switch**. A high-risk alert will be displayed if insecure protocols are enabled.

Parameter	Description	Default Value
Security level	Security level. This parameter can only be set to **Authenticated and encrypted** by default.	Authenticated and encrypted
Authentication protocol	Authentication protocol. • SHA2-256 • SHA2-384 • SHA2-512	SHA2-512

Parameter	Description	Default Value
Encryption protocol	Encryption protocol of SNMPv3. AES-128, AES-192, and AES-256 are supported.	AES-256
RFC specifications	Whether the engine ID complies with the specifications of requests for comments (RFC). • **Yes**: Converts the engine ID into a value that complies with the RFC specifications to report to the OSS. • **No**: Directly reports the engine ID to the OSS.	Yes
Engine ID	Engine ID, which is the unique identifier of an SNMP entity. **NOTE** The value of **Engine ID** contains 5 to 32 characters. Only combinations of the following characters are allowed: lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), spaces and special characters =~!@#%^&*()-_+[{}]:./?,. **Engine ID** cannot start or ends with spaces.	Engine ID automatically identified by the system. The default value is the IP address of the first NIC on the Common_Service node where CommonNBI service resides.

Heartbeat Period Settings

NCE can periodically send heartbeat information to the OSS through the SNMP NBI. Based on the heartbeat information, the OSS determines whether the communication is successful. The heartbeat settings are applicable only to the MIB1 and MIB2.

NOTE

There is no heartbeat information for the MIB3.

Table 6-3 Heartbeat parameters

Parameter	Description	Default Value
Report heartbeat notifications	Whether to send heartbeat traps. **Disable**: Heartbeat traps will not be sent. **Enable**: Heartbeat traps will be sent.	Enable

Parameter	Description	Default Value
Heartbeat period (second)	Period for sending heartbeat traps. The value of MIB1 ranges from 3 seconds to 300 seconds. The value of MIB2 ranges from 3 seconds to 3600 seconds. The default value is 60 seconds.	60
Heartbeat ID	ID of a heartbeat trap.	SNMP Agent

SNMP NBI Advanced Parameter Settings

Parameter	Description	Default Value
Parameter	Name of the configuration item of the SNMP interface. **NOTE** The default value is **CsnType** if **MIB type** is **MIB2**.	CsnType
Value	Name of the configuration item of the SNMP interface. **NOTE** The default value is **0** if **MIB type** is **MIB2**.	0

MIB Alarm Reporting Settings

The reported alarm field, also called VB, specifies the alarm information to be reported through the SNMP NBI.

NOTICE

This parameter is applicable to all third-party NMSs connected to the SNMP NBI.

NCE automatically fills the alarm field.

Table 6-4 T2000Support=0

Name	Name in the MIB	Description	Value	Parsing Supported
NE Name	hwNmNorthboundNEName	Name of the NE where an alarm is generated. • For alarms generated on an NE, the NE name is reported. • For alarms generated due to NE disconnection, the NE name is reported. For example, if alarms are generated due to NE login failures or NE disconnection, the NE name is reported. • If alarms are generated on a WDM NE that is mounted to an optical NE, the name of the optical NE is reported. • For other NMS alarms, the NMS name is reported. By default, **OSS** is reported. If the NMS name is changed, the name of the changed NMS is reported.	Octet string	No
NE Type	hwNmNorthboundNEType	Type of the NE on which alarms are generated. For NMS alarms, the NMS name is reported.	Octet string	No
Object Instance	hwNmNorthboundObjectInstance	Location information. For details, see **Table 12-3**.	Octet string	No

Name	Name in the MIB	Description	Value	Parsing Supported
Event Type	hwNmNorthboundEventType	Alarm type. The options are as follows: ● Environment ● Equipment ● Communication ● Service ● Process ● Security For X.733-compliant alarms, options are as follows: ● EnvironmentalAlarm ● EquipmentAlarm ● CommunicationsAlarm ● Quality of Service Alarm ● ProcessingErrorAlarm ● SecurityAlarm	Octet string	Yes. See the enumerated value.

Name	Name in the MIB	Description	Value	Parsing Supported
Alarm Occurrence Time	hwNmNorthboundEventTime	Time when an alarm is generated, cleared, acknowledged, unacknowledged, or changed. ● If an alarm is generated, this parameter indicates the time when the alarm is generated. ● If an alarm is cleared, this parameter indicates the time when the alarm is cleared. ● If an alarm is acknowledged, this parameter indicates the time when the alarm is acknowledged. ● If an alarm is unacknowledged, this parameter indicates the time when the alarm is unacknowledged. ● If an alarm is changed, this parameter indicates the time when the alarm is changed. ● UTC time in the format of YYYY/MM/DD - hh:mm:ssZ, for example, 2009/12/23 - 11:30:30Z. ● Local time (without a time zone) in the format of YYYY/MM/DD - hh:mm:ss, for example, 2009/12/23 - 19:30:30. ● Local time (with a time zone) in the format of YYYY/MM/DD - hh:mm:ss hh:mmTZ[DST], where	Octet string	Yes. See the time format.

Name	Name in the MIB	Description	Value	Parsing Supported
		TZ indicates the time zone. DST indicates the offset between the DST and local time. For example: – 2009/12/23 - 19:30:30 + 08:00[0] (The date is not in DST.) – 2009/12/23 - 19:30:30 + 08:00[3600] (The DST offset is 1 hour. The DST value is represented in seconds.) ● Local time in the format of YYYY-MM-dd hh:mm:ss +hh:mm TZ +hh:mm DST, where TZ indicates the time zone. DST indicates the offset between the DST and local time. For example: – 2009-12-23 19:30:30 + 08:00 TZ (The date is not in DST.) – 2009-12-23 19:30:30 + 08:00 TZ + 01:00 DST (The DST offset is 1 hour.) ● UTC time in the format of YYYY-MM-dd hh:mm:ss, for example, 2009-12-23 11:30:30.		
Alarm Cause	hwNmNorthboundProbableCause	Possible causes of an alarm. Format: ID:[Alarm ID],DeviceType:[DeviceType ID], Alarm Cause	Octet string	No

Name	Name in the MIB	Description	Value	Parsing Supported
Alarm Severity	hwNmNorthboundSeverity	Alarm severity. • Critical • Major • Minor • Warning • Cleared: This option is supported for X.733-compliant alarms.	Octet string	Yes. See the enumerated value.
Alarm Details	hwNmNorthboundEventDetail	ID, device type, and details of an alarm. Format: ID: [AlarmID],DeviceType: [DeviceType ID],Alarm Details	Octet string	No
Alarm Location	hwNmNorthboundAdditionalInfo	Specific location of the NE where an alarm is generated.	Octet string	No
Type Flag	hwNmNorthboundFaultFlag	Alarm type. The options are as follows: • **Event**: indicates that an event is generated. • **Fault**: indicates that an alarm is generated. • **Recovery**: indicates that the alarm is cleared. • **Acknowledge**: indicates that the alarm is acknowledged. • **Unacknowledge**: indicates that the alarm is unacknowledged. • **Change**: indicates that the alarm is changed.	Octet string	Yes. See the enumerated value.
Alarm Function Category	hwNmNorthboundFaultFunction	Alarm type based on functions, which is the same as hwNmNorthboundEvent-Type.	Octet string	Yes. See the enumerated value.

Name	Name in the MIB	Description	Value	Parsing Supported
Managed Equipment Address	hwNmNorthboundDeviceIP	IP address of an NE. • For transport NEs – If the NE that generates the alarm is a GNE, the IP address of the GNE is reported. – If the NE that generates the alarm is a non-GNE, **0.0.0.0** is reported. • For other NEs, the IP address of the NE is reported. • For NMS alarms, the IP address of the NMS server is reported.	IP address	No
Alarm SN	hwNmNorthboundSerialNo	SN of an alarm.	Integer	No
Alarm Clearance Advice	hwNmNorthboundProbableRepair	Advice for clearing alarms. Format: ID:[AlarmID],DeviceType:[DeviceType ID],Alarm Clearance Advice	Octet string	No
Resource ID	hwNmNorthboundResourceIDs	ID of the resource on NCE.	Octet string	No
Event Name	hwNmNorthboundEventName	Name of an alarm. Format: ID:[AlarmID],DeviceType:[DeviceType ID],Event Name	Octet string	No
Alarm Cause ID	hwNmNorthboundReasonID	Alarm cause ID.	Integer	No
Alarm ID	hwNmNorthboundFaultID	Alarm ID.	Integer	No
Managed Equipment Type	hwNmNorthboundDeviceType	Type ID of the managed device.	Octet string	No

Name	Name in the MIB	Description	Value	Parsing Supported
Trail Name	hwNmNorthboundTrailName	Name of the trail affected by an alarm. If alarm A affects a trail, a new change alarm B will be generated. The SN of alarm B is the same as that of alarm A. The severity of alarm B is **Change**. **Trail Name** in alarm B indicates the affected trail. However, for alarm A, **Trail Name** is blank. ● This parameter is applicable for transport and IP NEs. ● This parameter is always blank for access NEs.	Octet string	No
Root Alarm	hwNmNorthboundRootAlarm	Whether the alarm is a root alarm. The options are as follows: ● **0**: non-root alarm ● **1**: root alarm	Integer	Yes. See the enumerated value.
Group ID	hwNmNorthboundGroupID	ID of the alarm group. ● For transport and IP NEs, the alarm group ID and the alarm ID uniquely identify a static alarm. ● For access NEs, the alarm group ID, alarm ID, and alarm cause ID uniquely identify a static alarm.	Integer	No

Name	Name in the MIB	Description	Value	Parsing Supported
Engineering Alarm Status	hwNmNorthboundMaintainStatus	Whether this alarm is generated by the NE in the engineering maintenance state. Maintenance engineers can focus on engineering alarms selectively. ● **0**: non-engineering alarm ● **1**: engineering alarm **NOTE** NEs during engineering commissioning or service cutover generate a large number of alarms, and you can set the NEs to the engineering maintenance state. Therefore, the alarms generated by this kind of NE are engineering alarms.	Integer	Yes. See the enumerated value.
Root Alarm SN	hwNmNorthboundRootAlarmSerialNo	SN of the root alarm.	Octet string	No
Alarm Acknowledgement Status	hwNmNorthboundConfirmStatus	Alarm acknowledgement status. ● **1**: acknowledged ● **2**: unacknowledged	Integer	Yes. See the enumerated value.
Alarm Clearance Status	hwNmNorthboundRestoreStatus	Alarm clearance status. ● **1**: cleared ● **2**: uncleared	Integer	Yes. See the enumerated value.
Alarm additional information 1	hwNorthboundAdditionalVB1	Alarm UUID of the physical resources (NEs, boards, and ports) in the IP domain.	String	No
Alarm additional information 2	hwNorthboundAdditionalVB2	Reserved field, which is not enabled currently.	String	No
Alarm additional information 3	hwNorthboundAdditionalVB3	Reserved field, which is not enabled currently.	String	No

Name	Name in the MIB	Description	Value	Parsing Supported
Alarm additional information 4	hwNorthboundAdditionalVB4	Reserved field, which is not enabled currently.	String	No
Alarm additional information 5	hwNorthboundAdditionalVB5	Reserved field, which is not enabled currently.	String	No
Alarm additional information 6	hwNorthboundAdditionalVB6	Reserved field, which is not enabled currently.	String	No
Alarm additional information 7	hwNorthboundAdditionalVB7	Reserved field, which is not enabled currently.	String	No
Alarm additional information 8	hwNorthboundAdditionalVB8	Reserved field, which is not enabled currently.	String	No

6.2.3 Third-Party NMS

The third-party NMS refers to the NMS (also called SNMP manager) in the SNMP protocol. For the SNMP NBI, the third-party NMS functions as the OSS. The third-party NMS sends requests to the SNMP agent, receives responses or traps from the SNMP agent, parses these packets, and displays the result.

Description

NOTE

The receive/send address is not the IP address of the NCE server but the IP address of the third-party NMS. If the third-party NMS uses two servers to receive traps and send requests, the IP addresses for these two servers must be configured separately.

A maximum of 10 third-party NMSs are supported. **Table 6-5** lists the configuration requirements of the third-party NMSs.

Table 6-5 Configuration requirements of the third-party NMSs

MIB Type	SNMP Version	Configuration Requirements
MIB1	v1/v2c	You are advised to set different read and write community names for third-party NMSs. If multiple third-party NMSs (for example, NMS 1 and NMS 2) use the same read and write community names, ensure that the SNMP protocol versions used by the NMSs are the same.
	v3	You are advised to set different usernames for third-party NMSs. If multiple third-party NMSs (for example, NMS 1 and NMS 2) use the same username, the same authentication password or encryption password must be set for all the NMSs.
MIB2	v1/v2c	You are advised to set different read and write community names for third-party NMSs. If multiple third-party NMSs (for example, NMS 1 and NMS 2) use the same read and write community names, ensure that the SNMP protocol versions used by the NMSs are the same.
	v3	You are advised to set different usernames for third-party NMSs. If multiple third-party NMSs (for example, NMS 1 and NMS 2) use the same username, the same authentication password or encryption password must be set for all the NMSs.
MIB3	v1/v2c	Different read and write community names must be set for third-party NMSs.
	v3	Different usernames must be set for third-party NMSs.

NOTICE

For security purposes, change the initial password upon the first login and update it periodically according to complexity requirements.

The password must meet the following requirements to safeguard your user account:

- Contain 8 to 64 characters.
- Contain at least three of the following:
  - Lowercase letters (a–z)
  - Uppercase letters (A–Z)
  - Digits (0–9)
  - Special characters such as!"#$%&'()*+,-./:;<=>?@[\]^`{_|}~
- The password cannot contain only repeated strings and cannot be the same as the username of the reverse of the username.

Table 6-6 describes the upper-layer NMS parameters.

NOTE

If you need insecure protocols, log in to the O&M plane, open the Security Management app, and choose **Configuration Compliance** > **Security Configuration** from the main menu. On the **Configuration Check** page, click **SNMP NBI-SNMP security configuration** and enable **SNMP Insecure Switch**. Then open the System Settings app, choose **System Settings** > **Northbound Interface** from the main menu, choose **SNMP NBI** > **Third-party System Settings** from the navigation pane, and configure protocols. If insecure protocols are not needed, disable **SNMP Insecure Switch**. A high-risk alert will be displayed if insecure protocols are enabled.

Table 6-6 Parameters for the upper-layer NMS

Parameter	Description	Default Value
IP address type	IP address type of the OSS. • IPv4 • IPv6	IPv4
IPv4 address (IPv6 address)	IP address used by the OSS to receive traps.	Blank
Port	Port used by the OSS to receive traps. **IPv4 address** (or **IPv6 address**) and **Port** determine the destination of real-time alarm traps, current alarm query traps, and heartbeat traps.	8899
Protocol version	SNMP version. Only SNMPv3 is supported by default.	SNMPv3
Security username	SNMPv3 security user.	Blank
Authentication password	Authentication password of the OSS user. This parameter is used when SNMPv3 authentication is enabled.	Blank

Parameter	Description	Default Value
Data encryption password	Data encryption password of the OSS user. This parameter is used when SNMPv3 encryption is enabled. It is recommended that the parameter value be different from that of **Authorization and authentication password**.	Blank

Filter Settings

NOTE

Filter settings ensure that the third-party or upper-layer NMS servers will receive the alarms they need.

Table 6-7 Filter settings

Parameter	Description	Default Value
Filter mode	How to filter alarms and events. The options are as follows: • Mask • Report	Mask
Effective mode	How the filter mode takes effect. The options are as follows: • Any criterion • All criteria	Any criterion

Parameter	Description	Default Value
Alarm severity	Severities used to filter alarms. Multiple severities can be selected. Alarms at the selected severities will be reported or masked, depending on the value of **Filter mode**. The options are as follows: • Critical • Major • Minor • Warning	• If **Filter mode** is set to **Mask**, all the options are deselected. • If **Filter mode** is set to **Report**, all the options are selected.
Alarm category	Categories used to filter alarms. Multiple categories can be selected. Alarms in the selected categories will be reported or masked, depending on the value of **Filter mode**. The options are as follows: • Event • Fault alarm • Clear alarm • Acknowledge alarm • Unacknowledge alarm • Change alarm	• If **Filter mode** is set to **Mask**, all the options are deselected. • If **Filter mode** is set to **Report**, all the options are selected.
Engineering alarm	Whether to filter engineering alarms. The option is as follows: • Engineering alarms	• If **Filter mode** is set to **Mask**, the option is deselected. • If **Filter mode** is set to **Report**, the option is selected.

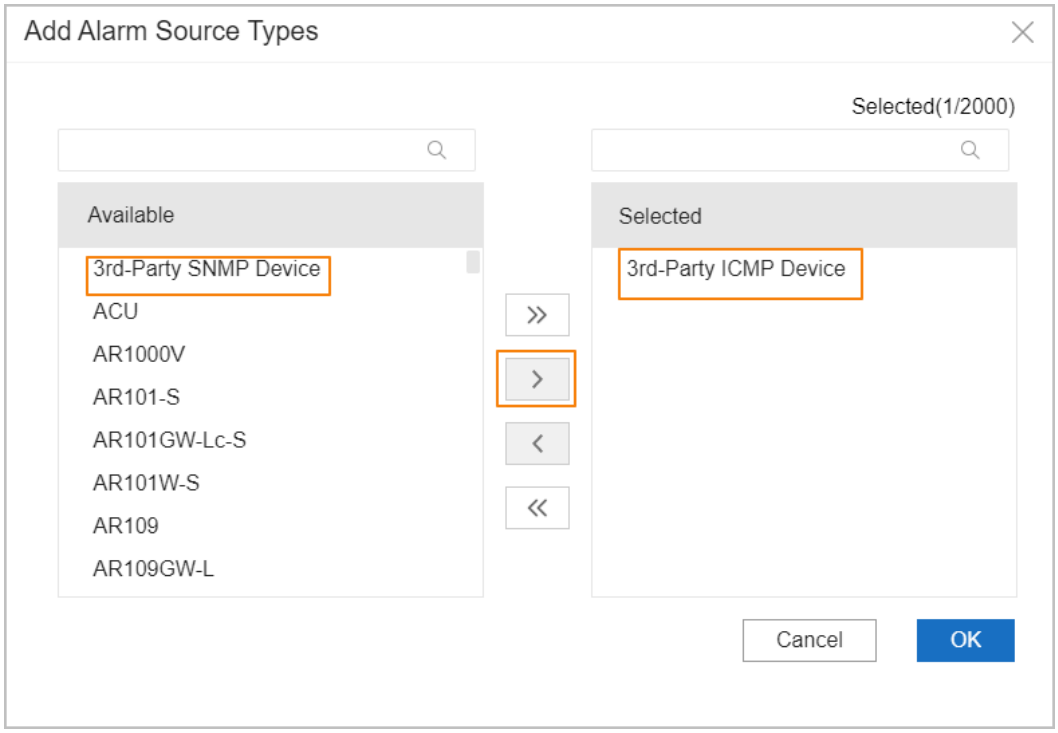
Parameter	Description	Default Value
Alarm mode	Modes used to filter alarms and events. Multiple modes can be selected. Alarms in the selected modes will be reported or masked, depending on the value of **Filter mode**. • All • NORMAL • GSM • UMTS • LTE • COMM • NB-loT Cell • FDD Cell • TDD Cell • RFA • LTE Other • NR	Blank
Add source types	Source types used to filter alarms. Multiple source types can be selected. Alarms from the selected types of sources will be reported or masked, depending on the value of **Filter mode**. For details, see **Alarm Source Types**.	Blank
Alarm sources	Sources used to filter alarms. Multiple sources can be selected. Alarms from the selected sources will be reported or masked, depending on the value of **Filter mode**. For details, see **Alarm Sources**.	Blank

Parameter	Description	Default Value
Alarms	Alarms or events to filter. Multiple alarms or events can be selected, which will be reported or masked, depending on the value of **Filter mode**. For details, see **Alarms**.	Blank

Alarm Source Types

Step 1 In the **Alarm source types** area, click **Add Alarm Source Types**.

Step 2 In the **Available** area, select the NEs whose alarms need to be masked or reported, and click .



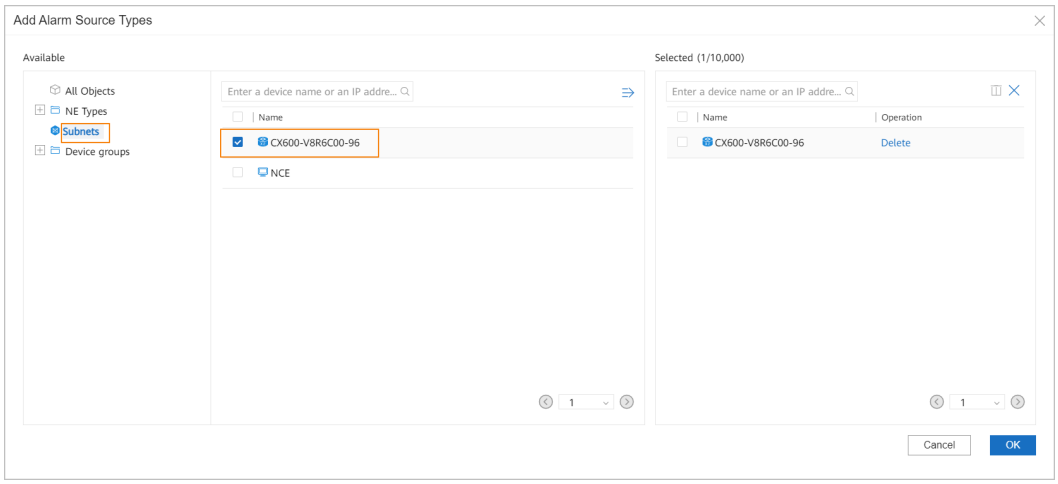
Step 3 Click **OK**.

----End

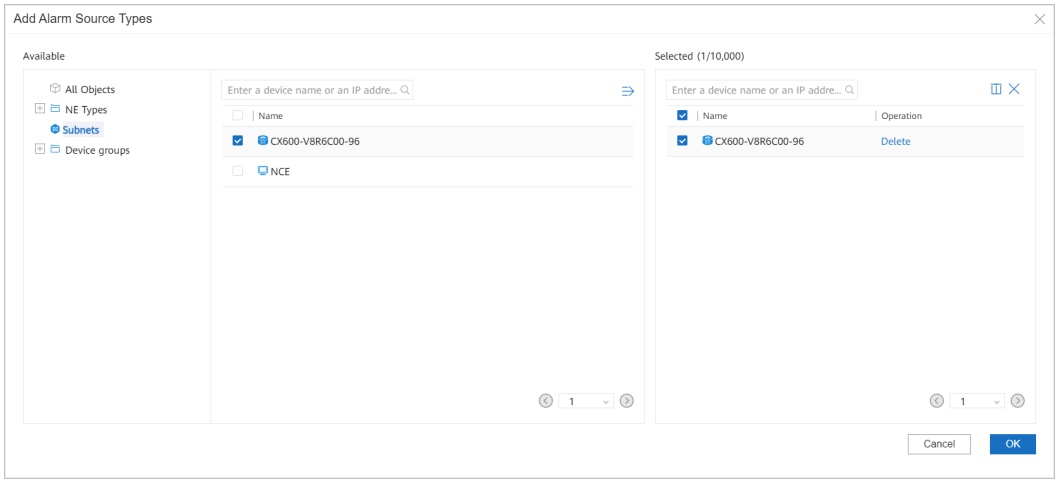
Alarm Sources

Step 1 In the **Alarm sources** area, click **Add Alarm Sources**.

Step 2 In the **Available** area, select the NEs whose alarms need to be masked or reported.



Step 3 In the **Selected** area, select the NEs set in **Step 2** and click **OK**.

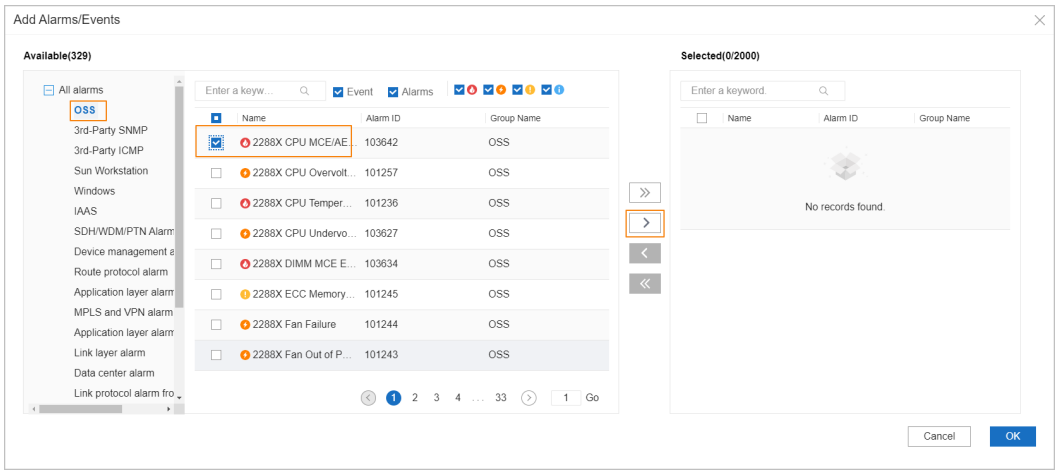


----End

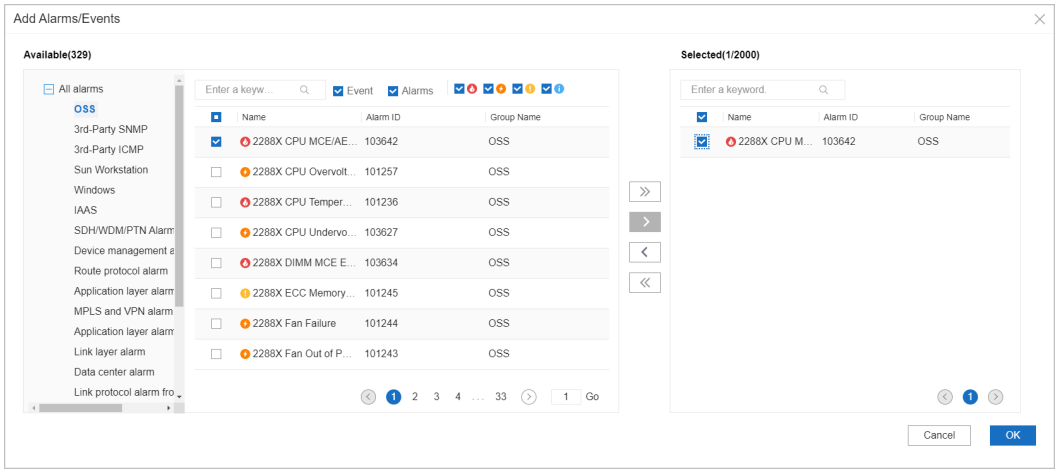
Alarms

Step 1 In the **Alarms** area, click **Add Alarms/Events**.

Step 2 In the **Available** area, select the alarms or events that need to be masked or reported, and click  .



Step 3 In the **Selected** area, select the alarms or events set in **Step 2** and click **OK**.



----End

6.3 Configuring a Security Policy

Security settings allow you to configure the lockout policy for the login IP address after the SNMP NBI authentication fails. By default, if incorrect passwords are entered for consecutive three times within 60 minutes, the login IP address will be locked for 5 minutes.

Prerequisites

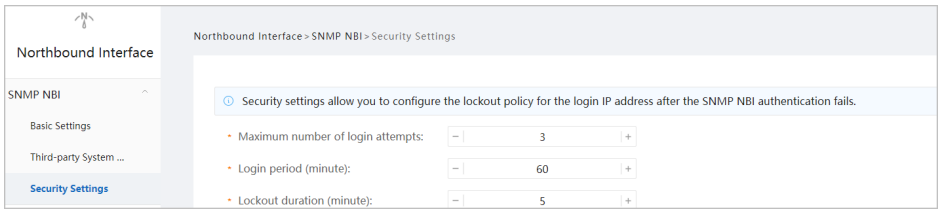
You have the **Northbound Interface** operation right.

Procedure

Step 1 Log in to the NCEO&M plane as the **admin** user.

Step 2 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 3 In the navigation pane, choose **SNMP NBI** > **Security Settings**.



Step 4 On the **Security Settings** page, retain the default settings.

Table 6-8 lists the SNMP NBI Security Policy parameters.

Table 6-8 Configuring a Security Policy

Parameter	Description	Default Value
Maximum number of login attempts	Maximum number of consecutive login failures on a client IP address.	3
Login period	Period (in minutes) within which consecutive login failures are measured.	60
Lockout duration	Lock period (in minutes) after consecutive login failures.	5

Step 5 Click **Save**.

----End

6.4 Configuration Sample

This section describes how to configure the SNMP NBI by using a configuration sample.

6.4.1 Configuring the SNMPv1 NBI

This section describes how to use SNMPv1 to configure the SNMP NBI. The deployment of the SNMPv2c NBI is similar to that of the SNMPv1 NBI.

Network Planning

As shown in Figure 6-2, the OSS loads the MIB file **HW-IMAPV1NORTHBOUND-TRAP-MIB.mib**. The OSS accesses NCE through SNMPv1 to manage and monitor alarms on Huawei network devices. Table 6-9 and Table 6-10 list detailed parameters.

You are advised to use default values for other relevant parameters. For details, see **6.2 Configuration Parameters**.

Figure 6-2 Network planning parameters for the SNMPv1 NBI

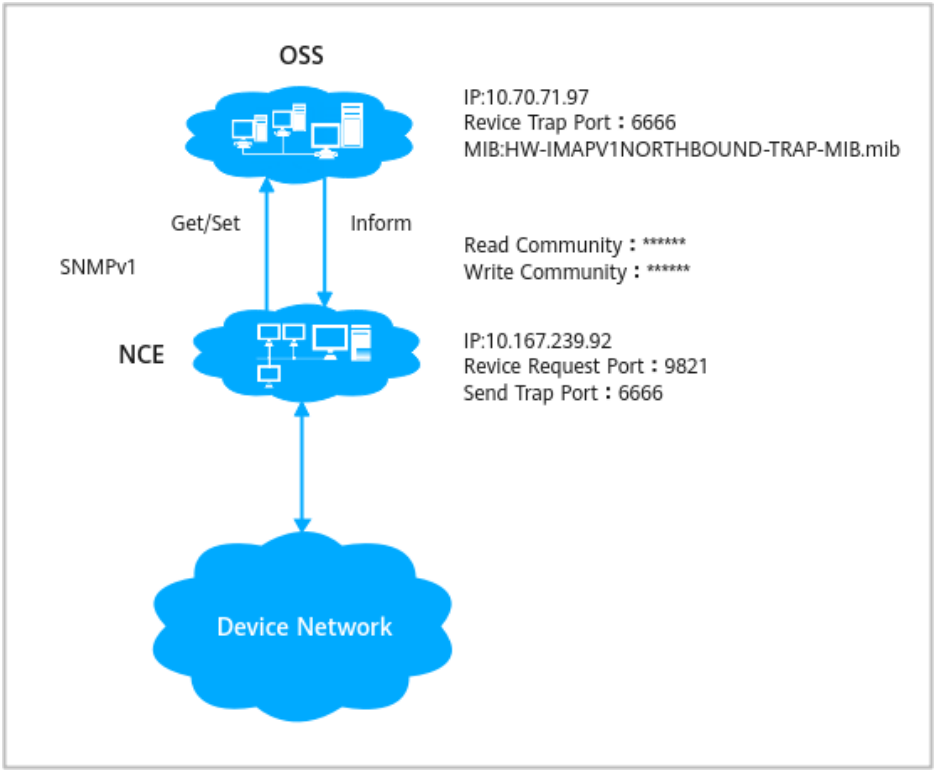


Table 6-9 Server parameters for the SNMPv1 NBI

Server	Parameter	Value
OSS	IP address	10.70.71.97
	Trap receiving port	6666
	MIB	HW-IMAPV1NORTHBOUND-TRAP-MIB.mib
NCE	IP address	10.167.239.92
	Trap sending port	6666
	Request receiving port	9812

Table 6-10 Communication parameters for the SNMPv1 NBI

Parameter	Value
Protocol version	SNMPv1
Read community	******
Write community	******

Procedure

Step 1 Log in to the NCE O&M plane.

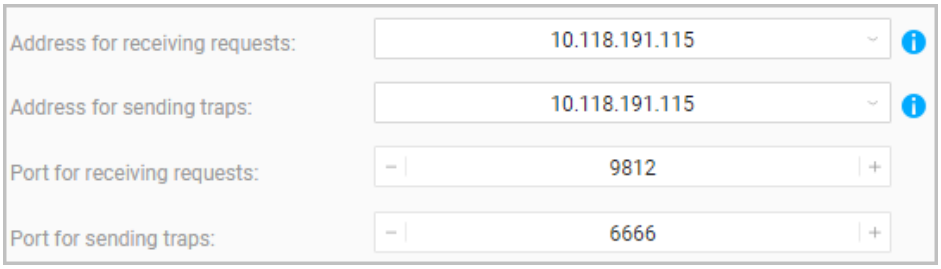
Step 2 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 3 In the navigation pane, choose **SNMP NBI** > **Basic Settings**.

Step 4 On the **Basic Settings** page, set the IP addresses and port numbers for receiving requests and sending traps.

General configuration parameters are NCE server parameters.

- Address for sending traps: 10.118.191.101; port number: 6666
- Address for receiving requests: 10.118.191.101; port number: 9812



NOTICE

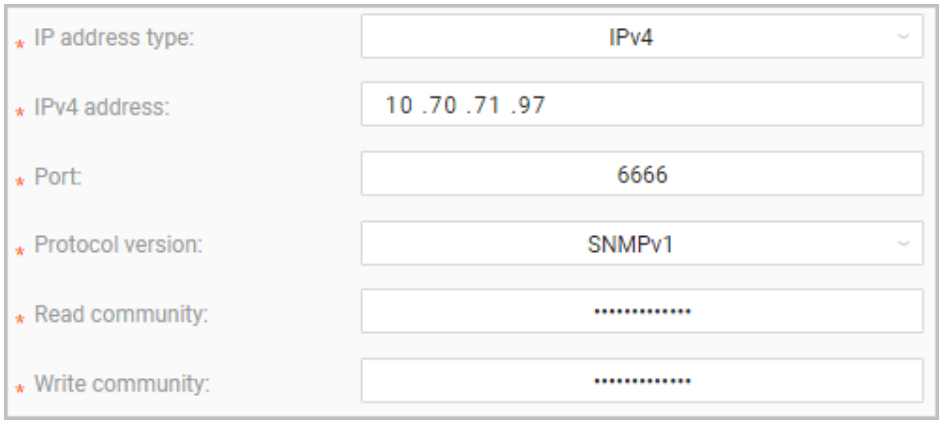
- The trap sending address and request receiving address are both the NCE server IP address. (You are advised to use the default IP address, that is, the planned network communication IP address of the SNMP NBI.In the Manager+Controller+Analyzer scenario without IP address convergence, use the northbound floating IP address instead of the default value. If you select other IPv4 addresses, NCE may fail to communicate with third-party systems. The SNMP NBI supports both IPv4 and IPv6. If third-party system A requires IPv4 but third-party system B requires IPv6, you can select both IPv4 and IPv6 addresses for the two systems to communicate with NCE at the same time.) Ensure that this IP address can be used for successful communication between NCE and the OSS.
- When configuring ports for the SNMP NBI, refer to *iMaster NCE Communication Matrix* to prevent port conflicts.
- On NCE, the recommended SNMP port range is 1025–32767.

Step 5 In the navigation pane, choose **Third-party System Settings**. In the right pane, click **Create** and set OSS parameters.

Set the following parameters as planned:

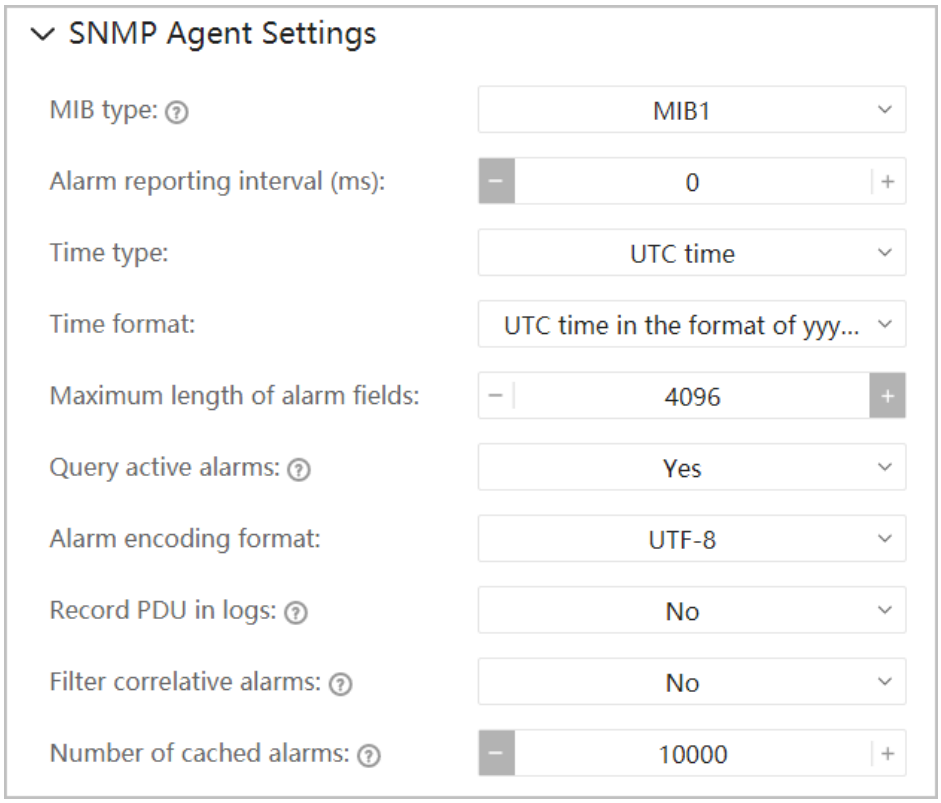
- **IPv4 address**: 10.70.71.97
- **Port**: 6666
- **Protocol version**: SNMPv1
- **Read community**: ******

- **Write community**: ******



Click **Save** to save the settings.

Step 6 In the **Advanced Settings** area of the **Basic Settings** page, expand **SNMP Agent Settings** and select **MIB1** from the **MIB type** drop-down list.



Step 7 Click **Save**.

----End

6.4.2 Configuring the SNMPv3 NBI

This section describes how to use SNMPv3 to configure the SNMP NBI. The SNMPv3 NBI provides a higher security level than SNMPv1 and SNMPv2c NBIs.

Network Planning

As shown in **Figure 6-3**, the OSS loads the MIB file **T2000-NETMANAGEMENT-MIB.mib**. The OSS accesses NCE through SNMPv3 to manage and monitor alarms on Huawei network devices. **Table 6-11** and **Table 6-12** list detailed parameters.

You are advised to use default values for other relevant parameters. For details, see **6.2 Configuration Parameters**.

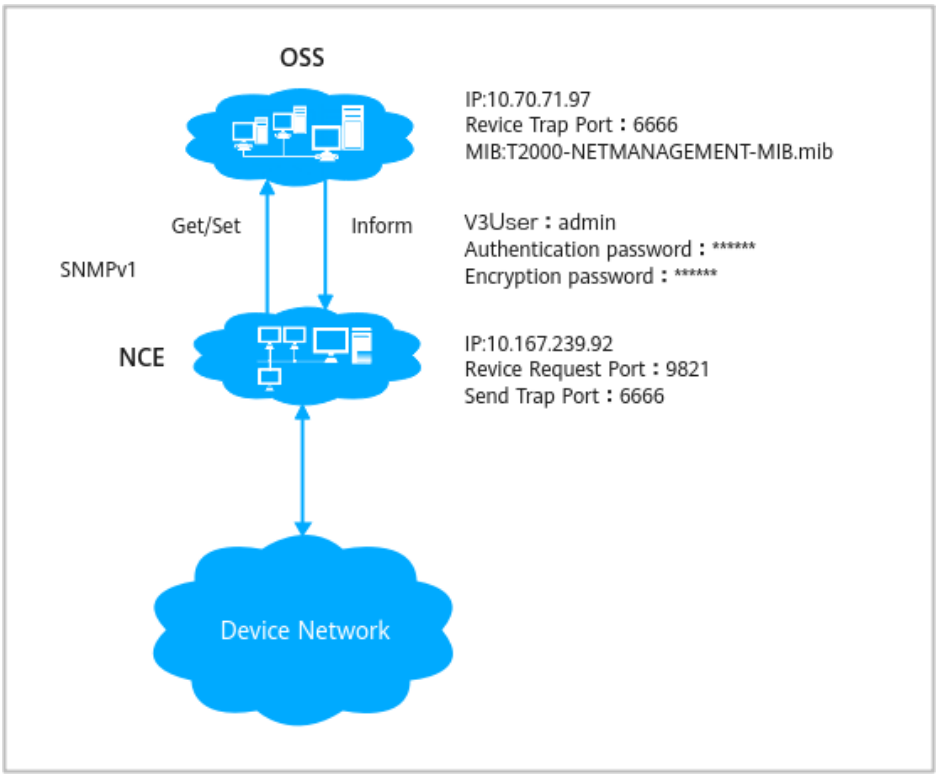
Table 6-11 Server parameters for the SNMPv3 NBI

Server	Parameter	Value
OSS	IP address	10.70.71.97
	Trap receiving port	6666
	MIB	T2000-NETMANAGEMENT-MIB.mib
NCE	IP address	10.167.239.92
	Trap sending port	6666
	Request receiving port	9812

Table 6-12 Communication parameters for the SNMPv3 NBI

Parameter	Value
SNMP version	v3
Security level	Authenticated and encrypted
Authentication protocol	SHA2-512
Encryption protocol	AES-256
Engine ID	28-6E-D4-8F-C5-1B
v3 username	admin
v3 authentication password	******
v3 encryption password	******

Figure 6-3 Network planning parameters for the SNMPv3 NBI



Procedure

Step 1 Log in to the NCE O&M plane.

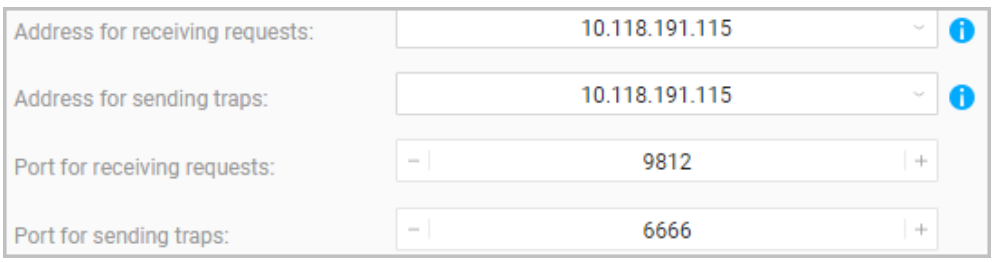
Step 2 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 3 In the navigation pane, choose **SNMP NBI** > **Basic Settings**.

Step 4 On the **Basic Settings** page, set the IP addresses and port numbers for receiving requests and sending traps.

General configuration parameters are NCE server parameters.

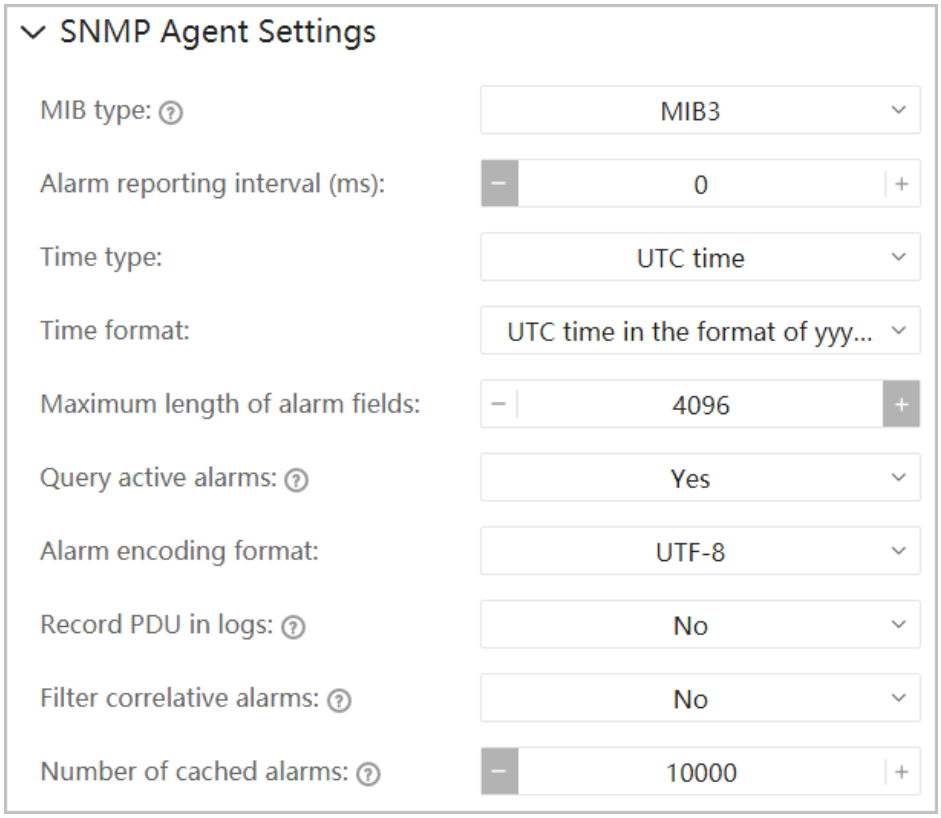
- Address for sending traps: 10.118.191.101; port number: 6666
- Address for receiving requests: 10.118.191.101; port number: 9812
- Security level: Authenticated and encrypted
- Authentication protocol: SHA2-512
- Encryption protocol: AES-256



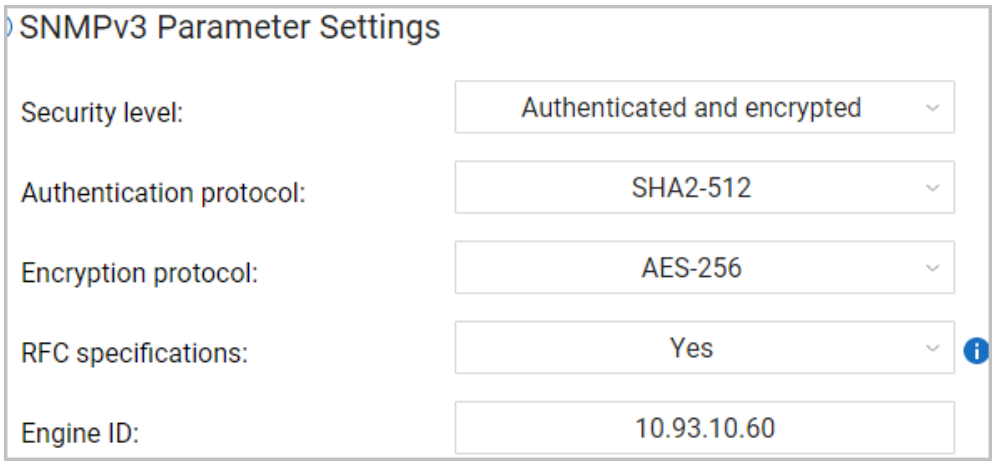
NOTICE

- The trap sending address and request receiving address are both the NCE server IP address. (You are advised to use the default IP address, that is, the planned network communication IP address of the SNMP NBI.In the Manager+Controller+Analyzer scenario without IP address convergence, use the northbound floating IP address instead of the default value. If you select other IPv4 addresses, NCE may fail to communicate with third-party systems. The SNMP NBI supports both IPv4 and IPv6. If third-party system A requires IPv4 but third-party system B requires IPv6, you can select both IPv4 and IPv6 addresses for the two systems to communicate with NCE at the same time.) Ensure that this IP address can be used for successful communication between NCE and the OSS.
- When configuring ports for the SNMP NBI, refer to *iMaster NCE Communication Matrix* to prevent port conflicts.
- On NCE, the recommended SNMP port range is 1025–32767.

Step 5 In the **Advanced Settings** area of the **Basic Settings** page, expand **SNMP Agent Settings** and select **MIB3** from the **MIB type** drop-down list.



Step 6 Expand **SNMPv3 Parameter Settings**, and set **Security level**, **Authentication protocol**, **Encryption protocol**, **RFC specifications**, and **Engine ID**.

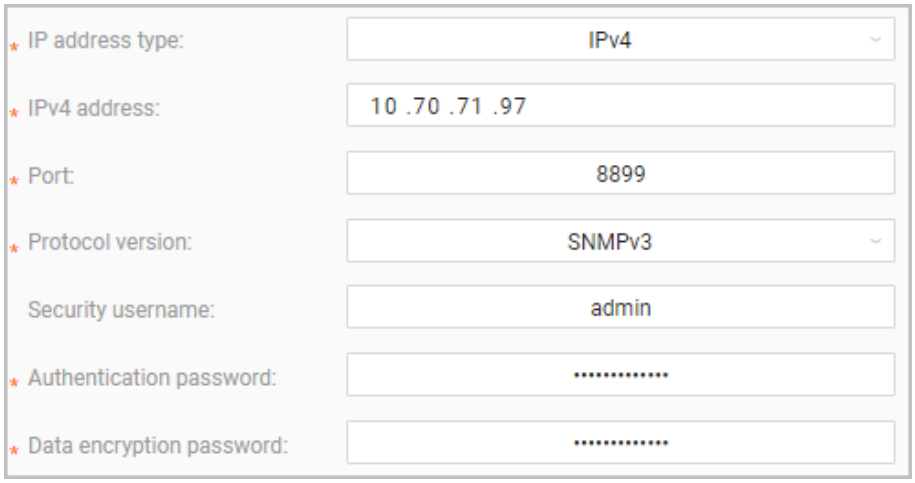


Click **Save**.

Step 7 In the navigation pane, choose **Third-party System Settings**. In the right pane, click **Create** and set OSS parameters.

Set the following parameters as planned:

- IPv4 address: 10.70.71.97
- Port: 6666
- Protocol version: SNMPv3
- Security username: admin
- Authorization and authentication password: ******
- Data encryption password: ******



Step 8 Click **Save**.

----End

7 Testing the SNMP NBI

This chapter describes how to check whether the SNMP NBI functions properly and whether it is successfully interconnected with the OSS.

7.1 MIB1

This section describes how to verify the running status of the SNMP NBI after the MIB1 is loaded. The MIB1 includes **HW-IMAPV1NORTHBOUND-TRAP-MIB.mib** and **HW-IMAPV2NORTHBOUND-TRAP-MIB.mib**.

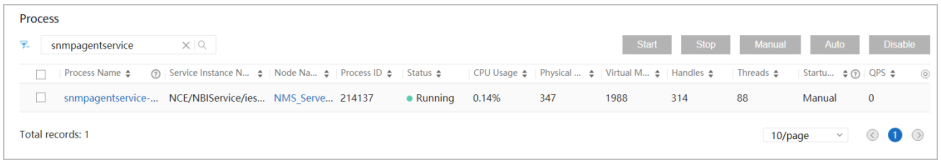
Prerequisites

- SnmpAgentService is correctly configured.
- NbiSnmpConfigWebsite is correctly configured.
- The SNMP heartbeat information is configured.
  - Heartbeat Period: 60s
  - Report Heartbeat Info: yes

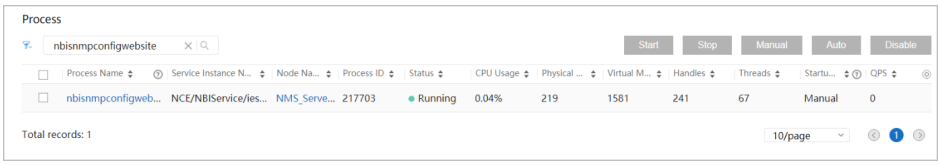
Procedure

Step 1 Log in to the NCE management plane and check the SNMP service status. If **Status** is **Running**, the SNMP NBI has been successfully started.

1. Log in to the NCE management plane.
2. Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.
3. In the navigation pane, choose **Service Monitoring**.
4. Click the **Process** tab and find the snmpagentservice process.
5. Check the status of the snmpagentservice process. (**Status** is **Running**.)



6. On the **Process** tab page, find the nbisnmpconfigwebsite process.
7. Check the status of the nbisnmpconfigwebsite process. (**Status** is **Running**.)



- If **Status** is **Not running**, refer to **10.6.1 SNMP NBI Processes Are Not Displayed**.
- If the SNMP NBI process fails to be started, refer to **10.6.2 SNMP Service Process Fails to Be Started**.

Step 2 Check whether heartbeat messages are received on the related OSS port. If no heartbeat message is received, refer to **10.6.4 OSS Cannot Receive Heartbeat Information**.

----End

7.2 MIB2

This section describes how to verify the running status of the SNMP NBI after the MIB2 is loaded. The MIB2 includes **IMAP_NORTHBOUND_MIB-V1.mib** and **IMAP_NORTHBOUND_MIB-V2.mib**. The prerequisites and procedure of MIB2 are the same as those of MIB1.

7.3 MIB3

This section describes how to verify the running status of the SNMP NBI after the MIB3 is loaded. The MIB3 includes **T2000-NETMANAGEMENT-MIB.mib**.

Prerequisites

- SnmpAgentService is correctly configured.
- NbiSnmpConfigWebsite is correctly configured.

Procedure

Log in to the NCE management plane and check the SNMP service status. If **Status** is **Running**, the SNMP NBI has been successfully started.

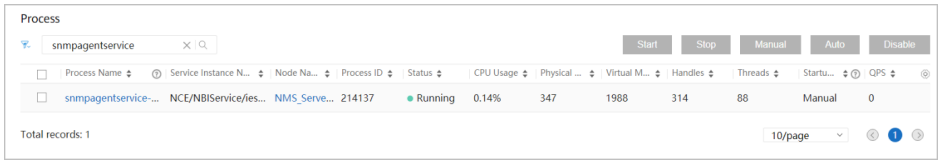
Step 1 Log in to the NCE management plane.

Step 2 Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.

Step 3 In the navigation pane, choose **Service Monitoring**.

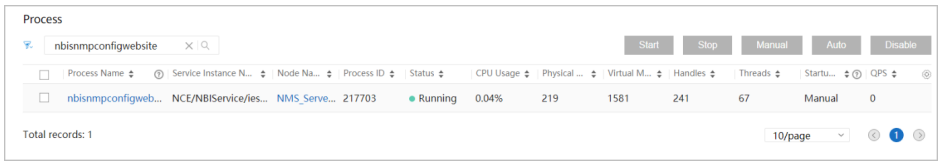
Step 4 Click the **Process** tab and find the snmpagentservice process.

Step 5 Check the status of the snmpagentservice process. (**Status** is **Running**.)



Step 6 On the **Process** tab page, find the nbisnmpconfigwebsite process.

Step 7 Check the status of the nbisnmpconfigwebsite process. (**Status** is **Running**.)



- If **Status** is **Not running**, refer to **10.6.1 SNMP NBI Processes Are Not Displayed**.
- If the SNMP NBI process fails to be started, refer to **10.6.2 SNMP Service Process Fails to Be Started**.

----End

8 Configuring the SNMP NBI on the OSS

About This Chapter

After the SNMP NBI is deployed properly, the OSS can receive real-time alarms. To connect to NCE and perform operations on reported alarms (such as synchronize, acknowledge, unacknowledge, and clear alarms), you also need to load the appropriate MIB file to the OSS and set relevant parameters. A maximum of 10 OSSs can be connected concurrently to NCE. For the OSS connection, SNMPv1, SNMPv2c, and SNMPv3 can be used.

8.1 Configuring the SNMPv1 or SNMPv2c NBI
The OSS connects to NCE through SNMPv1 and SNMPv2c NBIs by using communities for access authentication. Configurations are similar for SNMPv1 and SNMPv2c NBIs. Parameters include the request receiving IP address/port on NCE, SNMP version, and read/write communities.

8.2 Configuring the SNMPv3 NBI
Compared with SNMPv1 and SNMPv2c, the SNMPv3 NBI is characterized by higher security due to its user-based security model. In this model, usernames and passwords are used for access authentication and packet data is encrypted.

8.1 Configuring the SNMPv1 or SNMPv2c NBI

The OSS connects to NCE through SNMPv1 and SNMPv2c NBIs by using communities for access authentication. Configurations are similar for SNMPv1 and SNMPv2c NBIs. Parameters include the request receiving IP address/port on NCE, SNMP version, and read/write communities.

NOTE

SNMPv1 and SNMPv2c are insecure protocols. SNMPv3 is recommended for security concern.

Prerequisites

- The SNMP version has been set to SNMPv1 or SNMPv2c, and write and read communities have been configured.
- The third-party system has been created and its server can receive real-time alarms or heartbeats from NCE.

Procedure

Step 1 Confirm SNMP NBI parameters with the NCE administrator.

1. Log in to the NCE O&M plane.
2. Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.
3. Choose **SNMP NBI** > **Third-party System Settings** from the navigation pane.
4. Locate the OSS in the list and click  in the **Operation** column. On the displayed page, set the OSS parameters.

Parameter	Description	Default Value	Navigation Path
IP address type	IP address type of the OSS. – IPv4 – IPv6	IPv4	In the **Third-party System Settings** area, view **IP address type**.
IPv4 address (IPv6 address)	IP address used by the OSS to receive traps.	None	In the **Third-party System Settings** area, view the value of **IPv4** address (**IPv6 address**).
Port	Port used by the OSS to receive traps. **IPv4 address** (or **IPv6 address**) and **Port** determine the destination of real-time alarm traps, current alarm query traps, and heartbeat traps.	8899	In the **Third-party System Settings** area, view **Port**.
Protocol version	SNMP version for the SNMP NBI.	v3	In the **Third-party System Settings** area, view **Protocol version**.
Read/Write community	Access authentication for the OSS to connect to NCE through the SNMP NBI.	-	Learn the values of **Read community** and **Write community** from the administrator.

Step 2 Configure the OSS based on the preceding parameters set on NCE.

NOTICE

Confirm with the NCE administrator before modifying parameter settings. Otherwise, the connection may fail.

----End

Follow-up Procedure

When viewing OSS information, you can perform the following operations:

- Click to modify the OSS information.

  When **Protocol version** is set to **SNMPv1** or **SNMPv2c**, if you want to change the values of **Read community** and **Write community**, select **Change community** to modify the settings. If you do not need to modify the settings, deselect **Change community**.
- Click to delete the OSS.

8.2 Configuring the SNMPv3 NBI

Compared with SNMPv1 and SNMPv2c, the SNMPv3 NBI is characterized by higher security due to its user-based security model. In this model, usernames and passwords are used for access authentication and packet data is encrypted.

Prerequisites

- The SNMP version is set to SNMPv3, and **Authenticated and encrypted** is selected from the **Security level** drop-down list (navigation path: **Basic Settings** > **SNMPv3 Parameter Settings**).
- The OSS has been created and its server can receive real-time alarms or heartbeats from NCE.

Procedure

Step 1 Confirm SNMP NBI parameters with the NCE administrator.

1. Log in to NCE.
2. Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.
3. In the navigation pane, choose **SNMP NBI** > **Third-party System Settings**.
4. Locate the OSS in the list and click in the **Operation** column. On the page that is displayed, set the OSS parameters.

NOTE

For security purposes, from NCE V100R019C00, the SNMP NBI does not support the following insecure configuration items by default:

- **Protocol version**: **SNMPv1** and **SNMPv2c**
- **Security level**: **Not authenticated nor encrypted** and **Authenticated but not encrypted**
- **Authentication protocol**: **MD5**, **SHA**, and **SHA2-224**
- **Encryption protocol**: **DES**

  If you need insecure protocols, log in to the O&M plane, open the Security Management app, and choose **Configuration Compliance** > **Security Configuration** from the main menu. On the **Configuration Check** page, click **SNMP NBI-SNMP security configuration** and enable **SNMP Insecure Switch**. Then open the System Settings app, choose **System Settings** > **Northbound Interface** from the main menu, choose **SNMP NBI** > **Basic Settings** from the navigation pane, and configure protocols. If insecure protocols are not needed, disable **SNMP Insecure Switch**. A high-risk alert will be displayed if insecure protocols are enabled.

Parameter	Description	Default Value	Navigation Path
IP address type	IP address type of the OSS. – IPv4 – IPv6	IPv4	In the **Third-party System Settings** area, view **IP address type**.
IPv4 address (IPv6 address)	IP address used by the OSS to receive traps.	Blank	In the **Third-party System Settings** area, view the value of **IPv4 address** (**IPv6 address**).
Port	Port used by the OSS to receive traps. **IPv4 address** (or **IPv6 address**) and **Port** determine the destination of real-time alarm traps, current alarm query traps, and heartbeat traps.	8899	In the **Third-party System Settings** area, view **Port**.

Parameter	Description	Default Value	Navigation Path
Protocol version	SNMP version for the SNMP NBI.	v3 Change the value to **v3** if SNMPv3 is used.	In the **Third-party System Settings** area, view **Protocol version**.
Security level	Security level, including **Authenticated and encrypted**.	Authenticated and encrypted	In the **Basic Settings** > **SNMPv3 Parameter Settings** area, view **Security level**.
Authentication protocol	Authentication algorithm, including SHA2-256, SHA2-384, and SHA2-512.	HMACSHA	In the **Basic Settings** > **SNMPv3 Parameter Settings** area, view **Authentication protocol**.
Encryption protocol	Encryption algorithm, including AES-128, AES-192, and AES-256.	AES-256	In the **Basic Settings** > **SNMPv3 Parameter Settings** area, view **Encryption protocol**.
RFC specifications	Whether the engine ID complies with the specifications of requests for comments (RFC). – **Yes**: Converts the engine ID into a value that complies with the RFC specifications to report to the OSS. – **No**: Directly reports the engine ID to the OSS.	Yes	In the **Basic Settings** > **SNMPv3 Parameter Settings** area, view **RFC specifications**.

Parameter	Description	Default Value	Navigation Path
Engine ID	Engine ID, which is the unique identifier of an SNMP entity. **NOTE** The value of **Engine ID** contains 5 to 32 characters. Only combinations of the following characters can be used: lowercase letters(a to z), uppercase letters(A to Z), digits(0 to 9), and special characters (=~!@#%^&*()-_+[{}]:./?,).	Engine ID automatically identified by the system. The default value is the IP address of the first NIC on the Common_Service node where CommonNBI service resides.	In the **Basic Settings** > **SNMPv3 Parameter Settings** area, view **Engine ID**.
Security username	Username for authentication.	Blank	In the **Third-party System Settings** area, view **Security username**.
Authentication password	Password for authentication.	-	In the **Third-party System Settings** area, view **Authorization and authentication password**.
Data encryption password	Password for data encryption.	-	In the **Third-party System Settings** area, view **Data encryption password**.

Step 2 Configure the OSS based on the preceding parameters set on NCE.

NOTICE

Confirm with the NCE administrator before modifying parameter settings. Otherwise, the connection may fail.

----End

Follow-up Procedure

When viewing OSS information, you can perform the following operations:

- Click  to modify the OSS information.

  When **Protocol version** is configured as **SNMPv3**, if you want to change the values of **Authorization and authentication password** and **Data encryption password**, select **Change password** to modify the setting. If you do not need to modify the settings, deselect **Change password**.
- Click  to delete the OSS.

9 Calling the SNMP NBI

About This Chapter

The OSS calls the SNMP NBI to perform operations such as alarm synchronization on NCE. Available subinterfaces vary with the loaded MIB.

NOTE

Ensure that the OSS has been connected to NCE through the SNMP NBI and the desired operations have been licensed for use.

9.1 MIB1 Subinterfaces

When the OSS is loaded with the MIB1, the SNMP NBI provides subinterfaces to enable the following functions: reporting alarms automatically, synchronizing, clearing, acknowledging, unacknowledging, and filtering alarms.

NOTICE

Ensure that the MIB1 has been loaded to the OSS. To load the MIB1, set the MIB type to **MIB1** when configuring the SNMP NBI.

9.1.1 Reporting Real-Time Alarms

You do not need to set any parameters for the OSS to receive alarm packets from NCE through the SNMP NBI. After the SNMP NBI is properly configured on NCE, alarms will be reported to the OSS in real time.

The SNMP NBI has been configured on NCE.

After the trap receiving IP address or port and SNMP version have been set for the OSS on NCE, the OSS can receive real-time alarms.

You do not need to set related parameters on the OSS. Ensure that the OSS is properly connected to NCE and the related ports are permitted by the firewall.

For details about how to configure the SNMP NBI, see **6 Configuring the SNMP NBI**.

9.1.2 Changing Filter Criteria

The SNMP NBI allows the OSS to dynamically change filter criteria for reporting required alarms during its running.

Function

The OSS can call the alarm filtering interface to change alarm filter criteria dynamically when the SNMP NBI is running.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.1.3.5.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).hwNmAgent(1).hwNmFault(3).thirdNMSFaultFilter(5)

Node	Data Type	Maximum Access Permission	Description
thirdNMSFaultFilter	OCTET STRING	read-write	Alarm filter criteria are changed dynamically.

Setting Method

The OSS can set the value of the MIB node to change the alarm filter criteria. The format is as follows:

IPAddress:Port:AlarmFilterLevel:AlarmCategoryFilter

NOTICE

- The **thirdNMSFaultFilter** node only supports the set operation, that is, only the write attribute is enabled. Therefore, you need to query the setting results of the **thirdNMSFaultFilter** node on the NCE SNMP NBI configuration page.
- When you set the OID of the MIB node, you must add **.0** to the end of the original OID of the MIB node.

Table 9-1 Format description - changing filter criteria

Parameter	Description
IPAddress	IP address used by the OSS. This IP address is the trap receiving IP address preset when the SNMP NBI is configured.
Port	Port used by the OSS. This port is the trap receiving port preset when the SNMP NBI is configured.
AlarmFilterLevel	Alarm severity. Four binary digits are used to represent critical, major, minor, or warning in descending order. Each binary digit can be set to **0** or **1**. • **1**: indicates that the alarms of the corresponding alarm severity are filtered out and the OSS cannot receive alarms of that severity. • **0**: indicates that the alarms of the corresponding alarm severity are reported and the OSS can receive alarms of that severity.
AlarmCategoryFilter	Category of an alarm. Six binary digits are used to represent event, fault, clear, acknowledge, unacknowledge, or change alarm in descending order. • **1**: indicates that the alarms of the corresponding category are filtered out and the OSS cannot receive alarms of the category. • **0**: indicates that the alarms of the corresponding category are reported and the OSS can receive alarms of the category.

Sample

Prerequisites

- The IP address of the OSS is set to **10.70.73.97** and the port for receiving alarms is set to **6666**.
- The OSS connects to the SNMP NBI and can receive heartbeats or real-time alarms.

Purpose

To change the filter criteria so that only critical or major fault and clear alarms are reported.

The following table lists the parameters of this sample.

Table 9-2 Sample parameters - changing filter criteria

Parameter	Value	MIB Object
The IP of the upper-layer NMS	10.70.73.97	10.70.73.97
Receive Trap Port	6666	6666
Alarm Severity to be Reported	Critical, Major	0011
Alarm Category to be Reported	Fault Alarm, Clearance Alarm	100111

Procedure

1. The OSS sets the OID of the **thirdNMSFaultFilter** node to:
   1.3.6.1.4.1.2011.2.15.1.3.5.0.
2. The OSS sets **thirdNMSFaultFilter** to:
   10.70.73.97:6666:0011:100111.

The OSS receives responses from NCE, indicating that the filter criteria are changed successfully. The OSS will then receive the required alarms only.

9.1.3 Synchronizing Alarms

The SNMP NBI allows the OSS to initiate the synchronization operation to ensure that the alarm information on the OSS and NCE is consistent.

Function

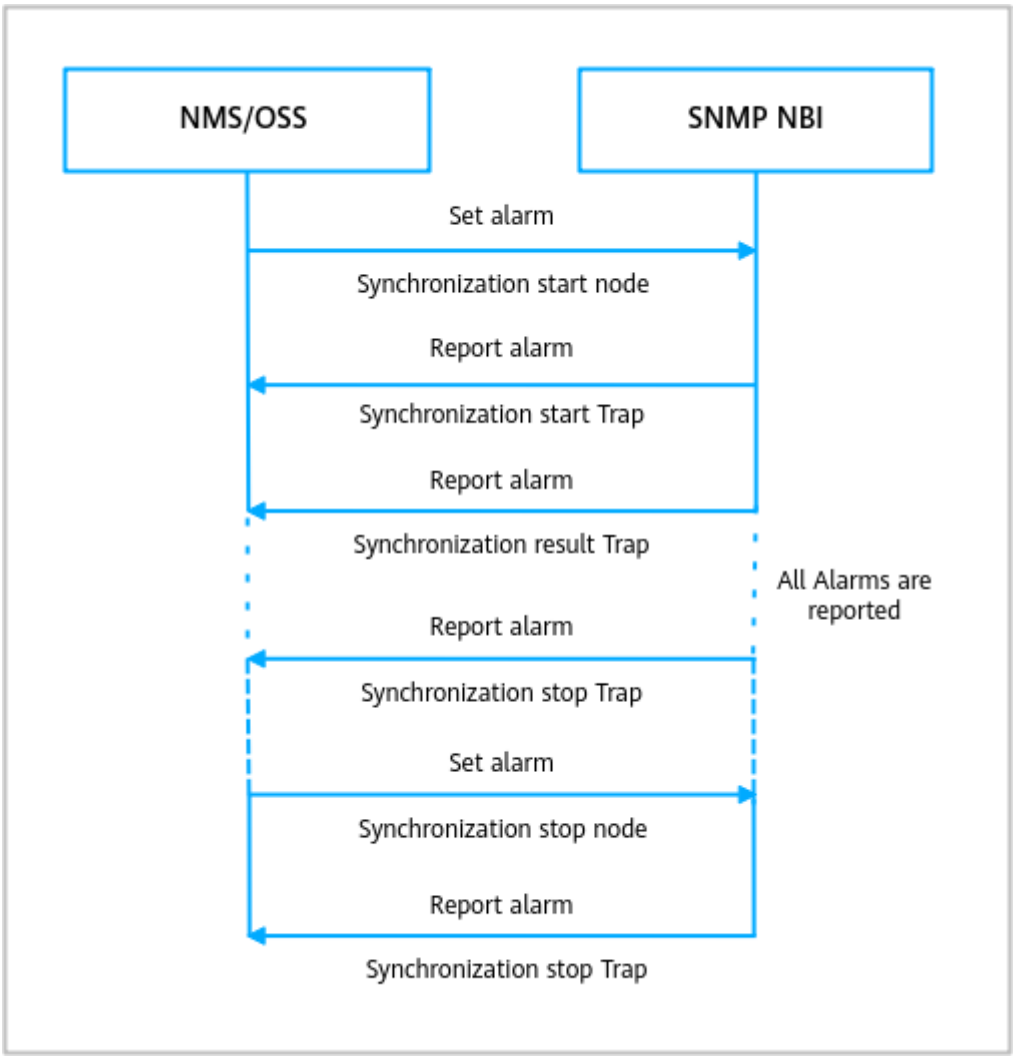
The UDP-based SNMP protocol cannot guarantee that all alarms are reported to the OSS. Therefore, the OSS synchronizes alarms to ensure alarm data consistency with NCE. The OSS can pause the synchronization as required.

When the synchronization starts, the SNMP NBI sends a "start" trap to inform the OSS that alarm synchronization has started.

When the synchronization is successfully complete or paused, the SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.

The following figure shows the alarm synchronization process.

Figure 9-1 Alarm synchronization process



Operation	Description
Synchronize alarms	1. The OSS synchronizes alarms. 2. The SNMP NBI sends a "start" trap to inform the OSS that alarm synchronization has started. 3. The SNMP NBI sends a result trap containing all valid alarms in the NCE database. 4. After all valid alarms are reported, the SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.
Stop the alarm synchronization	1. The OSS stops the alarm synchronization. 2. The SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.

NOTE

Active alarms (uncleared alarms) are synchronized by default.

For details about the alarm synchronization start trap, see **12.3.2 Alarm Synchronization Start Trap**.

For details about the alarm synchronization result trap, see **12.3.3 Alarm Synchronization Result Trap**.

For details about the alarm synchronization stop trap, see **12.3.4 Alarm Synchronization End Trap**.

MIB Definition

There are two MIB nodes for alarm synchronization: hwNmNorthboundEventSynchronizationCommandStart and hwNmNorthboundEventSynchronizationCommandStop. The former indicates starting alarm synchronization, whereas the latter indicates stopping alarm synchronization.

The OIDs are 1.3.6.1.4.1.2011.2.15.1.7.7.4 and 1.3.6.1.4.1.2011.2.15.1.7.7.5.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).hwNmAgent(1).hwNmNorthboundEvent(7).hwNmNorthboundEventSynchronization(7).hwNmNorthboundEventSynchronizationCommandStart(4)

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).hwNmAgent(1).hwNmNorthboundEvent(7).hwNmNorthboundEventSynchronization(7).hwNmNorthboundEventSynchronizationCommandStop(5)

Node	Data Type	Maximum Access Permission	Description
hwNmNorthboundEventSynchronizationCommandStart	OCTET STRING	read-write	Alarm synchronization is started.
hwNmNorthboundEventSynchronizationCommandStop	OCTET STRING	read-write	Alarm synchronization is stopped.

Setting Method

Start alarm synchronization.

The OSS can set the value of the MIB node to start alarm synchronization within a specified period. The format is as follows:

IP:port:start time:end time

Stop alarm synchronization.

The OSS can set the value of the MIB node to stop alarm synchronization. The format is as follows:

IP:port

NOTE

- When you set the OID of the MIB node, you must add **.0** to the end of the original OID of the MIB node.
- You do not need to set the start and end time to stop the alarm synchronization.

Table 9-3 Format description - synchronizing alarms

Parameter	Description
IP	IP address used by the OSS. This IP address is the trap receiving IP address preset when the SNMP NBI is configured.
port	Port used by the OSS. This port is the trap receiving port preset when the SNMP NBI is configured.
start time:endtime	Start and end time for alarm synchronization. The alarms generated within this period are synchronized. **NOTE** • If the end time is not set, the current system time of NCE is used as the end time. • If the start and end time are not set, all valid alarms are synchronized. • If the end time is set, the start time is mandatory. • Both the start and end time indicate the time when alarms are generated rather than when alarms are reported to NCE. • The UTC time, local time, and local time with the time zone are not distinguished. The start time and end time are in the format of YYYYMMDDhhmmss. • YYYY: Four-digit year. The value starts from 1970. • MM: Two-digit month. The value range is 01 to 12. • DD: Two-digit date. The value range is 01 to 31. • hh: Two-digit hour. The value range is 00 to 23. • mm: Two-digit minutes. The value range is 00 to 59. • ss: Two-digit seconds. The value range is 00 to 59.

Sample

Prerequisites

- The IP address of the OSS is set to **10.70.73.97** and the port for receiving alarms is set to **6666**.
- The OSS connects to the SNMP NBI and can receive heartbeats or real-time alarms.

Purpose

To synchronize alarms that are generated between **2011-03-01 00:00:00** and **2011-03-15 00:00:00**.

The following table lists the parameters of this sample.

Table 9-4 Sample parameters - synchronizing alarms

Parameter	Value	MIB Object
The IP of the upper-layer NMS	10.70.73.97	10.70.73.97
Receive Trap Port	6666	6666
Start time	2011-03-01 00:00:00	20110301000000
End Time	2011-03-15 00:00:00	20110315000000

Procedure

1. The OSS sets the OID of the hwNmNorthboundEventSynchronizationCommandStart node to:

   1.3.6.1.4.1.2011.2.15.1.7.7.4.0

2. The OSS sets the value of the hwNmNorthboundEventSynchronizationCommandStart node to:

   10.70.73.97:6666:20110301000000:20110315000000

   – If set successfully, the SNMP NBI sends a "start" trap to inform the OSS that alarm synchronization has started.

   – The OSS receives alarms (from the NCE database) that generated within the specified period. The SNMP NBI reports valid alarms to the OSS in the form of a result trap.

3. **(Optional)** To stop the synchronization, the OSS sets the hwNmNorthboundEventSynchronizationCommandStop node to:

   10.70.73.97:6666

4. When the synchronization is successfully complete or paused, the SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.

9.1.4 Acknowledging Alarms

The SNMP NBI allows the OSS to acknowledge alarms on NCE by alarm SN. An acknowledged alarm is an alarm that has been handled.

Function

The OSS can acknowledge NCE alarms based on the alarm SNs.

The alarm status will change after the alarm is acknowledged. If acknowledged alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms.

NOTE

The **Acknowledgement User** parameter is **SNMP Agent User** on the NCE client after an alarm is acknowledged by the OSS through the SNMP NBI.

Alarms with invalid or nonexistent SNs and historical alarms cannot be acknowledged and the SNs will be returned to the OSS.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.1.3.7.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).hwNmAgent(1).hwNmFault(3).hwNmAcknowledgeAlarms(7)

Node	Data Type	Maximum Access Permission	Description
hwNmAcknowledgeAlarms	OCTET STRING	read-write	Alarms are acknowledged based on SNs.

NOTE

The GET operation is not supported on this MIB node.

Setting Method

The OSS can set the value of the MIB node to acknowledge the active alarm on NCE. The format is as follows:

Serial Number,Serial Number,...

Table 9-5 Format description - acknowledging alarms

Parameter	Description
Serial Number,Serial Number,...	SN of an alarm. Integer, separated by a comma (,).

The following table lists the status changes when alarms are acknowledged.

Table 9-6 Alarm status - acknowledging alarms

No.	Alarm Status	Status Change	SET Response	Failed List
1	Unacknowledged and uncleared	Acknowledged and uncleared	Success	Empty
2	Unacknowledged and cleared	Acknowledged and cleared	Success	Empty
3	Acknowledged and uncleared	Acknowledged and uncleared	Success	Empty
4	Acknowledged and cleared	None	Success	Alarm SN

NOTE

If you set the lifecycle for acknowledged and cleared alarms and these alarms are not converted to historical alarms, no data will be returned after you acknowledge these alarms. The lifecycle specifies the period in which these alarms are saved in the current-alarm database.

When you set the OID of the MIB node, you must add **.0** to the end of the original OID of the MIB node.

Sample

Prerequisites

The OSS connects to the SNMP NBI and can receive heartbeats or real-time alarms.

Purpose

To acknowledge the alarm on NCE with the SN of 20,30,10005,18000.

The following table lists the parameters of this sample.

Table 9-7 Sample parameters - acknowledging alarms

Parameter	Value	MIB Object
Alarm SN	20,30,10005,18000	20,30,10005,18000

Procedure

1. The OSS sets the OID of the **hwNmAcknowledgeAlarms** node to: **1.3.6.1.4.1.2011.2.15.1.3.7.0**.
2. The OSS sets **hwNmAcknowledgeAlarms** to: **20,30,10005,18000**.

Query the alarm status on the OSS or NCE. The state for alarm 20,30,10005,18000 is **Acknowledge**, indicating that the alarm is acknowledged successfully. The **Acknowledgement User** parameter is **SNMP Agent User** on the NCE client.

NOTE

If acknowledged alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms. The alarm time is when the alarm is acknowledged.

9.1.5 Unacknowledging Alarms

The SNMP NBI allows the OSS to unacknowledge alarms on NCE by alarm SN. This function allows you to unacknowledge an acknowledged alarm if necessary.

Function

The OSS can unacknowledge alarms on NCE based on alarm SNs.

The alarm status will change after the alarm is unacknowledged. If unacknowledged alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms.

NOTE

The **Acknowledgement User** parameter is **SNMP Agent User** on the NCE client after an alarm is unacknowledged by the OSS through the SNMP NBI.

Alarms with invalid or nonexistent SNs and historical alarms cannot be unacknowledged and the SNs will be returned to the OSS.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.1.3.8.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).hwNmAgent(1).hwNmFault(3).hwNmUnAcknowledgeAlarms(8)

Node	Data Type	Maximum Access Permission	Description
hwNmUnAcknowledgeAlarms	OCTET STRING	read-write	Alarms are unacknowledged based on SNs.

NOTE

The GET operation is not supported on this MIB node.

Setting Method

The OSS can set the value of the MIB node to unacknowledge the active alarm on NCE. The format is as follows:

Serial Number,Serial Number,...

Table 9-8 Format description - acknowledging alarms

Parameter	Description
Serial Number,Serial Number,...	SN of an alarm. Integer, separated by a comma (,).

The following table lists the status changes when alarms are unacknowledged.

Table 9-9 Alarm status - unacknowledging alarms

No.	Alarm Status	Status Change	SET Response	Failed List
1	Unacknowledged and uncleared	Unacknowledged and uncleared	Success	Empty
2	Unacknowledged and cleared	Unacknowledged and cleared	Success	Empty
3	Acknowledged and uncleared	Unacknowledged and uncleared	Success	Empty
3	Acknowledged and cleared	None	Success	Alarm SN

NOTE

If you set the lifecycle for acknowledged and cleared alarms and these alarms are not converted to historical alarms, no data will be returned after you unacknowledge these alarms. The lifecycle specifies the period in which these alarms are saved in the current-alarm database.

When you set the OID of the MIB node, you must add **.0** to the end of the original OID of the MIB node.

Sample

Prerequisites

The OSS connects to the SNMP NBI and can receive heartbeats or real-time alarms.

Purpose

To unacknowledge the alarm on NCE with the SN of 20,30,10005,18000.

The following table lists the parameters of this sample.

Table 9-10 Sample parameters - unacknowledging alarms

Parameter	Value	MIB Object
Alarm SN	20,30,10005,18000	20,30,10005,18000

Procedure

- The OSS sets the OID of the **hwNmUnAcknowledgeAlarms** node to: **1.3.6.1.4.1.2011.2.15.1.3.8.0**.
- The OSS sets **hwNmUnAcknowledgeAlarms** to: **20,30,10005,18000**.

Query the alarm status on the OSS or NCE. The state for alarm 20,30,10005,18000 is **Unacknowledge**, indicating that the alarm is unacknowledged successfully. The **Acknowledgement User** parameter is **SNMP Agent User** on the NCE client.

NOTE

If unacknowledged alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms. The alarm time is when the alarm is generated.

9.1.6 Clearing Alarms

The SNMP NBI allows the OSS to clear alarms on NCE by alarm SN. Manually clear the alarm if NCE cannot automatically clear the alarm or this alarm does not exist on an NE.

Function

The OSS can clear alarms on NCE based on the alarm SNs.

The alarm status will change after the alarm is cleared. If cleared alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms.

NOTE

The **Clearance User** parameter is **SNMP Agent User** on the NCE client after an alarm is cleared by the OSS through the SNMP NBI.

Alarms with invalid or nonexistent SNs and historical alarms cannot be cleared and the SNs will be returned to the OSS.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.1.3.6.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).hwNmAgent(1).hwNmFault(3).hwNmClearAlarms(6)

Node	Data Type	Maximum Access Permission	Description
hwNmClearAlarms	OCTET STRING	read-write	Alarms are cleared based on SNs.

NOTE

The GET operation is not supported on this MIB node.

Setting Method

The OSS can set the value of the MIB node to clear the active alarm on NCE. The format is as follows:

Serial Number,Serial Number,...

Table 9-11 Format description - clearing alarms

Parameter	Description
Serial Number,Serial Number,...	SN of an alarm. Integer, separated by a comma (,).

The following table lists the status changes when alarms are cleared.

Table 9-12 Alarm status - clearing alarms

No.	Alarm Status	Status Change	SET Response	Failed List
1	Unacknowledged and uncleared	Unacknowledged and cleared	Success	Empty
2	Unacknowledged and cleared	Unacknowledged and cleared	Success	Empty
3	Acknowledged and uncleared	Acknowledged and cleared	Success	Empty
4	Acknowledged and cleared	None	Success	Alarm SN

NOTE

If you set the lifecycle for acknowledged and cleared alarms and these alarms are not converted to historical alarms, no data will be returned after you clear these alarms. The lifecycle specifies the period in which these alarms are saved in the current-alarm database.

When you set the OID of the MIB node, you must add **.0** to the end of the original OID of the MIB node.

Sample

Prerequisites

The OSS connects to the SNMP NBI and can receive heartbeats or real-time alarms.

Purpose

To clear the alarm on NCE with the SN of 20,30,10005,18000.

The following table lists the parameters of this sample.

Table 9-13 Sample parameters - clearing alarms

Parameter	Value	MIB Object
Alarm SN	20,30,10005,18000	20,30,10005,18000

Procedure

1. The OSS sets the OID of the **hwNmClearAlarms** node to:
   1.3.6.1.4.1.2011.2.15.1.3.6.0.
2. The OSS sets **hwNmClearAlarms** to:
   20,30,10005,18000.

Query the alarm status on the OSS or NCE. The state for alarm 20,30,10005,18000 is **Clear**, indicating that the alarm is cleared successfully. The **Clearance User** parameter is **SNMP Agent User** on the NCE client.

NOTE

If a cleared alarm is also an acknowledged one, it becomes a historical alarm.

If cleared alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms. The alarm time is when the alarm is cleared.

9.1.7 Reporting Alarm Acknowledgement Status

The SNMP NBI reports the alarm acknowledgement status.

Function

After you configure alarm acknowledgement status reporting through the SNMP NBI on NCE, the OSS receives alarm acknowledgement status in real time.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.1.7.1.33.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).netManagement(15).nmAgent(1).nmNorthboundEvent(7).hwNmNorthboundEventInfo(1).hwNmNorthboundConfirmStatus(33)

Node	Data Type	Maximum Access Permission	Description
hwNmNorthboundConfirmStatus	Integer32	read-write	• 1: acknowledged • 2: unacknowledged

NOTE

The Get and Set operations are not supported on this MIB node.

Setting Method

For details, see **6.1 Configuration Operations**.

9.1.8 Reporting Alarm Clearance Status

The SNMP NBI reports the alarm clearance status.

Function

After you configure alarm clearance status reporting through the SNMP NBI on NCE, the OSS receives alarm clearance status in real time.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.1.7.1.34.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).netManagement(15).nmAgent(1).nmNorthboundEvent(7).hwNmNorthboundEventInfo(1).hwNmNorthboundRestoreStatus(34)

Node	Data Type	Maximum Access Permission	Description
hwNmNorthboundRestoreStatus	Integer32	read-write	• 1: cleared • 2: uncleared

NOTE

The Get and Set operations are not supported on this MIB node.

Setting Method

For details, see **6.1 Configuration Operations**.

9.2 MIB2 Subinterfaces

When the OSS is loaded with the MIB2, the SNMP NBI provides subinterfaces to enable the following functions: reporting alarms automatically, synchronizing, clearing, acknowledging, and unacknowledging alarms, and obtaining the heartbeat period.

NOTICE

Ensure that the MIB2 has been loaded to the OSS. To load the MIB2, set the MIB type to **MIB2** when configuring the SNMP NBI.

9.2.1 Reporting Real-Time Alarms

You do not need to set any parameters for the OSS to receive alarm packets from NCE through the SNMP NBI. After the SNMP NBI is properly configured on NCE, alarms will be reported to the OSS in real time.

The SNMP NBI has been configured on NCE.

After the trap receiving IP address or port and SNMP version have been set for the OSS on NCE, the OSS can receive real-time alarms.

You do not need to set related parameters on the OSS. Ensure that the OSS is properly connected to NCE and the related ports are permitted by the firewall.

For details about how to configure the SNMP NBI, see **6 Configuring the SNMP NBI**.

9.2.2 Obtaining the Heartbeat Period

Function

The OSS obtains the heartbeat period.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.2.1.3.1.1.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).iMAPNorthbound(2).iMAPNorthboundCommon(1).iMAP

NorthboundCommuLinkMonitor(3).iMAPNorthboundHeartbeatSvc(1).iMAPNorthboundHeartbeatSvcReportInterval(1)

Node	Data Type	Maximum Access Permission	Description
iMAPNorthboundHeartbeatSvcReportInterval	Integer32	read-write	Obtain the heartbeat period.

Obtaining Method

The OSS queries the MIB node "iMAPNorthboundHeartbeatSvcReportInterval" to obtain the heartbeat period.

9.2.3 Synchronizing Alarms

The SNMP NBI allows the OSS to initiate the synchronization operation to ensure that the alarm information on the OSS and NCE is consistent.

Function

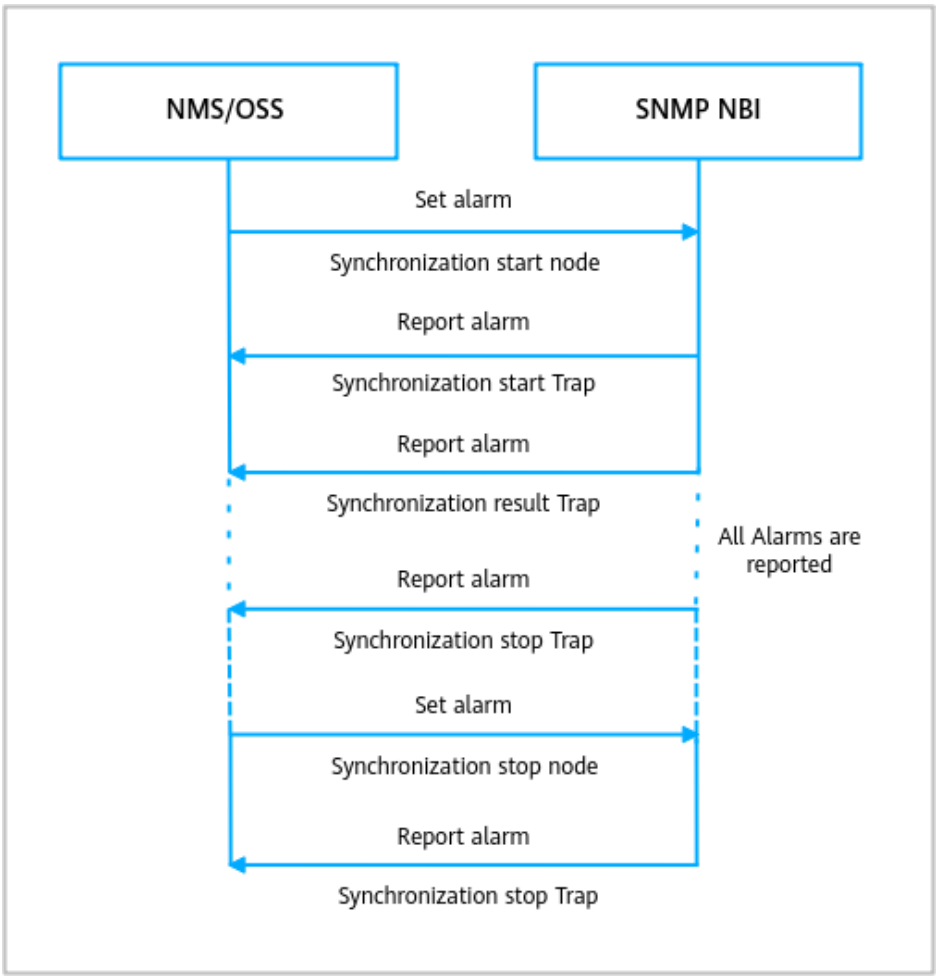
The UDP-based SNMP protocol cannot guarantee that all alarms are reported to the OSS. Therefore, the OSS synchronizes alarms to ensure alarm data consistency with NCE. The OSS can pause the synchronization as required.

When the synchronization starts, the SNMP NBI sends a "start" trap to inform the OSS that alarm synchronization has started.

When the synchronization is successfully complete or paused, the SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.

The following figure shows the alarm synchronization process.

Figure 9-2 Alarm synchronization process



Operation	Description
Synchronize alarms	1. The OSS synchronizes alarms. 2. The SNMP NBI sends a "start" trap to inform the OSS that alarm synchronization has started. 3. The SNMP NBI sends a result trap containing all valid alarms in the NCE database. 4. After all valid alarms are reported, the SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.
Stop the alarm synchronization	1. The OSS stops the alarm synchronization. 2. The SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.

NOTE

Active alarms (uncleared alarms) are synchronized by default.

For details about the alarm synchronization start trap, see **13.3.2 Alarm Synchronization Start Trap**.

For details about the alarm synchronization result trap, see **13.3.3 Alarm Synchronization Result Trap**.

For details about the alarm synchronization stop trap, see **13.3.4 Alarm Synchronization End Trap**.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.2.4.1.5.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).iMAPNorthbound(2).iMAPNorthboundFault(4).iMAPNorthboundFaultQuery(1).iMAPNorthboundAlarmQuery(5)

Node	Data Type	Maximum Access Permission	Description
iMAPNorthboundAlarmQuery	OCTET STRING	read-write	Query active alarms.

Setting Method

Start alarm synchronization.

The OSS can set the value of the MIB node **iMAPNorthboundAlarmQuery** to **1** to start alarm synchronization.

When alarm synchronization is in progress, the OSS cannot initiate another operation of synchronizing alarms.

Stop alarm synchronization.

The OSS can set the value of the MIB node **iMAPNorthboundAlarmQuery** to **0** to stop alarm synchronization.

The OSS can initiate an operation of stopping alarm synchronization only when alarm synchronization is in progress. Otherwise, an error message is returned.

Sample

Prerequisites

The OSS connects to the SNMP NBI and can receive heartbeats or real-time alarms.

Purpose

Synchronize all alarms on NCE.

The following table lists the parameters of this sample.

Table 9-14 Sample parameters - synchronizing alarms

Parameter	Value	MIB Object
Start alarm synchronization	1	1

Procedure

1. The OSS sets the OID of the iMAPNorthboundAlarmQuery node to:

1.3.6.1.4.1.2011.2.15.2.4.1.5.0

2. The OSS sets the value of the iMAPNorthboundAlarmQuery node to **1**.

- If set successfully, the SNMP NBI sends a "start" trap to inform the OSS that alarm synchronization has started.
- The OSS receives all alarms in the NCE database. The SNMP NBI reports valid alarms to the OSS in the form of a result trap.

  3. **(Optional)** To stop the synchronization, the OSS sets **iMAPNorthboundAlarmQuery** to **0**.

  4. When the synchronization is successfully complete or paused, the SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.

9.2.4 Acknowledging Alarms

The SNMP NBI allows the OSS to acknowledge alarms on NCE by alarm SN. An acknowledged alarm is an alarm that has been handled.

Function

The OSS can acknowledge NCE alarms based on the alarm SNs.

The alarm status will change after the alarm is acknowledged. If acknowledged alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms.

NOTE

The **Acknowledgement User** parameter is **SNMP Agent User** on the NCE client after an alarm is acknowledged by the OSS through the SNMP NBI.

Alarms with invalid or nonexistent SNs and historical alarms cannot be acknowledged and the SNs will be returned to the OSS.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.2.4.4.1.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).iMAPNorthbound(2).iMAPNorthboundFault(4).iMAPNorthboundFaultAcknowledge(4).iMAPNorthboundAlarmAcknowledge(1)

Node	Data Type	Maximum Access Permission	Description
iMAPNorthboundAlarmAcknowledge	OCTET STRING	read-write	Alarms are acknowledged based on SNs.

NOTE

The GET operation is not supported on this MIB node.

Setting Method

The OSS can set the value of the MIB node to acknowledge the active alarm on NCE. The format is as follows:

Serial Number,Serial Number,...

Parameter	Description
Serial Number,Serial Number,...	SN of an alarm. Integer, separated by a comma (,).

The following table lists the status changes when alarms are acknowledged.

No.	Alarm Status	Status Change	SET Response	Failed List
1	Unacknowledged and uncleared	Acknowledged and uncleared	Success	Empty
2	Unacknowledged and cleared	Acknowledged and cleared	Success	Empty
3	Acknowledged and uncleared	Acknowledged and uncleared	Success	Empty
4	Acknowledged and cleared	None	Success	Alarm SN

NOTE

If you set the lifecycle for acknowledged and cleared alarms and these alarms are not converted to historical alarms, no data will be returned after you acknowledge these alarms. The lifecycle specifies the period in which these alarms are saved in the current-alarm database.

When you set the OID of the MIB node, you must add **.0** to the end of the original OID of the MIB node.

Sample

Prerequisites

The OSS connects to the SNMP NBI and can receive heartbeats or real-time alarms.

Purpose

To acknowledge the alarm on NCE with the SN of 20,30,10005,18000.

The following table lists the parameters of this sample.

Parameter	Value	MIB Object
Alarm SN	20,30,10005,18000	20,30,10005,18000

Procedure

1. The OSS sets the OID of the **iMAPNorthboundAlarmAcknowledge** node to:

1.3.6.1.4.1.2011.2.15.2.4.4.1.0.

2. The OSS sets **iMAPNorthboundAlarmAcknowledge** to:

20,30,10005,18000.

Query the alarm status on the OSS or NCE. The state for alarm 20,30,10005,18000 is **Acknowledge**, indicating that the alarm is acknowledged successfully. The **Acknowledgement User** parameter is **SNMP Agent User** on the NCE client.

NOTE

If acknowledged alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms. The alarm time is when the alarm is acknowledged.

9.2.5 Unacknowledging Alarms

The SNMP NBI allows the OSS to unacknowledge alarms on NCE by alarm SN. This function allows you to unacknowledge an acknowledged alarm if necessary.

Function

The OSS can unacknowledge alarms on NCE based on alarm SNs.

The alarm status will change after the alarm is unacknowledged. If unacknowledged alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms.

NOTE

The **Acknowledgement User** parameter is **SNMP Agent User** on the NCE client after an alarm is unacknowledged by the OSS through the SNMP NBI.

Alarms with invalid or nonexistent SNs and historical alarms cannot be unacknowledged and the SNs will be returned to the OSS.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.2.4.5.1.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).iMAPNorthbound(2).iMAPNorthboundFault(4).iMAPNorthboundFaultUnAcknowledge(5).iMAPNorthboundAlarmUnAcknowledge(1)

Node	Data Type	Maximum Access Permission	Description
iMAPNorthboundAlarmUnAcknowledge	OCTET STRING	read-write	Alarms are unacknowledged based on SNs.

NOTE

The GET operation is not supported on this MIB node.

Setting Method

The OSS can set the value of the MIB node to unacknowledge the active alarm on NCE. The format is as follows:

Serial Number,Serial Number,...

Parameter	Description
Serial Number,Serial Number,...	SN of an alarm. Integer, separated by a comma (,).

The following table lists the status changes when alarms are unacknowledged.

No.	Alarm Status	Status Change	SET Response	Failed List
1	Unacknowledged and uncleared	Unacknowledged and uncleared	Success	Empty
2	Unacknowledged and cleared	Unacknowledged and cleared	Success	Empty
3	Acknowledged and uncleared	Unacknowledged and uncleared	Success	Empty
4	Acknowledged and cleared	None	Success	Alarm SN

NOTE

If you set the lifecycle for acknowledged and cleared alarms and these alarms are not converted to historical alarms, no data will be returned after you unacknowledge these alarms. The lifecycle specifies the period in which these alarms are saved in the current-alarm database.

When you set the OID of the MIB node, you must add **.0** to the end of the original OID of the MIB node.

Sample

Prerequisites

The OSS connects to the SNMP NBI and can receive heartbeats or real-time alarms.

Purpose

To unacknowledge the alarm on NCE with the SN of 20,30,10005,18000.

The following table lists the parameters of this sample.

Table 9-15 Sample parameters - unacknowledging alarms

Parameter	Value	MIB Object
Alarm SN	20,30,10005,18000	20,30,10005,18000

Procedure

- The OSS sets the OID of the **iMAPNorthboundAlarmUnAcknowledge** node to:

  1.3.6.1.4.1.2011.2.15.2.4.5.1.0.
- The OSS sets **iMAPNorthboundAlarmUnAcknowledge** to:

  20,30,10005,18000.

Query the alarm status on the OSS or NCE. The state for alarm 20,30,10005,18000 is **Unacknowledge**, indicating that the alarm is unacknowledged successfully.

NOTE

If unacknowledged alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms. The alarm time is when the alarm is generated.

9.2.6 Clearing Alarms

The SNMP NBI allows the OSS to clear alarms on NCE by alarm SN. Manually clear the alarm if NCE cannot automatically clear the alarm or this alarm does not exist on an NE.

Function

The OSS can clear alarms on NCE based on the alarm SNs.

The alarm status will change after the alarm is cleared. If cleared alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms.

NOTE

The **Clearance User** parameter is **SNMP Agent User** on the NCE client after an alarm is cleared by the OSS through the SNMP NBI.

Alarms with invalid or nonexistent SNs and historical alarms cannot be cleared and the SNs will be returned to the OSS.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.2.4.6.1.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).iMAPNorthbound(2).iMAPNorthboundFault(4).iMAPNorthboundFaultClear(4).iMAPNorthboundAlarmClear(1)

Node	Data Type	Maximum Access Permission	Description
iMAPNorthboundAlarmClear	OCTET STRING	read-write	Alarms are cleared based on SNs.

NOTE

The GET operation is not supported on this MIB node.

Setting Method

The OSS can set the value of the MIB node to clear the active alarm on NCE. The format is as follows:

Serial Number,Serial Number,...

Table 9-16 Format description - clearing alarms

Parameter	Description
Serial Number,Serial Number,...	SN of an alarm. Integer, separated by a comma (,).

The following table lists the status changes when alarms are cleared.

Table 9-17 Alarm status - clearing alarms

No.	Alarm Status	Status Change	SET Response	Failed List
1	Unacknowledged and uncleared	Unacknowledged and cleared	Success	Empty
2	Unacknowledged and cleared	Unacknowledged and cleared	Success	Empty
3	Acknowledged and uncleared	Acknowledged and cleared	Success	Empty
4	Acknowledged and cleared	None	Success	Alarm SN

NOTE

If you set the lifecycle for acknowledged and cleared alarms and these alarms are not converted to historical alarms, no data will be returned after you clear these alarms. The lifecycle specifies the period in which these alarms are saved in the current-alarm database.

When you set the OID of the MIB node, you must add **.0** to the end of the original OID of the MIB node.

Sample

Prerequisites

The OSS connects to the SNMP NBI and can receive heartbeats or real-time alarms.

Purpose

To clear the alarm on NCE with the SN of 20,30,10005,18000.

The following table lists the parameters of this sample.

Parameter	Value	MIB Object
Alarm SN	20,30,10005,18000	20,30,10005,18000

Procedure

1. The OSS sets the OID of the **iMAPNorthboundAlarmClear** node to: **1.3.6.1.4.1.2011.2.15.2.4.6.1.0**.

2. The OSS sets **iMAPNorthboundAlarmClear** to:

20,30,10005,18000.

Query the alarm status on the OSS or NCE. The state for alarm 20,30,10005,18000 is Clear, indicating that the alarm is cleared successfully. The **Clearance User** parameter is **SNMP Agent User** on the NCE client.

NOTE

If a cleared alarm is also an acknowledged one, it becomes a historical alarm.

If cleared alarms are specified as the filter criteria, the OSS will receive the information about state changes along with the alarms. The alarm time is when the alarm is cleared.

9.2.7 Reporting Alarm Acknowledgement Status

The SNMP NBI reports the alarm acknowledgement status.

Function

After you configure alarm acknowledgement status reporting through the SNMP NBI on NCE, the OSS receives alarm acknowledgement status in real time.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.2.4.3.3.13.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).iMAPNorthbound(2).iMAPNorthboundFault(4). iMAPNorthboundFaultNotification(3). iMAPNorthboundFaultAlarmNotification(3). iMAPNorthboundAlarmConfirm (13)

Node	Data Type	Maximum Access Permission	Description
iMAPNorthboundAlarmConfirm	Integer32	read-write	• 1: acknowledged • 2: unacknowledged

NOTE

The Get and Set operations are not supported on this MIB node.

Setting Method

For details, see **6.1 Configuration Operations**.

9.2.8 Reporting Alarm Clearance Status

The SNMP NBI reports the alarm clearance status.

Function

After you configure alarm clearance status reporting through the SNMP NBI on NCE, the OSS receives alarm clearance status in real time.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.2.4.3.3.12.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).iMAPNorthbound(2).iMAPNorthboundFault(4).iMAPNorthboundFaultNotification(3). iMAPNorthboundFaultAlarmNotification(3). iMAPNorthboundAlarmRestore(12)

Node	Data Type	Maximum Access Permission	Description
iMAPNorthboundAlarmRestore	Integer32	read-write	• 1: cleared • 2: uncleared

NOTE

The Get and Set operations are not supported on this MIB node.

Setting Method

For details, see **6.1 Configuration Operations**.

9.3 MIB3 Subinterfaces

When the OSS is loaded with the MIB3, the SNMP NBI provides subinterfaces to enable the following functions: reporting alarms automatically and synchronizing alarms.

NOTICE

Ensure that the MIB3 has been loaded to the OSS. To load the MIB3, set the MIB type to **MIB3** when configuring the SNMP NBI.

9.3.1 Reporting Real-Time Alarms

You do not need to set any parameters for the OSS to receive alarm packets from NCE through the SNMP NBI. After the SNMP NBI is properly configured on NCE, alarms will be reported to the OSS in real time.

The SNMP NBI has been configured on NCE.

After the trap receiving IP address or port and SNMP version have been set for the OSS on NCE, the OSS can receive real-time alarms.

You do not need to set related parameters on the OSS. Ensure that the OSS is properly connected to NCE and the related ports are permitted by the firewall.

For details about how to configure the SNMP NBI, see **6 Configuring the SNMP NBI**.

NOTICE

- The reported alarm field for the MIB3 consists of 36 VBs. For details, see **14.2 Alarm Fields Reported by MIB3**.
- The SNMP NBI of NCE cannot report events.

9.3.2 Synchronizing Alarms

The SNMP NBI allows the OSS to initiate the synchronization operation to ensure that the alarm information on the OSS and NCE is consistent.

Function

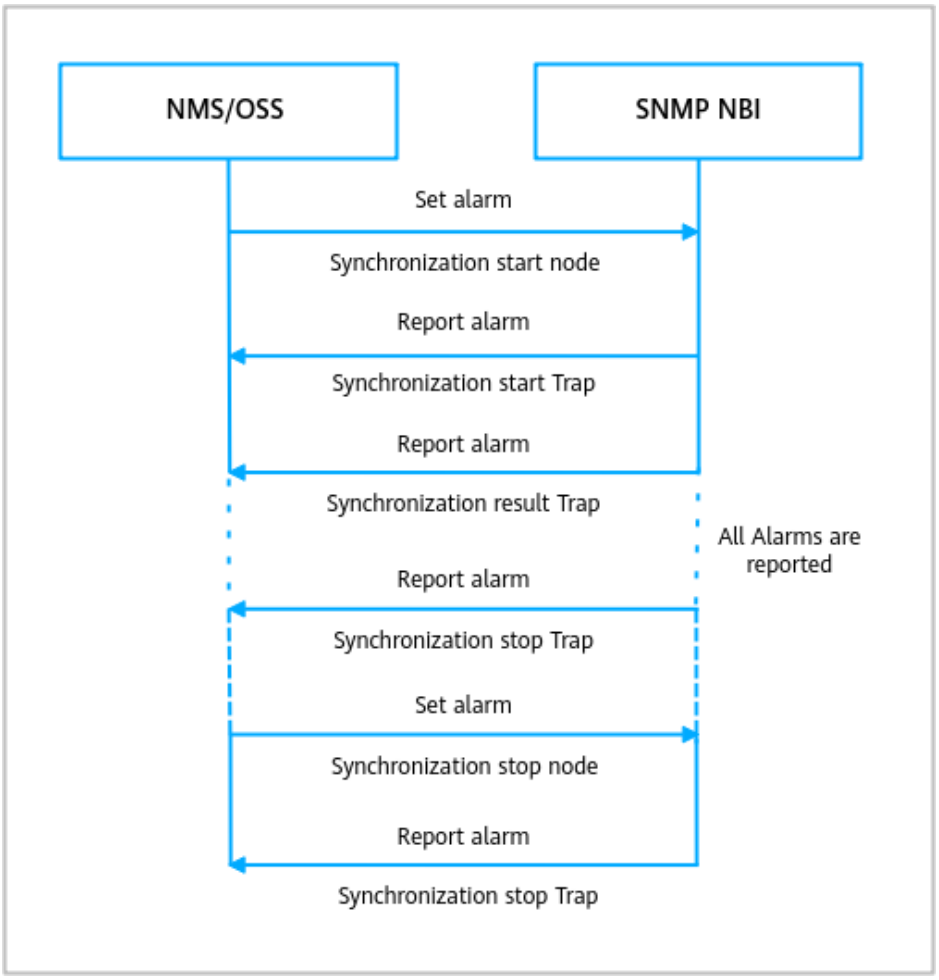
The UDP-based SNMP protocol cannot guarantee that all alarms are reported to the OSS. Therefore, the OSS synchronizes alarms to ensure alarm data consistency with NCE. The OSS can pause the synchronization as required.

When the synchronization starts, the SNMP NBI sends a "start" trap to inform the OSS that alarm synchronization has started.

When the synchronization is successfully complete or paused, the SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.

The following figure shows the alarm synchronization process.

Figure 9-3 Alarm synchronization process



Operation	Description
Synchronize alarms	1. The OSS synchronizes alarms. 2. The SNMP NBI sends a "start" trap to inform the OSS that alarm synchronization has started. 3. The SNMP NBI sends a result trap containing all valid alarms in the NCE database. 4. After all valid alarms are reported, the SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.
Stop the alarm synchronization	1. The OSS stops the alarm synchronization. 2. After all valid alarms are reported, the SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.

NOTE

Active alarms (uncleared alarms) are synchronized by default.

For details about the alarm synchronization start trap, see **14.3.2 Alarm Synchronization Start Trap**.

For details about the alarm synchronization result trap, see **14.3.3 Alarm Synchronization Result Trap**.

For details about the alarm synchronization stop trap, see **14.3.4 Alarm Synchronization End Trap**.

MIB Definition

The OID is 1.3.6.1.4.1.2011.2.15.1.7.4.1.

The full path is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).netManagement(15).nmAgent(1).nmNorthboundEvent(7).northboundSynchAlarm(4).northBoundSynchAlarmCommand(1)

Node	Data Type	Maximum Access Permission	Description
northBoundSynchAlarmCommand	INTEGER	read-write	Alarm synchronization is started or stopped.

Setting Method

The OSS can set the value of the MIB node to start or stop the synchronization. The format is as follows:

number

Table 9-18 Format description - synchronizing alarms

Parameter	Description
number	0, 1 • **0**: indicates the stop of alarm synchronization. • **1**: indicates the start of alarm synchronization.

Sample

Prerequisites

The OSS connects to the SNMP NBI and can receive heartbeats or real-time alarms.

Purpose

To start or stop the alarm synchronization.

Procedure

1. The OSS sets the OID of the northBoundSynchAlarmCommand node to **1.3.6.1.4.1.2011.2.15.1.7.4.1.0**.
2. The OSS sets the value of the northBoundSynchAlarmCommand node to **1**.
   - If set successfully, the SNMP NBI sends a "start" trap to inform the OSS that alarm synchronization has started.
   - The OSS receives valid alarms in the NCE database. The SNMP NBI reports valid alarms to the OSS in the form of a result trap.
3. **(Optional)** To stop the synchronization, set **northBoundSynchAlarmCommand** to **0**.
4. When the synchronization is successfully complete or paused, the SNMP NBI sends a "stop" trap to inform the OSS that alarm synchronization has stopped.

10 Maintaining the SNMP NBI

About This Chapter

This chapter introduces how to maintain the NCE SNMP NBI.

10.1 Maintenance Description
This section describes the basic requirements for maintaining the SNMP NBI.

10.2 Routine Maintenance
By routine maintenance, faults such as malfunction in the system operation can be detected in time and countermeasures are adopted to properly handle the problem. In this way, hidden troubles are cleared to prevent the occurrence of an accident. You are advised to perform routine maintenance once a week.

10.3 Stopping and Restarting the SNMP NBI

10.4 Changing the Startup Modes of NBI Processes

10.5 Checking the Northbound IP Address
This section describes how to check the northbound IP address used for interconnecting with the OSS.

10.6 Faults and Solutions
This section describes the faults of the SNMP NBI and the related solutions.

10.1 Maintenance Description

This section describes the basic requirements for maintaining the SNMP NBI.

To ensure that the NCE SNMP NBI works well, check that the following requirements are met:

1. The maintenance personnel are familiar with:
   - Euler
   - SNMP protocol
   - Basic concepts of the Telecommunication Management Network (TMN) and basic NCE networking structure
2. The license supports SNMP NBI functions.
3. The NCE server runs normally.

4. SNMP NBI parameters are correctly set on the NCE O&M plane.

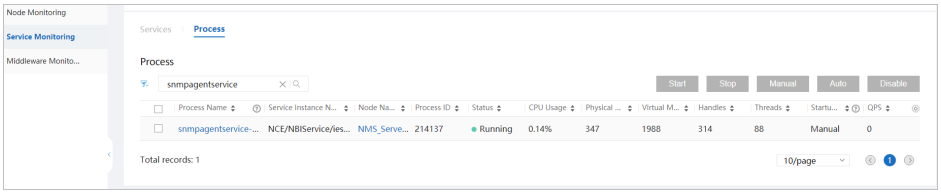
10.2 Routine Maintenance

By routine maintenance, faults such as malfunction in the system operation can be detected in time and countermeasures are adopted to properly handle the problem. In this way, hidden troubles are cleared to prevent the occurrence of an accident. You are advised to perform routine maintenance once a week.

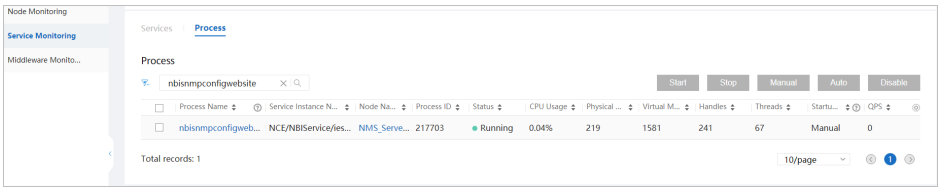
Checking the SNMP Service Running Status

Step 1 Log in to the NCE management plane and check the SNMP service status. If **Status** is **Running**, the SNMP NBI has been successfully started.

1. Log in to the NCE management plane.
2. Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.
3. In the navigation pane, choose **Service Monitoring**.
4. Click the **Process** tab and find the snmpagentservice process.
5. Check the status of the snmpagentservice process. (**Status** is **Running**.)



6. On the **Process** tab page, find the nbisnmpconfigwebsite process.
7. Check the status of the nbisnmpconfigwebsite process. (**Status** is **Running**.)



----End

Backing Up SNMP NBI Logs

The SNMP NBI logs of NCE are saved in **/opt/oss/log/NCE/SnmpAgentService** on the Common_Service node. To save disk space, you need to periodically back up the log files in this directory. These logs record the running information of the SNMP NBI and the operations performed by the OSS through the SNMP NBI. If the SNMP NBI throws exceptions, these logs will facilitate exception locating. To back up the SNMP NBI logs of NCE, manually copy them to the specified directory.

NOTE

On EulerOS, the environment variable is represented as **$Variable** (**Variable** indicates the variable name). The NCE server is installed in **/opt/oss** by default. Therefore, **$OSS_ROOT** points to **/opt/oss**.

10.3 Stopping and Restarting the SNMP NBI

This section describes how to stop an SNMP NBI when NCE temporarily does not need to provide this NBI to an external network and how to restart this NBI.

10.3.1 Stopping the SNMP NBI

If the SNMP NBI is no longer required, you can stop SNMP services on the NCE management plane.

Procedure

Step 1 Log in to the NCE management plane.

Step 2 Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.

Step 3 In the navigation pane, choose **Service Monitoring**.

Step 4 Click the **Process** tab and find the snmpagentservice process.

Step 5 Select the snmpagentservice process and click **Stop**. In the **Confirm** dialog box, click **OK**.

Step 6 On the **Process** tab page, find the nbisnmpconfigwebsite process.

Step 7 Select the nbisnmpconfigwebsite process and click **Stop**. In the **Confirm** dialog box, click **OK**.

----End

10.3.2 Restarting the SNMP NBI

After the SNMP NBI is stopped, you can restart it on the NCE management plane.

Prerequisites

- NCE is running.
- The snmpagentservice process is in the **Not Running** state.
- The nbisnmpconfigwebsite process is in the **Not Running** state.

Procedure

Step 1 Log in to the NCE management plane.

Step 2 Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.

Step 3 In the navigation pane, choose **Service Monitoring**.

Step 4 Click the **Process** tab and find the snmpagentservice process.

Step 5 Select the snmpagentservice process and click **Start**. In the **Confirm** dialog box, click **OK**.

Step 6 On the **Process** tab page, find the nbisnmpconfigwebsite process.

Step 7 Select the nbisnmpconfigwebsite process and click **Start**. In the **Confirm** dialog box, click **OK**.

----End

10.4 Changing the Startup Modes of NBI Processes

Procedure

Step 1 Open a browser, enter **https://***IP address of the management plane*:**31945** in the address bar, and press **Enter**.

Step 2 Enter a username and password, and click **Log In**.

NOTE

- If you are logging in locally, enter the username **admin** and its password. For security purposes, change the password upon the first login, update it periodically, and keep it secure.
- During first login to the management plane, change the initial password for the **admin** user as prompted. If you forget the password for the **admin** user, reinstall the management plane to restore the initial password.
- For security purposes, do not allow your browser to keep the password.
- If you enter an incorrect **admin** password for five consecutive times within 10 minutes, the login IP address will be locked for 10 minutes.

Step 3 Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.

Step 4 In the navigation pane, choose **Service Monitoring**.

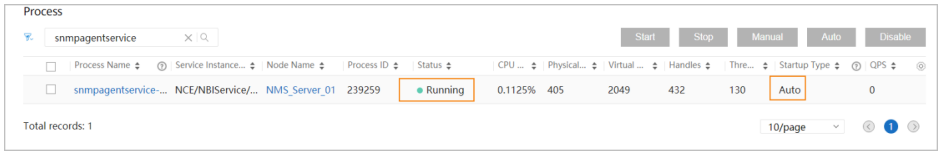
Step 5 Click the **Process** tab. The process list is displayed.

Step 6 Search for the snmpagentservice and nbisnmpconfigwebsite processes and perform **Step 7** to **Step 9** for each of them.

Step 7 Select the process, click **Start** above the process list, and confirm the operation as prompted.

Step 8 Select the process, click **Auto** above the process list, and confirm the operation as prompted.

Step 9 Check that **Status** and **Startup Type** are **Running** and **Auto**, respectively.



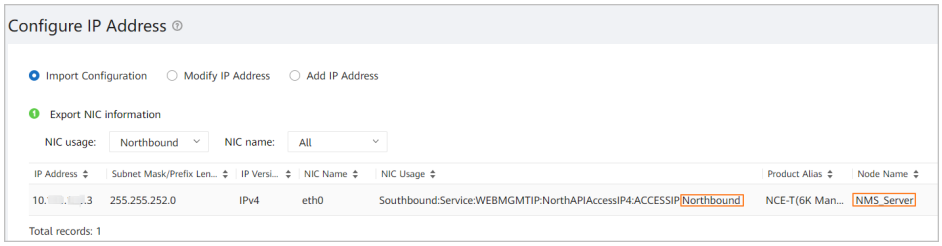
----End

10.5 Checking the Northbound IP Address

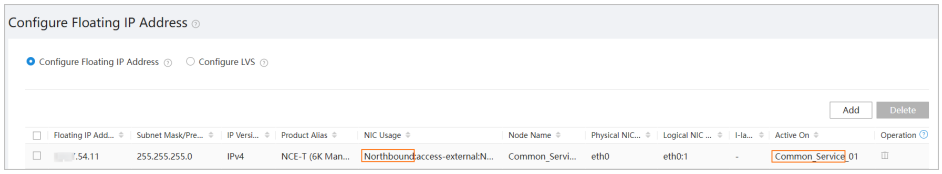
This section describes how to check the northbound IP address used for interconnecting with the OSS.

Procedure

- In Manager, it is the northbound IP address of the NMS_Server node.
  a. Log in to the management plane.
     Access https://*IP address of the management plane*:31945.Enter a username and password, and click **Log In**.
  b. Choose **Maintenance** > **Network Configuration** > **Configure IP Address** from the main menu.
  c. Click **Import Configuration**. In the **Export NIC information** area, set **NIC Usage** to **Northbound**.



     If no northbound IP address is displayed or the IP address is not the planned one, correct the IP address by referring to "Network Configuration" in *iMaster NCE Administrator Guide*.
- In Manager+Controller+Analyzer without IP address convergence, it is the northbound IP address of the Common_Service node.
  a. Log in to the management plane.
     Access https://*IP address of the management plane*:31945.Enter a username and password, and click **Log In**.
  b. Choose **Maintenance** > **Network Configuration** > **Configure Floating IP Address** from the main menu.
  c. Click **Configure Floating IP Address**. In the floating IP address list, check the IP address of the Common_Service node whose **NIC Usage** contains **Northbound**.



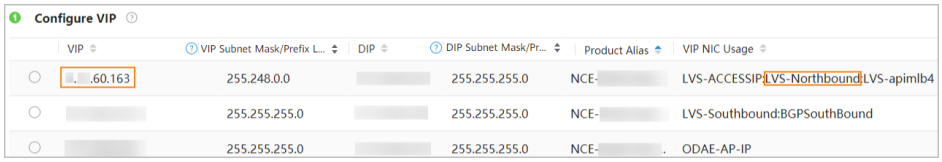
     If no northbound IP address is displayed or the IP address is not the planned one, correct the IP address by referring to "Network Configuration" in *iMaster NCE Administrator Guide*.
- In Manager+Controller+Analyzer with IP address convergence, it is the LVS-Northbound IP address of the GW node.

a. Log in to the management plane.

   Access https://*IP address of the management plane*:31945.Enter a username and password, and click **Log In**.

b. Choose **Maintenance** > **Global Load Balancing** > **Configure Global Load Balancing** from the main menu.

c. In the **Configure VIP** area, check the IP address of the GW node whose **VIP NIC Usage** contains **LVS-Northbound**.



   If no LVS-Northbound IP is displayed or the IP address is not the planned one, correct the IP address by referring to "Network Configuration" in *iMaster NCE Administrator Guide*.

10.6 Faults and Solutions

This section describes the faults of the SNMP NBI and the related solutions.

10.6.1 SNMP NBI Processes Are Not Displayed

Symptom

After the SNMP NBI is configured, the snmpagentservice and nbisnmpconfigwebsite processes are not displayed in the process list on the **Panoramic Monitoring** page of the NCE management plane.

Use PuTTY to log in to the server as the **sopuser** user and run the following commands:

> su - ossadm

Password:

> . /opt/oss/manager/bin/engr_profile.sh

> ipmc_adm -cmd statusapp | grep SnmpAgentService

No command output is displayed.

> su - ossadm

Password:

> . /opt/oss/manager/bin/engr_profile.sh

> ipmc_adm -cmd statusapp | grep NbiSnmpConfigWebsite

No command output is displayed.

Possible Causes

The SNMP NBI is not licensed.

Procedure

Step 1 Check whether the license for the SNMP NBI has been obtained. If no license is obtained, apply for one and use it to update the original license. For details, see **5 Checking the License**.

Step 2 If there is a license for the SNMP NBI, redeploy the SNMP NBI or restart the NMS. Then, check the snmpagentservice and nbisnmpconfigwebsite processes.

Step 3 If the snmpagentservice and nbisnmpconfigwebsite processes are not running, contact Huawei technical support.

----End

10.6.2 SNMP Service Process Fails to Be Started

Symptom

After NCE is started, the SNMP NBI service fails to be started.

Possible Causes

Port 9812 for configuring the SNMP NBI is occupied by other processes.

NOTICE

- On NCE, the recommended port number of the SNMP protocol is from 1025 to 32767.
- To learn details about NCE ports, read *iMaster NCE Communication Matrix*.

Procedure

Step 1 Use PuTTY to log in to the OS as the **sopuser** user. Check whether other processes are using the port of the SNMP NBI service.

Run the **netstat -an** command to view the service ports enabled by the system.

On the Euler OS, run the **netstat -an | grep port_number** command to view the status of a specified port.

For example, run the **netstat -an | grep 6666** command to view the status of port 6666.

NOTE

If there are routers or firewalls between NCE and the OSS, check all ports used by the source and the sink. Ensure that these ports can be normally enabled to support the communication between the source and sink.

Table 10-1 Service ports of an SNMP NBI

Service Name	Serving Port/ Protocol Type	Direction (with the Server as the Reference Object)	Description
SnmpAgentService	6666/UDP	OUT	SNMP trap sending
SnmpAgentService	9812/UDP	IN	SNMP request receiving

Step 2 If the port is occupied by other processes, negotiate with OSS engineers to modify the port for the SNMP NBI, or end the processes if they are not needed.

----End

10.6.3 OSS User Cannot Connect to the SNMP NBI

Symptom

The OSS user cannot connect to the SNMP NBI.

Possible Causes

- The snmpagentservice process is not started.
- The nbisnmpconfigwebsite process is not started.
- As listed in the following table, the communication parameters of the OSS do not match those of the SNMP NBI.

Protocol Version	Communication Parameter
SNMPv1 and SNMPv2	• Receive Request from NMS address/port • SNMP version • Read community • Write community
SNMPv3	• Receive Request from NMS address/port • SNMP version • User name • Authentication password and encryption password • Security model • Authentication protocol and encryption protocol

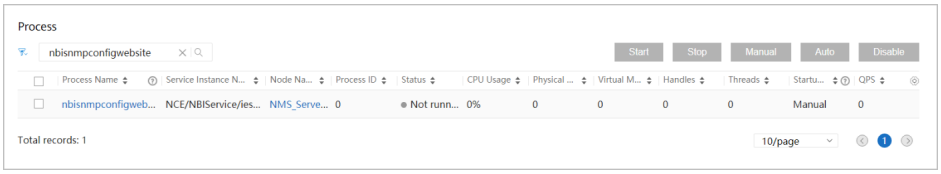
- The firewall blocks the communication between the request sending port on the OSS and the request receiving port on NCE.

Procedure

Step 1 Log in to the NCE management plane and check the statuses of the snmpagentservice and nbisnmpconfigwebsite processes. If **Status** is **Not running**, the snmpagentservice and nbisnmpconfigwebsite processes fail to be started.

1. Log in to the NCE management plane.
2. Choose **Maintenance** > **Operation and Maintenance Management** > **Panoramic Monitoring** from the main menu.
3. In the navigation pane, choose **Service Monitoring**.
4. Click the **Process** tab and find the snmpagentservice process.
5. Check the status of the snmpagentservice process. If **Status** is **Not running**, the snmpagentservice process fails to be started.

6. On the **Process** tab page, find the nbisnmpconfigwebsite process.
7. Check the status of the nbisnmpconfigwebsite process. If **Status** is **Not running**, the nbisnmpconfigwebsite process fails to be started.



For details, see **10.6.2 SNMP Service Process Fails to Be Started**.

Step 2 If the snmpagentservice and nbisnmpconfigwebsite processes have been started, determine the communication parameters with OSS engineers and redeploy the SNMP NBI.

Step 3 Ensure that the communication between the request sending port on the OSS and the request receiving port on NCE is not blocked by the firewall.

----End

10.6.4 OSS Cannot Receive Heartbeat Information

Symptom

The OSS can receive alarms but cannot receive heartbeat information from NCE.

Possible Causes

- The OSS is loaded with the MIB3 that does not support heartbeat transmission.
- The heartbeat function is disabled when the SNMP NBI is configured.

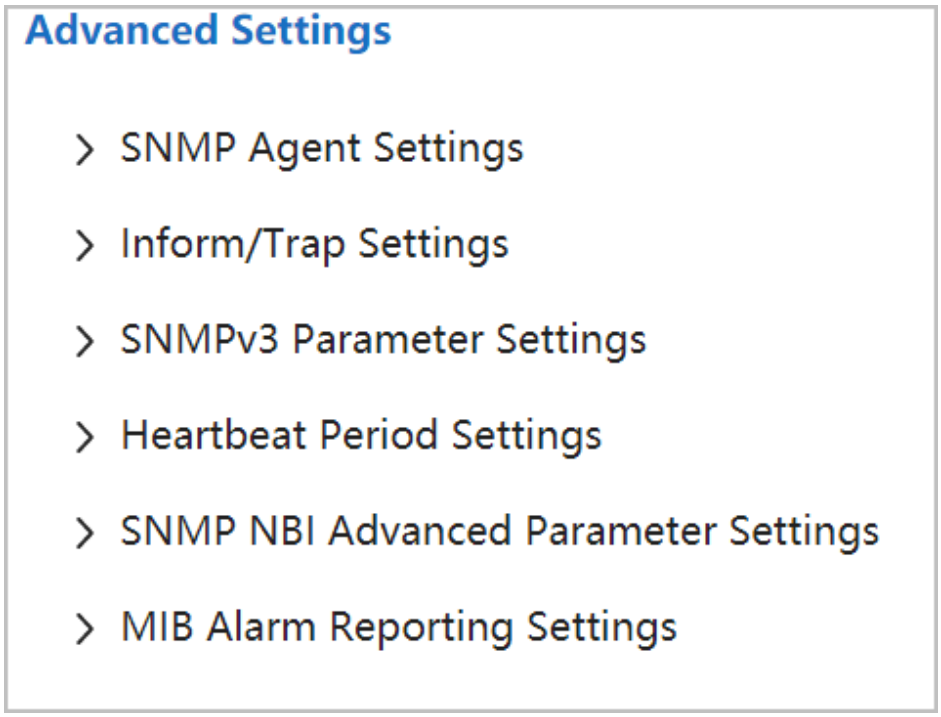
Procedure

Step 1 Log in to the NCE O&M plane.

Step 2 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 3 In the navigation pane, choose **SNMP NBI** > **Basic Settings**.

Step 4 In the **Advanced Settings** area of the **Basic Settings** page, configure information as required.



Step 5 Check whether the correct type of MIB is loaded for the SNMP NBI. In the **SNMP Agent Settings** area, check whether **MIB type** is **MIB3**. The MIB3 does not support heartbeat transmission.

Step 6 Check whether heartbeat reporting is disabled.

In the **Heartbeat Period Settings** area, check whether **Report heartbeat notifications** is set to **Enable**. If it is not, set it to **Enable** and click **Save**.

----End

10.6.5 OSS Cannot Receive Real-Time Alarms

Symptom

The OSS cannot receive real-time alarms.

Possible Causes

- The following parameters are incorrect when the SNMP NBI is configured:

  - Send Trap address/port in SNMP Agent
  - Receive Trap address/port in third-party system
- The trap receiving port on the OSS and the trap sending port on NCE are disabled on the firewall, and therefore they cannot communicate with each other.
  - The trap sending port on NCE is 6666 by default.

Procedure

Step 1 After confirming the preceding parameters with OSS engineers, log in to the NCE web client, go to the SNMP NBI configuration page, and reconfigure the SNMP NBI based on the confirmation.

Step 2 Check that the trap receiving port on the OSS and the trap sending port on NCE are enabled on the firewall to ensure that they can communicate with each other.

----End

10.6.6 Acknowledging, Unacknowledging, or Clearing Alarms Fails

Symptom

The OSS can receive heartbeats and alarms, but active alarms cannot be acknowledged, unacknowledged, or cleared.

Possible Causes

- The alarm has been converted to the historical alarm.
- The dependent services, such as log service and fault service, are down.
- The version of the MIB file is not matched.
  - The MIB2 and MIB3 do not support the function of acknowledging, unacknowledging, or clearing alarms.
  - The MIB file loaded to the OSS does not match the NCE version.

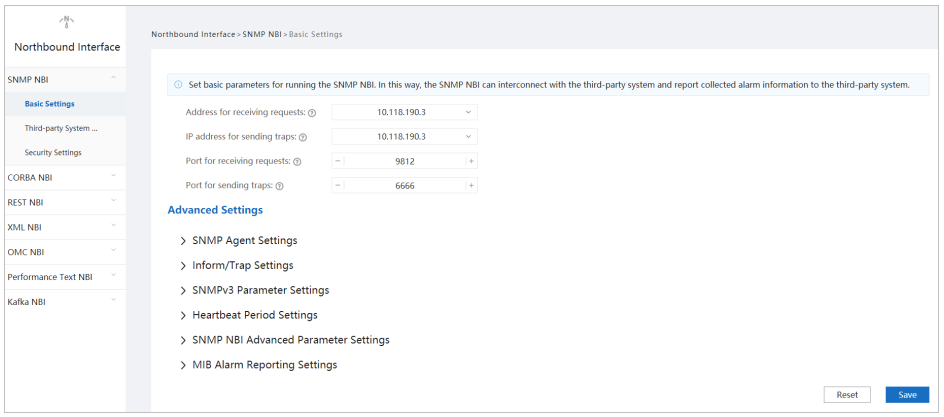
Procedure

Step 1 Log in to the NCE O&M plane and browse the historical alarms. Check whether the SN exists. If the SN exists, the alarm is converted to a historical alarm. In this case, you cannot acknowledge, unacknowledge, or clear historical alarms.

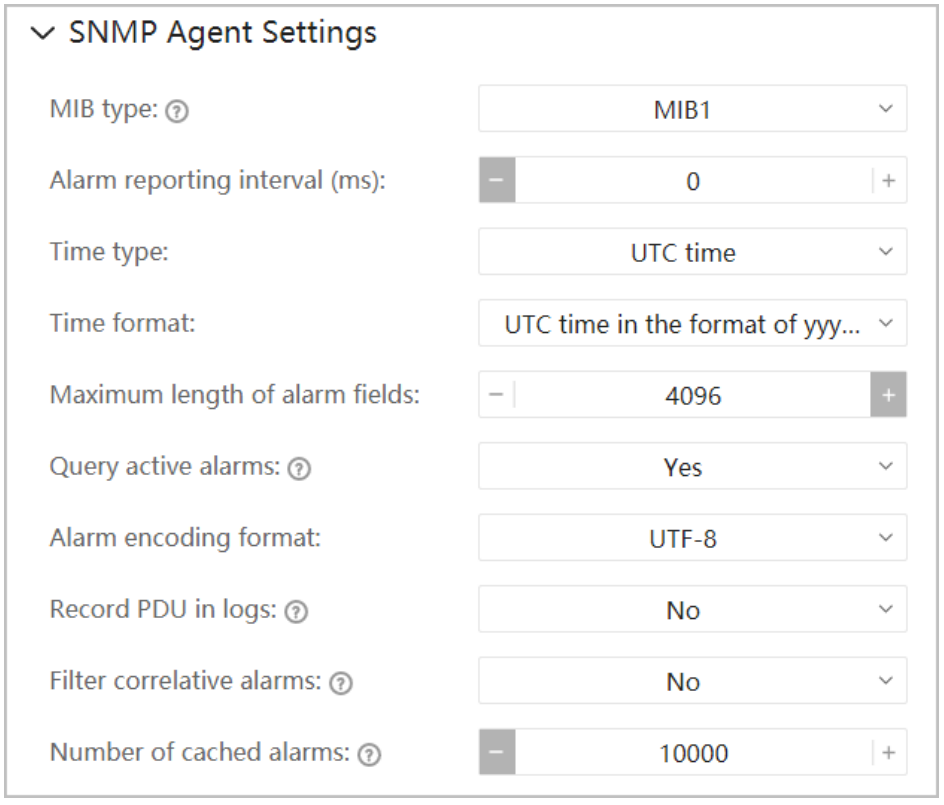
Step 2 Log in to the NCE management plane and check whether the log service and fault service are running normally. If they are not started, restart the processes.

Step 3 Check whether the correct MIB is loaded for the SNMP NBI.

1. Log in to the NCE O&M plane.
2. Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.
3. In the navigation pane, choose **SNMP NBI** > **Basic Settings**.



4. In the **Advanced Settings** area of the **Basic Settings** page, expand **SNMP Agent Settings**, change **MIB type** to **MIB1** if it is **MIB2** or **MIB3** and click **Save**.



----End

10.6.7 How Do I Enable Event Alarm Reporting?

Question

By default, the SNMP NBI cannot report the event alarm. How do I enable the event alarm reporting function?

NOTICE

The SNMP NBI of NCE cannot report events.

Answer

The OSS can change filter criteria in real time to enable event alarm reporting. For details, see **9.1.2 Changing Filter Criteria** or step 4.

Step 1 Log in to the NCE O&M plane.

Step 2 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 3 Choose **SNMP NBI** > **Third-party System Settings** from the navigation pane. Locate the OSS in the list and click the **Edit** icon in the **Operation** column.

Step 4 On the displayed page, click **Expand filter settings**. Make sure **Filter mode** is set to **report**. Check whether **Event** is selected. If it is not, select it and click **Save**.

----End

10.6.8 How Do I Enable or Disable Clear Alarm Reporting?

Question

How do I enable or disable the clear alarm reporting function?

Answer

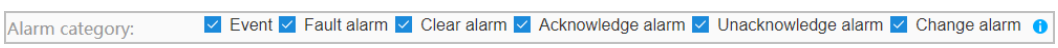
By default, clear alarms are reported after a third-party OSS system is configured. The OSS can change filter criteria in real time to enable or disable clear alarm reporting. For details, see **9.1.2 Changing Filter Criteria** or step 4.

Step 1 Log in to the NCE O&M plane.

Step 2 Open the System Settings app and choose **System Settings** > **Northbound Interface** from the main menu.

Step 3 Choose **SNMP NBI** > **Third-party System Settings** from the navigation pane. Locate the OSS in the list and click the **Edit** icon in the **Operation** column.

Step 4 On the displayed page, click **Expand filter settings**. Make sure **Filter mode** is set to **report**. Check whether **Clear alarm** is selected. If it is not, select it and click **Save**.



----End

10.6.9 A Non-floating IP Address Is Displayed at the Secondary Site After a Switchover in a DR System

Symptom

In a DR system, a floating IP address is configured for the SNMP NBI at the primary site. After a switchover, however, a non-floating IP address is displayed for the SNMP NBI at the secondary site.

Answer

Manually set a floating IP address for the SNMP NBI at the secondary site.

11 Service Port Description

This chapter describes service ports used by NBIs and how to query service ports.

Precautions

In the practical communication process, the source (the server) and the sink (the client) use relevant ports. Usually you only need to specify the source port, and the sink port is dynamically created.

Note the following during the project implementation:

- The service ports used by NCE should not be disabled. Run the following command to view the system service ports:
  ```
  netstat -an
  ```
- If there are routers or firewalls between the source and the sink, check all ports used by the source and the sink. Ensure that these ports can be normally enabled to support the communication between the source and sink.
- On Euler, the port ID of NBIs ranges from 1024 to 65535.

Ports Used Between the NCE Server and the OSS

This part describes the ports used between the NCE server and the OSS.

If a firewall is configured between the NCE server and the OSS, ensure that any port on the OSS can set up connections with ports on NCE.

For ports used by NCE, see iMaster NCE Communication Matrix.

12 MIB1

MIB1 is used mainly used in the management of a multi-domain network or upgrades of NMSs such as the N2000 DMS and N2000 BMS.

MIB1 has two versions: HW-IMAPV1NORTHBOUND-TRAP-MIB and HW-IMAPV2NORTHBOUND-TRAP-MIB. The OSS selects a version based on its supported SMI version.

This document uses HW-IMAPV1NORTHBOUND-TRAP-MIB as an example.

SMI Version	MIB
SMI-V1	HW-IMAPV1NORTHBOUND-TRAP-MIB.mib
SMI-V2	HW-IMAPV2NORTHBOUND-TRAP-MIB.mib

MIB1 supports five types of traps: alarm notification trap, alarm synchronization start trap, alarm synchronization result trap, alarm synchronization end trap, and heartbeat trap. The samples in this section use SNMPv1 as an example. SNMPv2c and SNMPv3 are similar to SNMPv1.

12.1 MIB Description

The complete HW-IMAPV1NORTHBOUND-TRAP-MIB MIB node information is as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).hwNmAgent(1)

The MIB tree is shown as follows:

```
--- huawei(2011)
```



```
        |--- products(2)
            |--- hwNetManagement(15)
                |--- hwNmAgent(1)
                    |---- hwNmFault(3)
```

hwNmFault defines the SNMP NBI of NCE.

For details about the function interfaces of MIB1, see **9.1 MIB1 Subinterfaces**.

For details about the structure and detailed parameters of MIB1, see *iMaster NCE SNMP NBI MIB File*.

NOTE

iMaster NCE SNMP NBI MIB File is available on the Huawei technical support website. To obtain this document, contact the local technical support.

12.2 Alarm Fields Reported by MIB1

MIB1 supports 21 alarm fields. You can customize the alarm fields as required.

When the MIB frame is set to **MIB1**, the SNMP NBI reports the following alarm fields. You can customize them as required.

T2000Support=0

Table 12-1 describes the fields reported by the SNMP NBI if **T2000Support** is **0**.

Table 12-1 T2000Support=0

Name	Name in the MIB	Description	Value	Parsing Supported
NE Name	hwNmNorthboundNEName	Name of the NE where an alarm is generated. • For alarms generated on an NE, the NE name is reported. • For alarms generated due to NE disconnection, the NE name is reported. For example, if alarms are generated due to NE login failures or NE disconnection, the NE name is reported. • If alarms are generated on a WDM NE that is mounted to an optical NE, the name of the optical NE is reported. • For other NMS alarms, the NMS name is reported. By default, **OSS** is reported. If the NMS name is changed, the name of the changed NMS is reported.	Octet string	No
NE Type	hwNmNorthboundNEType	Type of the NE on which alarms are generated. For NMS alarms, the NMS name is reported.	Octet string	No
Object Instance	hwNmNorthboundObjectInstance	Location information. For details, see **Table 12-3**.	Octet string	No

Name	Name in the MIB	Description	Value	Parsing Supported
Event Type	hwNmNorthboundEventType	Alarm type. The options are as follows: • Environment • Equipment • Communication • Service • Process • Security For X.733-compliant alarms, options are as follows: • EnvironmentalAlarm • EquipmentAlarm • CommunicationsAlarm • Quality of Service Alarm • ProcessingErrorAlarm • SecurityAlarm	Octet string	Yes. See the enumerated value.

Name	Name in the MIB	Description	Value	Parsing Supported
Alarm Occurrence Time	hwNmNorthboundEventTime	Time when an alarm is generated, cleared, acknowledged, unacknowledged, or changed. ● If an alarm is generated, this parameter indicates the time when the alarm is generated. ● If an alarm is cleared, this parameter indicates the time when the alarm is cleared. ● If an alarm is acknowledged, this parameter indicates the time when the alarm is acknowledged. ● If an alarm is unacknowledged, this parameter indicates the time when the alarm is unacknowledged. ● If an alarm is changed, this parameter indicates the time when the alarm is changed. ● UTC time. The format is **YYYY/MM/DD - hh:mm:ssZ**. Example: 2009/12/23 - 11:30:30Z ● Local time without the time zone. The format is **YYYY/MM/DD - hh:mm:ss**. Example: 2009/12/23 - 19:30:30 ● Local time with the time zone. The format is **YYYY/MM/DD - hh:mm:ss, hh:mmTZ[DST]**, where TZ stands for the time zone information and	Octet string	Yes. See the time format.

Name	Name in the MIB	Description	Value	Parsing Supported
		DST stands for the DST offset. For example: – 2009/12/23 - 19:30:30 + 08:00[0] (The date is not in DST.) – 2009/12/23 - 19:30:30 + 08:00[+01:00] (The DST offset is 1 hour.) ● Local time. The format is YYYY-MM-dd hh:mm:ss + hh:mm TZ + hh:mm DST, where TZ stands for the time zone information and DST stands for the DST offset. For example: – 2009-12-23 19:30:30 + 08:00 TZ (The date is not in DST.) – 2009-12-23 19:30:30 + 08:00 TZ + 01:00 DST (The DST offset is 1 hour.) ● UTC time. The format is YYYY-MM-dd hh:mm:ss. Example: 2009-12-23 11:30:30		
Alarm Cause	hwNmNorthboundProbableCause	Possible causes of an alarm. Format: ID: [ReasonId],DeviceType: [DeviceTypeId],Alarm Cause	Octet string	No

Name	Name in the MIB	Description	Value	Parsing Supported
Alarm Severity	hwNmNorthboundSeverity	Alarm severity. • Critical • Major • Minor • Warning • Cleared: This option is supported for X.733-compliant alarms.	Octet string	Yes. See the enumerated value.
Alarm Details	hwNmNorthboundEventDetail	ID, device type, and details of an alarm. Format: ID: [AlarmId],DeviceType: [DeviceTypeId],Alarm Details	Octet string	No
Alarm Location	hwNmNorthboundAdditionalInfo	Specific location of the NE where an alarm is generated.	Octet string	No
Type Flag	hwNmNorthboundFaultFlag	Alarm type. The options are as follows: • Event: indicates that an event is generated. • Fault: indicates that an alarm is generated. • Recovery: indicates that the alarm is cleared. • Acknowledge: indicates that the alarm is acknowledged. • Unacknowledge: indicates that the alarm is unacknowledged. • Change: indicates that the alarm is changed.	Octet string	Yes. See the enumerated value.
Alarm Function Category	hwNmNorthboundFaultFunction	Alarm type based on functions, which is the same as hwNmNorthboundEvent-Type.	Octet string	Yes. See the enumerated value.

Name	Name in the MIB	Description	Value	Parsing Supported
Managed Equipment Address	hwNmNorthboundDeviceIP	IP address of an NE. • For transport NEs – If the NE that generates the alarm is a GNE, the IP address of the GNE is reported. – If the NE that generates the alarm is a non-GNE, **0.0.0.0** is reported. • For other NEs, the IP address of the NE is reported. • For NMS alarms, the IP address of the NMS server is reported.	IP address	No
Alarm SN	hwNmNorthboundSerialNo	SN of an alarm.	Integer	No
Alarm Clearance Advice	hwNmNorthboundProbableRepair	Advice for clearing alarms. Format: ID: [ReasonId],DeviceType: [DeviceTypeId], Alarm Clearance Advice	Octet string	No
Resource ID	hwNmNorthboundResourceIDs	ID of the resource on NCE.	Octet string	No
Event Name	hwNmNorthboundEventName	Name of an alarm. Format: ID: [AlarmId],DeviceType: [DeviceTypeId], Event Name	Octet string	No
Alarm Cause ID	hwNmNorthboundReasonID	Alarm cause ID.	Integer	No
Alarm ID	hwNmNorthboundFaultID	Alarm ID.	Integer	No
Managed Equipment Type	hwNmNorthboundDeviceType	Type ID of the managed device.	Octet string	No

Name	Name in the MIB	Description	Value	Parsing Supported
Trail Name	hwNmNorthboundTrailName	Name of the trail affected by an alarm. If alarm A affects a trail, a new change alarm B will be generated. The SN of alarm B is the same as that of alarm A. The severity of alarm B is **Change**. **Trail Name** in alarm B indicates the affected trail. However, for alarm A, **Trail Name** is blank. ● This parameter is applicable for transport and IP NEs. ● This parameter is always blank for access NEs.	Octet string	No
Root Alarm	hwNmNorthboundRootAlarm	Whether the alarm is a root alarm. The options are as follows: ● **0**: non-root alarm ● **1**: root alarm	Integer	Yes. See the enumerated value.
Group ID	hwNmNorthboundGroupID	ID of the alarm group. ● For transport and IP NEs, the alarm group ID and the alarm ID uniquely identify a static alarm. ● For access NEs, the alarm group ID, alarm ID, and alarm cause ID uniquely identify a static alarm.	Integer	No

Name	Name in the MIB	Description	Value	Parsing Supported
Engineering Alarm Status	hwNmNorthboundMaintainStatus	Whether this alarm is generated by the NE in the engineering maintenance state. Maintenance engineers can focus on engineering alarms selectively. • **0**: non-engineering alarm • **1**: engineering alarm **NOTE** NEs during engineering commissioning or service cutover generate a large number of alarms, and you can set the NEs to the engineering maintenance state. Therefore, the alarms generated by this kind of NE are engineering alarms.	Integer	Yes. See the enumerated value.
Root Alarm SN	hwNmNorthboundRootAlarmSerialNo	SN of the root alarm.	Octet string	No
Alarm Acknowledgement Status	hwNmNorthboundConfirmStatus	Alarm acknowledgement status. • 1: acknowledged • 2: unacknowledged	Integer	Yes. See the enumerated value.
Alarm Clearance Status	hwNmNorthboundRestoreStatus	Alarm clearance status. • 1: cleared • 2: uncleared	Integer	Yes. See the enumerated value.

T2000Support=1

Table 12-2 describes the fields reported by the SNMP NBI if **T2000Support** is **1**.

Table 12-2 T2000Support=1

Name	Name in the MIB	T2000Support=1
Object Instance	hwNmNorthboundObjectInstance	Format: source=[NE Name] location=[location information] **source** indicates the alarm source, and **location** indicates the location information. The preceding rule is supported for transport, access, and IP NEs. Example: source=CE1-test-1 location=User name=VTY user IP=10.78.224.206 User channel=VTY4 SN:649018
Alarm Cause	hwNmNorthboundProbableCause	The alarm cause ID and NE ID are not reported, and only the alarm cause is contained. Example: The user logs out or fails to log in.
Alarm Details	hwNmNorthboundEventDetail	The alarm ID and NE ID are not reported, and only the alarm details are contained. Example: NE_NOT_LOGIN
Alarm Clearance Advice	hwNmNorthboundProbableRepair	The alarm cause ID and NE ID are not reported, and only the alarm clearance advice is contained. Example: None
Event Name	hwNmNorthboundEventName	The alarm ID and NE ID are not reported, and only the event name is contained. Example: NE_NOT_LOGIN

Location Information Format

For NE alarms, the location information varies depending on the NE domain.

Table 12-3 Location information format

Domain	Location Information Format	Description
Transport NE (SDH, OSN, MSTP, WDM, PTN, and RTN)	Format: Frame=[Frame ID] Slot=[Slot ID] Port=[Port Number] TTP_TYPE=[Function Block ID] [Location Information] • Frame: indicates the subrack ID. It is the NE ID by default. • Slot: indicates the slot ID. • Port: indicates the logical or physical port on which the alarm is generated. • TTP_TYPE: indicates the function module ID. It is internal information. • Location Information: You cannot parse it.	When a WDM NE is mounted to an optical NE, **Frame ID** is the WDM NE ID. For PTN NEs, **Frame ID** is the NE ID. • The subrack ID is displayed. This field is reported only for NEs with subracks. For example, for SDH NEs that do not have subracks, the subrack ID is not reported. • For port alarms, the slot and port IDs are reported. • For board alarms, the following situations may occur: Only the slot ID is reported; the slot and port IDs are reported, but the port ID is fixed to 65535. • For NE alarms or NMS alarms, the slot or port ID is not reported.
Access NE	Format: Frame=[Frame ID] Slot=[Slot ID] Subslot=[subslot ID] Port=[Port Number] ONUID=[ONU ID] [Non-Physical Location Information] • Frame: indicates the NE ID. • Slot: indicates the slot ID. • Subslot: indicates the subslot ID. • Port: indicates the logical or physical port on which the alarm is generated. • ONUID: indicates the ONU ID. • Non-Physical Location Information: indicates the alarm object name, type, and alias.	Location information reported by NEs. ONUs include MDUs and ONTs.
IP NE (Router, Switch, Security)	Format: [Location Information] [Additional Information]	Alarm information of IP NEs.

12.3 MIB1 Trap

The SNMP NBI supports the following traps when MIB1 is loaded.

12.3.1 Alarm Notification Trap

The active alarm notification trap (**hwNmNorthboundEventNotify**) is reported when new alarms are generated or alarm information changes on NCE.

Function

When alarms are generated on NEs or NCE, the SNMP NBI automatically sends this type of traps to inform the OSS of real-time alarms.

Trigger Condition

When alarms are generated on NEs or NCE, alarm notification traps are triggered.

Definition

Name	ENTERPRISE	Type	Description
hwNmNorthboundEventNotify	hwNmNorthboundEventInfo	Trap/Inform	Real-time alarms are reported.

VB List

In the following table, listed data types are for SNMPv1. The data types complying with SNMPv2c and SNMPv3 are not described if they are the same as those complying with SNMPv1. For any differences, details will be described in brackets.

NOTE

- The definitions of alarm fields in alarm synchronization result traps are the same as those in alarm notification traps. The only difference is that the former is NCE's response to the query of valid alarms, whereas the latter is actively reported by NCE.

Name in the MIB	OID	Type	Description
hwNmNorthboundNEName	1.3.6.1.4.1.2011.2.15.1.7.1.1	Octet string	NE name.
hwNmNorthboundNEType	1.3.6.1.4.1.2011.2.15.1.7.1.2	Octet string	NE type.

Name in the MIB	OID	Type	Description
hwNmNorthboundObjectInstance	1.3.6.1.4.1.2011.2.15.1.7.1.3	Octet string	Alarm location. The options are as follows: • Rack • Frame • Slot • Subslot • Port
hwNmNorthboundEventType	1.3.6.1.4.1.2011.2.15.1.7.1.4	Octet string	Type of an event. The options are as follows: • Communication • Environment • Equipment • Service • Process • Security
hwNmNorthboundEventTime	1.3.6.1.4.1.2011.2.15.1.7.1.5	Octet string	Time when the alarm was generated. The format is as follows: • Local time without time zone in the format of yyyy/MM/dd - hh:mm:ss • UTC time in the format of yyyy/MM/dd - hh:mm:ssZ • Local time with time zone in the format of yyyy/MM/dd - hh:mm:ssTZ[DST] • Local time in the format of yyyy-MM-dd hh:mm:ss + hh:mm TZ + hh:mm DST • UTC time in the format of YYYY-MM-dd hh:mm:ss
hwNmNorthboundProbableCause	1.3.6.1.4.1.2011.2.15.1.7.1.6	Octet string	Possible causes of an alarm.

Name in the MIB	OID	Type	Description
hwNmNorthboundSeverity	1.3.6.1.4.1.2011.2.15.1.7.1.7	Octet string	Alarm severity. The options are as follows: • Critical • Major • Minor • Warning • Indeterminate
hwNmNorthboundEventDetail	1.3.6.1.4.1.2011.2.15.1.7.1.8	Octet string	Alarm ID and detailed information.
hwNmNorthboundAdditionalInfo	1.3.6.1.4.1.2011.2.15.1.7.1.9	Octet string	Additional information of an NE.
hwNmNorthboundFaultFlag	1.3.6.1.4.1.2011.2.15.1.7.1.10	Octet string	Flag bit for an alarm. The options are as follows: • Event: indicates that an event is generated. • Fault: indicates that an alarm is generated. • Recovery: indicates that the alarm is cleared. • Acknowledge: indicates that the alarm is acknowledged. • Unacknowledge: indicates that the alarm is unacknowledged. • Change: indicates that the alarm is changed. • UNKNOWN_EVENT_TYPE: unknown event type.
hwNmNorthboundFaultFunction	1.3.6.1.4.1.2011.2.15.1.7.1.11	Octet string	Alarm type. The options are as follows: • Environment • Equipment • Communication • Service • Security • Process
hwNmNorthboundDeviceIP	1.3.6.1.4.1.2011.2.15.1.7.1.12	IpAddress	IP address of an NE.

Name in the MIB	OID	Type	Description
hwNmNorthboundSerialNo	1.3.6.1.4.1.2011.2.15.1.7.1.13	INTEGER	SN of an alarm.
hwNmNorthboundProbableRepair	1.3.6.1.4.1.2011.2.15.1.7.1.14	Octet string	Alarm troubleshooting suggestions.
hwNmNorthboundResourceIDs	1.3.6.1.4.1.2011.2.15.1.7.1.15	Octet string	ID of a resource.
hwNmNorthboundsAdditionalVB1	1.3.6.1.4.1.2011.2.15.1.7.1.16	Octet string	Alarm UUID of the physical resources (NEs, boards, and ports) in the IP domain.
hwNmNorthboundsAdditionalVB2	1.3.6.1.4.1.2011.2.15.1.7.1.17	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB3	1.3.6.1.4.1.2011.2.15.1.7.1.18	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB4	1.3.6.1.4.1.2011.2.15.1.7.1.19	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB5	1.3.6.1.4.1.2011.2.15.1.7.1.20	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB6	1.3.6.1.4.1.2011.2.15.1.7.1.21	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB7	1.3.6.1.4.1.2011.2.15.1.7.1.22	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB8	1.3.6.1.4.1.2011.2.15.1.7.1.23	Octet string	Reserved field.
hwNmNorthboundEventName	1.3.6.1.4.1.2011.2.15.1.7.1.24	Octet string	Name of an event.
hwNmNorthboundReasonID	1.3.6.1.4.1.2011.2.15.1.7.1.25	INTEGER	Alarm ID.
hwNmNorthboundFaultID	1.3.6.1.4.1.2011.2.15.1.7.1.26	INTEGER	Fault ID of an alarm.
hwNmNorthboundDeviceType	1.3.6.1.4.1.2011.2.15.1.7.1.27	Octet string	Device type ID of an alarm.

Name in the MIB	OID	Type	Description
hwNmNorthboundTrailName	1.3.6.1.4.1.2011.2.15.1.7.1.28	Octet string	Name of the trail affected by an alarm.
hwNmNorthboundRootAlarm	1.3.6.1.4.1.2011.2.15.1.7.1.29	Integer	Whether the alarm is the root alarm. • **0**: non-root alarm • **1**: root alarm
hwNmNorthboundGroupID	1.3.6.1.4.1.2011.2.15.1.7.1.30	Integer	Alarm group ID.
hwNmNorthboundMaintainStatus	1.3.6.1.4.1.2011.2.15.1.7.1.31	Integer	Engineering alarm status.
hwNmNorthboundRootAlarmSerialNo	1.3.6.1.4.1.2011.2.15.1.7.1.32	Octet string	SN of the root alarm.
hwNmNorthboundConfirmStatus	1.3.6.1.4.1.2011.2.15.1.7.1.33	Integer	Alarm acknowledgement status. • 1: acknowledged • 2: unacknowledged
hwNmNorthboundRestoreStatus	1.3.6.1.4.1.2011.2.15.1.7.1.34	Integer	Alarm clearance status. • 1: cleared • 2: uncleared

12.3.2 Alarm Synchronization Start Trap

The alarm synchronization start trap (**hwNmNorthboundEventSynchronizationCommandStart**) informs the OSS that alarm synchronization has started.

Function

After the OSS sends alarm query requests, the SNMP NBI returns this type of trap to the OSS to indicate that alarm synchronization has started.

Trigger Condition

The OSS triggers the alarm synchronization. For details, see **9.1.3 Synchronizing Alarms**.

The OSS sets **hwNmNorthboundEventSynchronizationCommandStart** in the following format:

NMS IP address:Port:Start time:End time

NOTE

- *NMS IP address:Port* refers to the IP address and port of the OSS.
- The format for the start time and end time is *YYYYMMDDhhmmss*.

Definition

Name	ENTERPRISE	Type	Description
hwNmNorthboundEventSynchronizationStartNotify	hwNmNorthboundEventSynchronizationStart	Trap/Inform	Alarm synchronization start trap.

VB List

None

12.3.3 Alarm Synchronization Result Trap

The alarm synchronization result trap (**hwNmNorthboundEventSynchronizationQueryResult**) carries information about alarms on NCE.

Function

After the OSS initiates the alarm synchronization, the SNMP NBI sends this type of traps to report required alarms on NCE to the OSS.

Trigger Condition

The OSS triggers the alarm synchronization. For details, see **9.1.3 Synchronizing Alarms**.

The OSS sets **hwNmNorthboundEventSynchronizationCommandStart** in the following format:

NMS IP address:Port:Start time:End time

NOTE

- *NMS IP address:Port* refers to the IP address and port of the OSS.
- The format for the start time and end time is *YYYYMMDDhhmmss*.

Definition

Name	ENTERPRISE	Type	Description
hwNmNorthboundEventSynchronizationQueryResultNotify	hwNmNorthboundEventSynchronizationQueryResult	Trap/Inform	Alarm synchronization result.

VB List

In the following table, listed data types are for SNMPv1. The data types complying with SNMPv2c and SNMPv3 are not described if they are the same as those complying with SNMPv1. For any differences, details will be described in brackets.

NOTE

- The definitions of alarm fields in alarm synchronization result traps are the same as those in alarm notification traps. The only difference is that the former is NCE's response to the query of valid alarms, whereas the latter is actively reported by NCE.

Name in the MIB	OID	Type	Description
hwNmNorthboundNEName	1.3.6.1.4.1.2011.2.15.1.7.1.1	Octet string	NE name.
hwNmNorthboundNEType	1.3.6.1.4.1.2011.2.15.1.7.1.2	Octet string	NE type.
hwNmNorthboundObjectInstance	1.3.6.1.4.1.2011.2.15.1.7.1.3	Octet string	Alarm location. The options are as follows: • Rack • Frame • Slot • Subslot • Port
hwNmNorthboundEventType	1.3.6.1.4.1.2011.2.15.1.7.1.4	Octet string	Type of an event. The options are as follows: • Communication • Environment • Equipment • Service • Process • Security

Name in the MIB	OID	Type	Description
hwNmNorthboundEventTime	1.3.6.1.4.1.2011.2.15.1.7.1.5	Octet string	Time when the alarm was generated. The format is as follows: • Local time without time zone in the format of yyyy/MM/dd - hh:mm:ss • UTC time in the format of yyyy/MM/dd - hh:mm:ssZ • Local time with time zone in the format of yyyy/MM/dd - HH:mm:ss TZ[DST] • Local time in the format of yyyy-MM-dd hh:mm:ss + hh:mm TZ + hh:mm DST • UTC time in the format of YYYY-MM-dd hh:mm:ss
hwNmNorthboundProbableCause	1.3.6.1.4.1.2011.2.15.1.7.1.6	Octet string	Possible causes of an alarm.
hwNmNorthboundSeverity	1.3.6.1.4.1.2011.2.15.1.7.1.7	Octet string	Alarm severity. The options are as follows: • Critical • Major • Minor • Warning • Indeterminate
hwNmNorthboundEventDetail	1.3.6.1.4.1.2011.2.15.1.7.1.8	Octet string	Alarm ID and detailed information.
hwNmNorthboundAdditionalInfo	1.3.6.1.4.1.2011.2.15.1.7.1.9	Octet string	Additional information of an NE.

Name in the MIB	OID	Type	Description
hwNmNorthboundFaultFlag	1.3.6.1.4.1.2011.2.15.1.7.1.10	Octet string	Flag bit for an alarm. The options are as follows: • Event: indicates that an event is generated. • Fault: indicates that an alarm is generated. • Recovery: indicates that the alarm is cleared. • Acknowledge: indicates that the alarm is acknowledged. • Unacknowledge: indicates that the alarm is unacknowledged. • Change: indicates that the alarm is changed. • UNKNOWN_EVENT_TYPE: unknown event type.
hwNmNorthboundFaultFunction	1.3.6.1.4.1.2011.2.15.1.7.1.11	Octet string	Alarm type. The options are as follows: • Communication • Environment • Equipment • Service • Process • Security
hwNmNorthboundDeviceIP	1.3.6.1.4.1.2011.2.15.1.7.1.12	IpAddress	IP address of an NE.
hwNmNorthboundSerialNo	1.3.6.1.4.1.2011.2.15.1.7.1.13	INTEGER	SN of an alarm.
hwNmNorthboundProbableRepair	1.3.6.1.4.1.2011.2.15.1.7.1.14	Octet string	Alarm troubleshooting suggestions.
hwNmNorthboundResourceIDs	1.3.6.1.4.1.2011.2.15.1.7.1.15	Octet string	ID of a resource.
hwNmNorthboundsAdditionalVB1	1.3.6.1.4.1.2011.2.15.1.7.1.16	Octet string	Alarm UUID of the physical resources (NEs, boards, and ports) in the IP domain.

Name in the MIB	OID	Type	Description
hwNmNorthboundsAdditionalVB2	1.3.6.1.4.1.2011.2.15.1.7.1.17	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB3	1.3.6.1.4.1.2011.2.15.1.7.1.18	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB4	1.3.6.1.4.1.2011.2.15.1.7.1.19	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB5	1.3.6.1.4.1.2011.2.15.1.7.1.20	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB6	1.3.6.1.4.1.2011.2.15.1.7.1.21	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB7	1.3.6.1.4.1.2011.2.15.1.7.1.22	Octet string	Reserved field.
hwNmNorthboundsAdditionalVB8	1.3.6.1.4.1.2011.2.15.1.7.1.23	Octet string	Reserved field.
hwNmNorthboundEventName	1.3.6.1.4.1.2011.2.15.1.7.1.24	Octet string	Name of an event.
hwNmNorthboundReasonID	1.3.6.1.4.1.2011.2.15.1.7.1.25	INTEGER	Alarm ID.
hwNmNorthboundFaultID	1.3.6.1.4.1.2011.2.15.1.7.1.26	INTEGER	Fault ID of an alarm.
hwNmNorthboundDeviceType	1.3.6.1.4.1.2011.2.15.1.7.1.27	Octet string	Device type ID of an alarm.
hwNmNorthboundTrailName	1.3.6.1.4.1.2011.2.15.1.7.1.28	Octet string	Name of the trail affected by an alarm.
hwNmNorthboundRootAlarm	1.3.6.1.4.1.2011.2.15.1.7.1.29	Integer	Whether the alarm is the root alarm. • **0**: non-root alarm • **1**: root alarm
hwNmNorthboundGroupID	1.3.6.1.4.1.2011.2.15.1.7.1.30	Integer	Alarm group ID.

Name in the MIB	OID	Type	Description
hwNmNorthboundMaintainStatus	1.3.6.1.4.1.2011.2.15.1.7.1.31	Integer	Engineering alarm status.
hwNmNorthboundRootAlarmSerialNo	1.3.6.1.4.1.2011.2.15.1.7.1.32	Octet string	SN of the root alarm.
hwNmNorthboundConfirmStatus	1.3.6.1.4.1.2011.2.15.1.7.1.33	Integer	Alarm acknowledgement status. • 1: acknowledged • 2: unacknowledged
hwNmNorthboundRestoreStatus	1.3.6.1.4.1.2011.2.15.1.7.1.34	Integer	Alarm clearance status. • 1: cleared • 2: uncleared

12.3.4 Alarm Synchronization End Trap

The alarm synchronization end trap (**hwNmNorthboundEventSynchronizationCommandStop**) informs the OSS that alarm synchronization has ended.

Function

NCE sends this type of traps to inform the OSS of the end of alarm synchronization.

Trigger Condition

Alarm synchronization end traps are triggered when:

- All required alarms on NCE have been reported to the OSS in trap packets.
- The OSS stops the synchronization.

The OSS triggers the termination of synchronization. For details, see **9.1.3 Synchronizing Alarms**.

The OSS set **hwNmNorthboundEventSynchronizationCommandStop** in the following format: *NMS IP address:port number*.

NOTE

NMS IP address:Port refers to the IP address and port of the OSS.

Definition

Name	ENTERPRISE	Type	Description
hwNmNorthboundEventSynchronizationEndNotify	hwNmNorthboundEventSynchronizationEnd	Trap/Inform	Alarm synchronization end trap.

VB List

In the following table, listed data types are for SNMPv1. The data types complying with SNMPv2c and SNMPv3 are not described if they are the same as those complying with SNMPv1. For any differences, details will be described in brackets.

VB	OID	Data Type	Description
hwNmNorthboundEventSynchronizationEndStatus	1.3.6.1.4.1.2011.2.15.1.7.7.3.1	INTEGER	Alarm synchronization result. The options are as follows: 1: normalEnd(1), which indicates that the synchronization was complete. 2: stopped(2), which indicates that the OSS stopped the synchronization. 3: error(3), which indicates that exceptions occurred during the synchronization.
hwNmNorthboundEventSynchronizationEndStatusDetail	1.3.6.1.4.1.2011.2.15.1.7.7.3.2	OCTET STRING	Details about the synchronization result.

12.3.5 KeepAlive Info (Heartbeat) Trap

The heartbeat notification trap (**hwNmNorthboundEventKeepAliveInfo**) informs the OSS that it is properly communicating with NCE.

Function

NCE sends the KeepAlive info (heartbeat) to the OSS regularly each period. If the OSS receives the trap, the connection between the OSS and NCE works. If the OSS does not receive the trap in this period and the heartbeat is disabled, the OSS disconnects with NCE.

NOTE

You can configure the heartbeat period. For details, see **6.2.2 Advanced Settings**.

Trigger Condition

NCE sends the KeepAlive info (heartbeat) trap to the OSS regularly in the preset period.

Definition

Name	ENTERPRISE	OID	Type	Description
hwNmNorthboundEventKeepAlive	hwNmNorthboundEventKeepAliveInfo	1.3.6.1.4.1.2011.2.15.1.7.2.0.2	Trap/Inform	Notification for the Keep Alive traps.

VB List

In the following table, listed data types are for SNMPv1. The data types complying with SNMPv2c and SNMPv3 are not described if they are the same as those complying with SNMPv1. For any differences, details will be described in brackets.

Name	OID	Data Type	Description
hwNmAgent	1.3.6.1.4.1.2011.2.15.1	OCTET STRING	By default, this field is reported.
hwNmNorthboundKeepAlive	1.3.6.1.4.1.2011.2.15.1.7.2.1	OCTET STRING	You can make configurations for the heartbeat notification trap to report this field.

NOTICE

By default, the heartbeat notification trap reports the **hwNMAgent** field. You can make modifications for the trap to report the **hwNmNorthboundKeepAlive** field.

12.4 MIB1 Trap Sample

MIB1 supports five types of traps: alarm notification trap, alarm synchronization start trap, alarm synchronization result trap, alarm synchronization end trap, and heartbeat trap. The samples in this section use SNMPv1 as an example. SNMPv2c and SNMPv3 are similar to SNMPv1.

12.4.1 Alarm Notification Trap

Two formats are available for alarm notifications when the MIB1 is used. They are used to manage multi-domain devices and optical devices of the transport domain, respectively.

Description of the T2000support Configuration Item

The default value of the **T2000support** configuration item is **1**. Check and change the value before an upgrade to ensure compatibility. You must configure the item manually.

Table 12-4 Configuration file path

Version	File Path
Versions earlier than NCE V100R018C00	$IMAP_ROOT/server/etc/nbi/snmp/snmpagent.xml
NCE V100R018C00 and later versions	There is no configuration file, and the configuration items can be configured on the NCEO&M plane.

Table 12-5 Description of the T2000support configuration item

Scenario	T2000support Configuration Item	Example Value of hwNmNorthboundObjectInstance	Description
Managing multi-domain NEs	mib1.T2000Support=0	hwNmNorthboundObjectInstance.0 *** (octets) Slot=4 Port=1 TTP_TYPE=1 4-N1SL16-1(SDH-1)-SPI:1	• This mode applies to the multi-domain NE scenario. • Alarm field: The reported alarm location information contains only the alarm ID. • Information about optical NEs cannot be reported.
Managing optical NEs of the transport domain	mib1.T2000Support=01	hwNmNorthboundObjectInstance.0 *** (octets) source=NE (9-3500) location=4-N1SL16-1(SDH-1)-SPI:1	• Alarm field: The redundant information, such as the alarm ID and device type, is deleted from the reported alarm information. • Information about optical NEs can be reported.

mib1.T2000Support=0

```
13: Specific trap hwNmNorthboundEventInfo::hwNmNorthboundEventNotify #1 trap(v1)
received from: 10.71.224.13 at 2011-12-01 16:19:58
  Time stamp: 0 days 00h:05m:29s.09th
  Agent address: 10.71.224.13 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.70.71.97 Port: 6666 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.71.224.13
  Enterprise: hwNmNorthboundEventInfo
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventNotify, Module: HW-IMAPV1NORTHBOUND-TRAP-MIB,
Enterprise: hwNmNorthboundEventInfo
  Bindings (24)
    Binding #1: hwNmNorthboundNEName.0 *** (octets) NE(9-3500)
    Binding #2: hwNmNorthboundNEType.0 *** (octets) OptiX OSN 3500
    Binding #3: hwNmNorthboundObjectInstance.0 *** (octets) Slot=4 Port=1 TTP_TYPE=1 4-
N1SL16-1(SDH-1)-SPI:1
    Binding #4: hwNmNorthboundEventType.0 *** (octets) Communication
    Binding #5: hwNmNorthboundEventTime.0 *** (octets) 2011/04/27 - 16:11:30
    Binding #6: hwNmNorthboundProbableCause.0 *** (octets) ID:1,DeviceType:0,
(1)The fiber jumper is not connected at the optical interface of the board;
(2)The laser of the board on the opposite station is shutdown;
(3)A fiber break occurs in the transm ...
    Binding #7: hwNmNorthboundSeverity.0 *** (octets) Critical
    Binding #8: hwNmNorthboundEventDetail.0 *** (octets) ID:1,DeviceType:0,Loss of signal
    Binding #9: hwNmNorthboundAdditionalInfo.0 *** (octets)
Alarm Parameter(hex) 0x01 0x00 0x01 0x01 0x01
    Binding #10: hwNmNorthboundFaultFlag.0 *** (octets) Fault
    Binding #11: hwNmNorthboundFaultFunction.0 *** (octets) Communication
    Binding #12: hwNmNorthboundDeviceIP.0 *** (ipaddr) 10.70.71.97
    Binding #13: hwNmNorthboundSerialNo.0 *** (int32) 85415
    Binding #14: hwNmNorthboundProbableRepair.0 *** (octets) ID:1,DeviceType:0,
    Binding #15: hwNmNorthboundResourceIDs.0 *** (octets) 3145893.-1.4.1.1.1.-1.-1
    Binding #16: hwNmNorthboundEventName.0 *** (octets) ID:1,DeviceType:0,R_LOS
    Binding #17: hwNmNorthboundReasonID.0 *** (int32) 1
    Binding #18: hwNmNorthboundFaultID.0 *** (int32) 1
    Binding #19: hwNmNorthboundDeviceType.0 *** (octets) 0
    Binding #20: hwNmNorthboundTrailName.0 *** (octets) PWE3:2
    Binding #21: hwNmNorthboundRootAlarm.0 *** (int32) 0
    Binding #22: hwNmNorthboundGroupID.0 *** (int32) 268374017
    Binding #23: hwNmNorthboundMaintainStatus.0 *** (int32) 0
    Binding #24: hwNmNorthboundRootAlarmSerialNo.0 *** (octets) (zero-length)
```

mib1.T2000Support=1

```
21: Specific trap hwNmNorthboundEventInfo::hwNmNorthboundEventNotify #1 trap(v1)
received from: 10.71.224.13 at 2011-12-01 16:25:24
  Time stamp: 0 days 00h:02m:02s.27th
  Agent address: 10.71.224.13 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.70.71.97 Port: 6666 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.71.224.13
  Enterprise: hwNmNorthboundEventInfo
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventNotify, Module: HW-IMAPV1NORTHBOUND-TRAP-MIB,
Enterprise: hwNmNorthboundEventInfo
  Bindings (24)
    Binding #1: hwNmNorthboundNEName.0 *** (octets) NE(9-3500)
    Binding #2: hwNmNorthboundNEType.0 *** (octets) OptiX OSN 3500
    Binding #3: hwNmNorthboundObjectInstance.0 *** (octets) source=NE(9-3500) location=4-
N1SL16-1(SDH-1)-SPI:1
```



```
   Binding #4: hwNmNorthboundEventType.0 *** (octets) Communication
   Binding #5: hwNmNorthboundEventTime.0 *** (octets) 2011/04/27 - 16:11:30
   Binding #6: hwNmNorthboundProbableCause.0 *** (octets)
(1)The fiber jumper is not connected at the optical interface of the board;
(2)The laser of the board on the opposite station is shutdown;
(3)A fiber break occurs in the transmission line;
(4) T ...
   Binding #7: hwNmNorthboundSeverity.0 *** (octets) Critical
   Binding #8: hwNmNorthboundEventDetail.0 *** (octets) Loss of signal
   Binding #9: hwNmNorthboundAdditionalInfo.0 *** (octets)
Alarm Parameter(hex) 0x01 0x00 0x01 0x01 0x01
   Binding #10: hwNmNorthboundFaultFlag.0 *** (octets) Fault
   Binding #11: hwNmNorthboundFaultFunction.0 *** (octets) Communication
   Binding #12: hwNmNorthboundDeviceIP.0 *** (ipaddr) 10.70.71.97
   Binding #13: hwNmNorthboundSerialNo.0 *** (int32) 85417
   Binding #14: hwNmNorthboundProbableRepair.0 *** (octets) (zero-length)
   Binding #15: hwNmNorthboundResourceIDs.0 *** (octets) 3145893.-1.4.1.1.1.-1.-1
   Binding #16: hwNmNorthboundEventName.0 *** (octets) R_LOS
   Binding #17: hwNmNorthboundReasonID.0 *** (int32) 1
   Binding #18: hwNmNorthboundFaultID.0 *** (int32) 1
   Binding #19: hwNmNorthboundDeviceType.0 *** (octets) 0
   Binding #20: hwNmNorthboundTrailName.0 *** (octets) PWE3:2
   Binding #21: hwNmNorthboundRootAlarm.0 *** (int32) 0
   Binding #22: hwNmNorthboundGroupID.0 *** (int32) 268374017
   Binding #23: hwNmNorthboundMaintainStatus.0 *** (int32) 0
   Binding #24: hwNmNorthboundRootAlarmSerialNo.0 *** (octets) (zero-length)
```

12.4.2 Alarm Synchronization Start Trap

After the OSS sends alarm synchronization requests, the SNMP NBI returns the start notification of alarm synchronization.

```
18: Specific trap
hwNmNorthboundEventSynchronizationStart::hwNmNorthboundEventSynchronizationStartNotif
y #9 trap(v1) received from: 10.71.88.151 at 2010-11-24 15:56:45
  Time stamp: 0 days 00h:06m:24s.69th
  Agent address: 10.71.88.151 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.70.73.96 Port: 8888 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.71.88.151
  Enterprise: hwNmNorthboundEventSynchronizationStart
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventSynchronizationStartNotify, Module: HW-
IMAPV1NORTHBOUND-TRAP-MIB, Enterprise: hwNmNorthboundEventSynchronizationStart
  Bindings (0)
    None.
```

12.4.3 Alarm Synchronization Result Trap

After the OSS sends alarm synchronization requests, the SNMP NBI will report the alarms meeting filter criteria to the OSS.

```
101: Specific trap
hwNmNorthboundEventSynchronizationQueryResult::hwNmNorthboundEventSynchronizationQu
eryResultNotify #10 trap(v1) received from: 10.71.88.151 at 2011-12-01 15:56:49
  Time stamp: 0 days 00h:06m:28s.55th
  Agent address: 10.71.88.151 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.70.73.96 Port: 8888 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.71.88.151
  Enterprise: hwNmNorthboundEventSynchronizationQueryResult
```



```
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventSynchronizationQueryResultNotify, Module: HW-
IMAPV1NORTHBOUND-TRAP-MIB, Enterprise:
hwNmNorthboundEventSynchronizationQueryResult
  Bindings (24)
    Binding #1: hwNmNorthboundNEName.0 *** (octets) NE(9-1954)
    Binding #2: hwNmNorthboundNEType.0 *** (octets) OptiX PTN 3900
    Binding #3: hwNmNorthboundObjectInstance.0 *** (octets) TUNNEL:
(463,10.10.10.11,10.10.10.12)
    Binding #4: hwNmNorthboundEventType.0 *** (octets) Communication
    Binding #5: hwNmNorthboundEventTime.0 *** (octets) 2010/10/31 - 17:09:46
    Binding #6: hwNmNorthboundProbableCause.0 *** (octets) ID:12814,DeviceType:128450560,
1. The physical link fails.
2. The network is severely congested.
3. The opposite equipment is faulty.
    Binding #7: hwNmNorthboundSeverity.0 *** (octets) Critical
    Binding #8: hwNmNorthboundEventDetail.0 *** (octets) ID:12814,DeviceType:128450560,Loss
of Connectivity Verification defect
    Binding #9: hwNmNorthboundAdditionalInfo.0 *** (octets)
Alarm Parameter II(hex) 0x0f
    Binding #10: hwNmNorthboundFaultFlag.0 *** (octets) Fault
    Binding #11: hwNmNorthboundFaultFunction.0 *** (octets) Communication
    Binding #12: hwNmNorthboundDeviceIP.0 *** (octets) 10.78.217.248
    Binding #13: hwNmNorthboundSerialNo.0 *** (int32) 60229
    Binding #14: hwNmNorthboundProbableRepair.0 *** (octets) ID:12814,DeviceType:128450560,
    Binding #15: hwNmNorthboundResourceIDs.0 *** (octets) 3145793.-1.-1.-1.-1.-1.-1.-1
    Binding #16: hwNmNorthboundEventName.0 *** (octets) ID:12814,DeviceType:
128450560,MPLS_TUNNEL_LOCV
    Binding #17: hwNmNorthboundReasonID.0 *** (int32) 12814
    Binding #18: hwNmNorthboundFaultID.0 *** (int32) 0
    Binding #19: hwNmNorthboundDeviceType.0 *** (octets) 128450560
    Binding #20: hwNmNorthboundTrailName.0 *** (octets) PWE3:2
    Binding #21: hwNmNorthboundRootAlarm.0 *** (int32) 0
    Binding #22: hwNmNorthboundGroupID.0 *** (int32) 268374017
    Binding #23: hwNmNorthboundMaintainStatus.0 *** (int32) 0
    Binding #24: hwNmNorthboundRootAlarmSerialNo.0 *** (octets) (zero-length)
```

12.4.4 Alarm Synchronization End Trap

Alarm synchronization end traps are triggered when all required alarms have been reported to the OSS or the OSS automatically stops the synchronization.

Synchronization Stopped After Alarm Reporting Was Complete

After all required alarms are reported to the OSS, SNMP NBI sends traps through the SNMP NBI to inform the OSS of the stop of alarm reporting.

```
1335: Specific trap
hwNmNorthboundEventSynchronizationEnd::hwNmNorthboundEventSynchronizationEndNotify
#11 trap(v1) received from: 10.71.88.151 at 2010-11-24 15:57:45
  Time stamp: 0 days 00h:07m:25s.16th
  Agent address: 10.71.88.151 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.70.73.96 Port: 8888 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.71.88.151
  Enterprise: hwNmNorthboundEventSynchronizationEnd
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventSynchronizationEndNotify, Module: HW-
IMAPV1NORTHBOUND-TRAP-MIB, Enterprise: hwNmNorthboundEventSynchronizationEnd
  Bindings (2)
    Binding #1: hwNmNorthboundEventSynchronizationEndStatus.0 *** (int32) normalEnd(1)
```



```
  Binding #2: hwNmNorthboundEventSynchronizationEndStatusDetail.0 *** (octets) Sync End:
Successfully queried all alarms!
```

Synchronization Was Stopped by the OSS

The OSS can also stop the synchronization as required. The SNMP NBI then reports traps to inform the OSS of the stop of alarm synchronization, as a response to the request.

```
2420: Specific trap
hwNmNorthboundEventSynchronizationEnd::hwNmNorthboundEventSynchronizationEndNotify
#11 trap(v1) received from: 10.71.88.151 at 2010-11-24 16:04:01
 Time stamp: 0 days 00h:13m:40s.35th
 Agent address: 10.71.88.151 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
 Manager address: 10.70.73.96 Port: 8888 Transport: IP/UDP
Community: ******
 SNMPv1 agent address: 10.71.88.151
 Enterprise: hwNmNorthboundEventSynchronizationEnd
 Specific Trap MIB Lookup Results
  Name: hwNmNorthboundEventSynchronizationEndNotify, Module: HW-
IMAPV1NORTHBOUND-TRAP-MIB, Enterprise: hwNmNorthboundEventSynchronizationEnd
 Bindings (2)
  Binding #1: hwNmNorthboundEventSynchronizationEndStatus.0 *** (int32) stopped(2)
  Binding #2: hwNmNorthboundEventSynchronizationEndStatusDetail.0 *** (octets) Sync
Stopped: The synchronization is stopped by the NMS's command!
```

Synchronization Was Stopped Unexpectedly

```
403: Specific trap
hwNmNorthboundEventSynchronizationEnd::hwNmNorthboundEventSynchronizationEndNotify
#11 trap(v1) received from: 10.71.224.13 at 2011-4-27 16:44:56
 Time stamp: 0 days 00h:03m:31s.64th
 Agent address: 10.71.224.13 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
 Manager address: 10.70.71.97 Port: 6666 Transport: IP/UDP
Community: ******
 SNMPv1 agent address: 10.71.224.13
 Enterprise: hwNmNorthboundEventSynchronizationEnd
 Specific Trap MIB Lookup Results
  Name: hwNmNorthboundEventSynchronizationEndNotify, Module: HW-
IMAPV1NORTHBOUND-TRAP-MIB, Enterprise: hwNmNorthboundEventSynchronizationEnd
 Bindings (2)
  Binding #1: hwNmNorthboundEventSynchronizationEndStatus.0 *** (int32) error(3)
  Binding #2: hwNmNorthboundEventSynchronizationEndStatusDetail.0 *** (octets) Sync Error:
Query failed as Agent shutting down!
```

12.4.5 Heartbeat Trap

The SNMP NBI sends heartbeat traps to the OSS periodically. Based on the heartbeats, the OSS determines whether the connection with the SNMP NBI is proper.

NOTE

Two OIDs are supported.

hwNmAgent (Default)

```
795: Specific trap hwNmNorthboundEventKeepAliveInfo::hwNmNorthboundEventKeepAlive #2
trap(v1) received from: 10.71.88.151 at 2010-11-24 15:57:20
 Time stamp: 0 days 00h:07m:00s.12th
```



```
  Agent address: 10.71.88.151 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.70.73.96 Port: 8888 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.71.88.151
  Enterprise: hwNmNorthboundEventKeepAliveInfo
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventKeepAlive, Module: HW-IMAPV1NORTHBOUND-TRAP-MIB,
Enterprise: hwNmNorthboundEventKeepAliveInfo
  Bindings (1)
    Binding #1: hwNmAgent *** (octets) SNMP Agent
```

hwNmNorthboundKeepAlive (Configurable-1.3.6.1.4.1.2011.2.15.1.7.2.1)

```
8: Specific trap hwNmNorthboundEventKeepAliveInfo::hwNmNorthboundEventKeepAlive #2
trap(v1) received from: 10.67.192.220 at 2012/6/26 11:19:13
  Time stamp: 0 days 00h:00m:15s.04th
  Agent address: 10.67.192.220 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.66.102.169 Port: 6666 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.67.192.220
  Enterprise: hwNmNorthboundEventKeepAliveInfo
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventKeepAlive, Module: HW-IMAPV1NORTHBOUND-TRAP-MIB,
Enterprise: hwNmNorthboundEventKeepAliveInfo
  Bindings (1)
    Binding #1: hwNmNorthboundKeepAlive *** (octets) SNMP Agent
```

hwNmNorthboundKeepAlive (Configurable-1.3.6.1.4.1.2011.2.15.1.7.2.1.0)

```
3: Specific trap hwNmNorthboundEventKeepAliveInfo::hwNmNorthboundEventKeepAlive #2
trap(v1) received from: 10.78.219.70 at 2012/7/26 19:11:29
  Time stamp: 0 days 00h:01m:45s.11th
  Agent address: 10.78.219.70 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.66.103.78 Port: 6666 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.78.219.70
  Enterprise: hwNmNorthboundEventKeepAliveInfo
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventKeepAlive, Module: HW-IMAPV1NORTHBOUND-TRAP-MIB,
Enterprise: hwNmNorthboundEventKeepAliveInfo
  Bindings (1)
    Binding #1: hwNmNorthboundKeepAlive.0 *** (octets) SNMP Agent
```


13 MIB2

The MIB2 has two versions: IMAP_NORTHBOUND_MIB-V1.mib and IMAP_NORTHBOUND_MIB-V2.mib. The OSS selects a version based on its supported SMI version.

This document uses IMAP_NORTHBOUND_MIB-V1.mib as an example.

SMI Version	MIB
SMI-V1	IMAP_NORTHBOUND_MIB-V1.mib
SMI-V2	IMAP_NORTHBOUND_MIB-V2.mib

MIB2 supports five types of traps: alarm notification trap, alarm synchronization start trap, alarm synchronization result trap, alarm synchronization end trap, and heartbeat trap. The samples in this section use SNMPv1 as an example. SNMPv2c and SNMPv3 are similar to SNMPv1.

13.1 MIB Description

The complete HW-IMAPV1NORTHBOUND-TRAP-MIB node is:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).hwNetManagement(15).hwNmAgent(1)

The MIB tree is shown as follows:

```
--- huawei(2011)
        |--- products(2)
            |--- hwNetManagement(15)
                |--- hwNmAgent(1)
                    |---- hwNmFault(3)
```


hwNmFault defines the SNMP NBI of NCE.

For details about the function interfaces of MIB2, see **9.2 MIB2 Subinterfaces**.

For details about the structure and detailed parameters of MIB2, see *iMaster NCE SNMP NBI MIB File*.

NOTE

iMaster NCE SNMP NBI MIB File is available on the Huawei technical support website. To obtain this document, contact the local technical support.

13.2 Alarm Fields Reported by MIB2

When the MIB frame is set to **MIB2**, the SNMP NBI reports the following alarm fields. You can customize them as required.

Table 13-1 Alarm fields

Name	Name in the MIB	Description	Value	Parsing Supported
Alarm SN	iMAPNorthboundAlarmCSN	Network SN of an alarm, which uniquely identifies an alarm.	Octet string	No
Alarm Category	iMAPNorthboundAlarmCategory	Category of an alarm, which can be set to: • 1: Fault • 2: Clear • 4: Acknowledge • 5: Unacknowledge • 9: Change	Octet string	Yes. See the enumerated value.
Alarm Occurrence Time	iMAPNorthboundAlarmOccurTime	Time when an alarm is generated.	Octet string	No
Device Name	iMAPNorthboundAlarmMOName	Name of a device.	Octet string	No

Name	Name in the MIB	Description	Value	Parsing Supported
Product Series ID	iMAPNorthboundAlarmProductID	ID of product series, which can be set to: ● 0: Unknown ● 1: PhysicalServer ● 2: NetworkDevice ● 3: StorageDevice ● 4: PhysicalHost ● 5: VM ● 6: ManagementSystem ● 7: LogicalLocation ● 8: PhysicalLocation ● 9: Component ● 10: NFVResPool ● 11: SystemService	Integer	Yes. See the enumerated value.
Device Type	iMAPNorthboundAlarmNEType	Device type.	Octet string	No
ID of a device	iMAPNorthboundAlarmNEDevID	ID of a device, which uniquely identifies a device.	Octet string	No
Device SN	iMAPNorthboundAlarmDevCsn	Device SN of an alarm, which is unique for the same type of NE.	Octet string	No
Alarm ID	iMAPNorthboundAlarmID	ID of an alarm, which is used to identify alarm types for the same type of device. You are advised to use **iMAPNorthboundAlarmExtendProductItem6** (alarm ID of the string type) field as the alarm ID.	Integer	No

Name	Name in the MIB	Description	Value	Parsing Supported
Alarm Type	iMAPNorthboundAlarmType	Type of an alarm, which can be set to: • 1: Communication alarm • 2: Equipment alarm • 3: Processing error alarm • 4: Quality of service alarm • 5: Environmental alarm • 6: Integrity alarm • 7: Operation alarm • 8: Physical resource alarm • 9: Security alarm • 10: Time domain alarm • 11: Property change • 12: Object creation • 13: Object delete • 14: Relationship change • 15: State change • 16: Route change • 17: Protection switching • 18: Over limit • 19: File transfer status • 20: Backup status • 21: Heart beat	Integer	Yes. See the enumerated value.
Alarm Severity	iMAPNorthboundAlarmLevel	Severity of an alarm, which can be set to: • 1: Critical • 2: Major • 3: Minor • 4: Warning • 5: Indeterminate • 6: Cleared	Integer	Yes. See the enumerated value.

Name	Name in the MIB	Description	Value	Parsing Supported
Alarm Clearance Status	iMAPNorthboundAlarmRestore	Clearance identifier, which can be set to: ● 1: Cleared ● 2: Uncleared	Integer	Yes. See the enumerated value.
Alarm Acknowledgement Status	iMAPNorthboundAlarmConfirm	Acknowledgement identifier, which can be set to: ● 1: Acknowledged ● 2: Unacknowledged	Integer	Yes. See the enumerated value.
Alarm Acknowledgement Time	iMAPNorthboundAlarmAckTime	Time when an alarm is acknowledged.	Octet string	No
Alarm Clearance Time	iMAPNorthboundAlarmRestoreTime	Time when an alarm is cleared.	Octet string	No
Alarm Acknowledgement Operator	iMAPNorthboundAlarmOperator	Operator who acknowledges an alarm.	Octet string	No
Location Information	iMAPNorthboundAlarmExtendInfo	Extended information, which contains the location information about an alarm.	Integer	No
Alarm Cause	iMAPNorthboundAlarmProbablecause	Cause of an alarm.	Octet string	No
Alarm troubleshooting suggestions.	iMAPNorthboundAlarmProposedrepairactions	Suggestion for handling an alarm.	Octet string	No
Alarm Detail Cause	iMAPNorthboundAlarmSpecificproblems	Detailed cause of an alarm.	Octet string	No
NE IP	iMAPNorthboundAlarmExtendProductItem1	IP address of an NE.	Octet string	No

Name	Name in the MIB	Description	Value	Parsing Supported
Root Alarm	iMAPNorthboundAlarmExtendProductItem2	Whether the alarm is a root alarm. The options are as follows: ● **0**: non-root alarm ● **1**: root alarm	Octet string	No
Associated Alarm Group	iMAPNorthboundAlarmExtendProductItem3	Information about an associated alarm group.	Octet string	No
Alarm Arrival Time	iMAPNorthboundAlarmExtendProductItem4	Time when an alarm arrives at the NMS.	Octet string	No
Name of the service affected by the alarm	iMAPNorthboundAlarmExtendProductItem5	Name of the service affected by the alarm.	Octet string	No
Alarm ID (character string type)	iMAPNorthboundAlarmExtendProductItem6	Alarm ID (character string type). It is recommended that this field be used as the alarm ID during the interconnection.	Octet string	No
Alarm Name	iMAPNorthboundAlarmExtendProductItem7	Alarm name.	Octet string	No
Result of the Alarm RCA	iMAPNorthboundAlarmExtendProductItem8	Result of the alarm RCA.	Octet string	No
Alarm Clearance Operator	iMAPNorthboundAlarmClearOperator	Operator who clears an alarm.	Octet string	Yes. See the enumerated value.
Object Instance	iMAPNorthboundAlarmObjectInstanceType	Type of an alarm object instance. This field is not in use, and the value **0** is always reported.	Octet string	No

Name	Name in the MIB	Description	Value	Parsing Supported
Alarm Clearance Category	iMAPNorthboundAlarmClearCategory	Alarm clearance category, which can be set to: • 1: Alarms that can be cleared automatically. • 2: Alarms that cannot be cleared automatically.	Octet string	Yes. See the enumerated value.
Alarm clearance type	iMAPNorthboundAlarmClearType	Alarm clearance type, which can be set to: • 0: Uncleared • 1: Normal Clear • 2: Restore Clear • 3: Manual Clear • 4: Configure Clear • 5: Co-relation Clear • 6: System Clear • 7: Synchronization Clear	Octet string	Yes. See the enumerated value.
ServiceAffectFlag	iMAPNorthboundAlarmServiceAf-fectFlag	Whether a service is affected. • 1: Yes • 2: No	Octet string	Yes. See the enumerated value.
Alarm AdditionalInfo	iMAPNorthboundAlarmAddionalInfo	Additional information.	Octet string	No

13.3 MIB2 Trap

The SNMP NBI supports the following traps when MIB2 is loaded.

13.3.1 Alarm Notification Trap

The active alarm notification trap (**iMAPNorthboundFaultAlarmReportNotificationType**) is reported when new alarms are generated or alarm information changes on NCE.

Function

When alarms are generated on NEs or NCE, the SNMP NBI automatically sends this type of traps to inform the OSS of real-time alarms.

Trigger Condition

When alarms are generated on NEs or NCE, alarm notification traps are triggered.

Definition

Name	ENTERPRISE	Type	Description
iMAPNorthbound FaultAlarmReport NotificationType	iMAPNorthbound FaultAlarmNotifi-cation	Trap/Inform	Real-time alarms are reported.

Trap Content

Alarm traps consist of the following:

- Device information
- Alarm information
- Basic alarm attributes
- Additional information
- Reserved fields

Device Information

The device information contains the following fields:

- **iMAPNorthboundAlarmProductID**: ID of the product managing the device where an alarm is generated.
- **iMAPNorthboundAlarmNEType**: device type.
- **iMAPNorthboundAlarmNEDevID**: ID of the device where an alarm is generated. On NCE, device IDs are unique.
- **iMAPNorthboundAlarmMOName**: name of the device where an alarm is generated.

Alarm Information

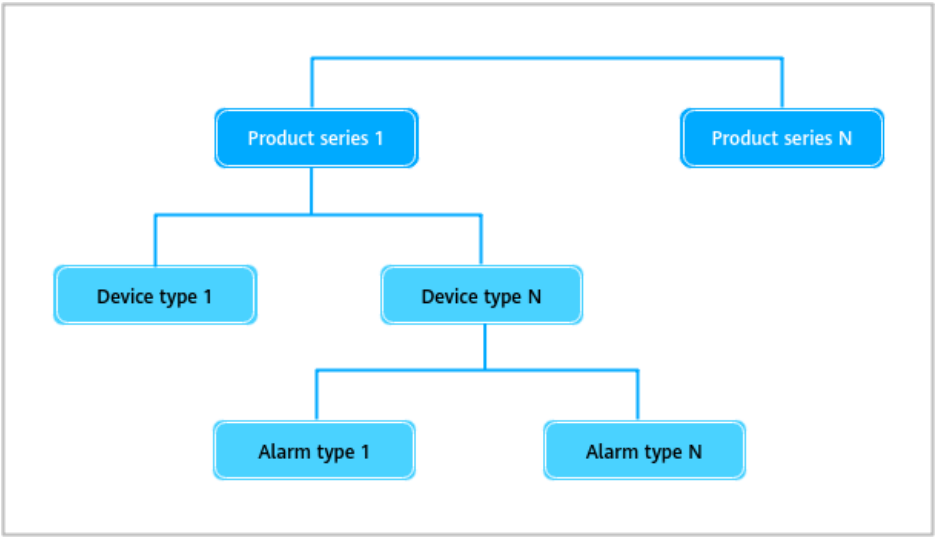
The alarm information contains the **iMAPNorthboundAlarmID** field, which is described as follows:

iMAPNorthboundAlarmID: alarm ID. You can define multiple alarm categories for a device type. After you define alarm categories for a device type, the device type can only report alarms of the predefined alarm categories. **Figure 13-1** shows the mapping between device types and alarm categories. Each alarm category is uniquely identified by the following fields: product ID, device type, and alarm ID. Using the three fields, the OSS determines the alarm category to which a received alarm belongs.

NOTE

- This alarm ID is an integer.
- You are advised to use **iMAPNorthboundAlarmExtendProductItem6** (alarm ID of the string type) field as the alarm ID.

Figure 13-1 Mapping between device types and alarm categories



Basic Alarm Attributes

The basic alarm attributes contain the following fields:

- **iMAPNorthboundAlarmType**: alarm type. The options are as follows:
  - 1: Communication alarm
  - 2: Equipment alarm
  - 3: Processing error alarm
  - 4: Quality of service alarm
  - 5: Environmental alarm
  - 6: Integrity alarm
  - 7: Operation alarm
  - 8: Physical resource alarm
  - 9: Security alarm
  - 10: Time domain alarm
  - 11: Property change
  - 12: Object creation
  - 13: Object delete
  - 14: Relationship change
  - 15: State change
  - 16: Route change
  - 17: Protection switching
  - 18: Over limit

  - 19: File transfer status
  - 20: Backup status
  - 21: Heart beat
- **iMAPNorthboundAlarmLevel**: alarm severity. The options are as follows:
  - 1: Critical
  - 2: Major
  - 3: Minor
  - 4: Warning
  - 5: Indeterminate
  - 6: Cleared
- **iMAPNorthboundAlarmOccurTime**: alarm occurrence time on devices.
- **iMAPNorthboundAlarmDevCsn**: device alarm SN. This field identifies the SN of an alarm generated on a device. The alarm SN is unique on the device.
- **iMAPNorthboundAlarmCSN**: network alarm SN.
- **iMAPNorthboundAlarmCategory**: alarm category. The options are as follows:
  - 1: Fault
  - 2: Clear
  - 3: Event
  - 4: Acknowledge
  - 5: Unacknowledge
  - 9: Change
- **iMAPNorthboundAlarmConfirm**: acknowledgment identifier. This field can be set to:
  - 1: Acknowledged
  - 2: Unacknowledged
- **iMAPNorthboundAlarmAckTime**: alarm acknowledgment time.
- **iMAPNorthboundAlarmRestore**: alarm clearance status.
  - 1: Cleared
  - 2: Uncleared
- **iMAPNorthboundAlarmRestoreTime**: alarm clearance time.
- **iMAPNorthboundAlarmOperator**: operator who acknowledges an alarm.
- **iMAPNorthboundAlarmClearOperator**: operator who clears an alarm.
- **iMAPNorthboundAlarmExtendProductItem1**: NE IP address.
- **iMAPNorthboundAlarmExtendProductItem2**: root alarm.
- **iMAPNorthboundAlarmExtendProductItem3**: information about an associated alarm group.
- **iMAPNorthboundAlarmExtendProductItem4**: time when the alarm arrives at NCE.
- **iMAPNorthboundAlarmExtendProductItem5**: name of the service affected by the alarm.

NOTE

- **iMAPNorthboundAlarmExtendProductItem5** uses the name-value pair format. The names are separated by commas (,) and spaces, for example, vpn=vpn1, tenant=tenant1.
- When the value of this field is not empty, do not forcibly bind the parameter location and the number of parameters (the parameter names may be the same but have different values) when parsing **iMAPNorthboundAlarmExtendProductItem5**. Instead, you are advised to parse the field based on the parameter name. When parsing the parameter name, do not distinguish the uppercase and lowercase letters in the parameter name.
- In the CloudVPN scenario, this field of some alarms also includes service information, such as VPN, private line, Internet access, remote access, and tenant name.

- **iMAPNorthboundAlarmExtendProductItem6**: alarm ID (character string type).

NOTE

- This field is an alarm ID of the character string type. It is used to identify a type of alarms on an interconnected system or device.
- It is recommended that the OSS supports the alarm ID of the character string type when the alarm ID field is modeled. In addition, the NMS should preferentially obtain the alarm ID from the current field of the northbound alarm SNMP interface.

- **iMAPNorthboundAlarmExtendProductItem7**: alarm name.
- **iMAPNorthboundAlarmExtendProductItem8**: result of the alarm RCA.

NOTE

- RCA: The alarm root cause analysis service enables you to quickly locate root alarms from a large number of alarms based on the correlation between cross-domain alarms and resources.
- The alarm RCA result uses the name-value pair format. The names are separated by commas (,) and spaces, for example, RCARuleName=XXXX, RCAGroupId=YYYY, RCAResult=ZZZZ.
- RCARuleName corresponds to the rule name in the RCA result.
- RCAGroupId: RCA group ID, which is used by the upper-layer system to assemble the RCA result. If the RCAGroupID is the same, the analysis results come from the same group.
- RCAResult: RCA result. The value **0** indicates that the analysis is not performed. The value **1** indicates that the analysis result is P in the same group. The value **2** indicates that the analysis result in the same group is C.
- The RCA requires some time. When a new alarm is reported, the value of the **iMAPNorthboundAlarmExtendProductItem8** field is empty. After the RCA is complete, the NBI reports a change alarm. The change alarm contains the RCA result.
- If an alarm does not contain the RCA information, the value of the **iMAPNorthboundAlarmExtendProductItem8** field is empty.

Additional Information

The additional information contains the following fields:

- **iMAPNorthboundAlarmExtendInfo**: extended information. This field contains the location information about an alarm.
- **iMAPNorthboundAlarmProbablecause**: cause of an alarm.
- **iMAPNorthboundAlarmProposedrepairactions**: alarm handling suggestion. This field provides the suggestion for handling an alarm.

- **iMAPNorthboundAlarmSpecificProblems**: detailed alarm cause.
- **iMAPNorthboundAlarmObjectInstanceType**: type of an alarm object instance.
- **iMAPNorthboundAlarmClearCategory**: alarm clearance category.
- **iMAPNorthboundAlarmClearType**: alarm clearance type.
- **iMAPNorthboundAlarmServiceAffectFlag**: identifies whether a service is affected.
- **iMAPNorthboundAlarmAddionalInfo**: additional alarm information.

VB List

In the following table, listed data types are for SNMPv1. The data types complying with SNMPv2c and SNMPv3 are not described if they are the same as those complying with SNMPv1. For any differences, details will be described in brackets.

NOTE

- The definitions of alarm fields in alarm synchronization result traps are the same as those in alarm notification traps. The only difference is that the former is NCE's response to the query of valid alarms, whereas the latter is actively reported by NCE.

Name in the MIB	OID	Type	Description
iMAPNorthboundAlarmCSN	1.3.6.1.4.1.2011.2.15.2.4.3.3.1	Octet string	Network SN of an alarm, which uniquely identifies an alarm.
iMAPNorthboundAlarmCategory	1.3.6.1.4.1.2011.2.15.2.4.3.3.2	Octet string	Alarm category. The options are as follows: • 1: Fault • 2: Clear • 4: Acknowledge • 5: Unacknowledge • 9: Change
iMAPNorthboundAlarmOccurTime	1.3.6.1.4.1.2011.2.15.2.4.3.3.3	Octet string	Time when an alarm is generated.
iMAPNorthboundAlarmMOName	1.3.6.1.4.1.2011.2.15.2.4.3.3.4	Octet string	Name of a device.

Name in the MIB	OID	Type	Description
iMAPNorthboundAlarmProductID	1.3.6.1.4.1.2011.2.15.2.4.3.3.5	Integer	ID of the product series. The options are as follows: • 0: Unknown • 1: PhysicalServer • 2: NetworkDevice • 3: StorageDevice • 4: PhysicalHost • 5: VM • 6: ManagementSystem • 7: LogicalLocation • 8: PhysicalLocation • 9: Component • 10: NFVResPool • 11: SystemService
iMAPNorthboundAlarmNEType	1.3.6.1.4.1.2011.2.15.2.4.3.3.6	Octet string	Name of a device type.
iMAPNorthboundAlarmNEDevID	1.3.6.1.4.1.2011.2.15.2.4.3.3.7	Octet string	ID of a device, which uniquely identifies a device.
iMAPNorthboundAlarmDevCsn	1.3.6.1.4.1.2011.2.15.2.4.3.3.8	Octet string	Device SN of an alarm, which is unique for the same type of NE.
iMAPNorthboundAlarmID	1.3.6.1.4.1.2011.2.15.2.4.3.3.9	Integer	ID of an alarm, which is used to identify alarm types for the same type of device. You are advised to use **iMAPNorthboundAlarmExtendProductItem6** (alarm ID of the string type) field as the alarm ID.

Name in the MIB	OID	Type	Description
iMAPNorthboundAlarmType	1.3.6.1.4.1.2011.2.15.2.4.3.3.10	Integer	Alarm type. The options are as follows: • 1: Communication alarm • 2: Equipment alarm • 3: Processing error alarm • 4: Quality of service alarm • 5: Environmental alarm • 6: Integrity alarm • 7: Operation alarm • 8: Physical resource alarm • 9: Security alarm • 10: Time domain alarm • 11: Property change • 12: Object creation • 13: Object delete • 14: Relationship change • 15: State change • 16: Route change • 17: Protection switching • 18: Over limit • 19: File transfer status • 20: Backup status • 21: Heart beat
iMAPNorthboundAlarmLevel	1.3.6.1.4.1.2011.2.15.2.4.3.3.11	Integer	Alarm severity. The options are as follows: • 1: Critical • 2: Major • 3: Minor • 4: Warning • 5: Indeterminate • 6: Cleared
iMAPNorthboundAlarmRestore	1.3.6.1.4.1.2011.2.15.2.4.3.3.12	Integer	Alarm clearance status. The options are as follows: • 1: Cleared • 2: Uncleared

Name in the MIB	OID	Type	Description
iMAPNorthboundAlarmConfirm	1.3.6.1.4.1.2011.2.15.2.4.3.3.13	Integer	Alarm acknowledgment status. The options are as follows: • 1: Acknowledged • 2: Unacknowledged
iMAPNorthboundAlarmAckTime	1.3.6.1.4.1.2011.2.15.2.4.3.3.14	Octet string	Time when an alarm is acknowledged.
iMAPNorthboundAlarmRestoreTime	1.3.6.1.4.1.2011.2.15.2.4.3.3.15	Octet string	Time when an alarm is cleared.
iMAPNorthboundAlarmOperator	1.3.6.1.4.1.2011.2.15.2.4.3.3.16	Octet string	Operator who acknowledges an alarm.
iMAPNorthboundAlarmExtendInfo	1.3.6.1.4.1.2011.2.15.2.4.3.3.27	Integer	Extended information, which contains the location information about an alarm.
iMAPNorthboundAlarmProbablecause	1.3.6.1.4.1.2011.2.15.2.4.3.3.28	Octet string	Cause of an alarm.
iMAPNorthboundAlarmProposedrepairactions	1.3.6.1.4.1.2011.2.15.2.4.3.3.29	Octet string	Suggestion for handling an alarm.
iMAPNorthboundAlarmSpecificproblems	1.3.6.1.4.1.2011.2.15.2.4.3.3.30	Octet string	Detailed cause of an alarm.
iMAPNorthboundAlarmExtendProductItem1	1.3.6.1.4.1.2011.2.15.2.4.3.3.31	Octet string	IP address of an NE.
iMAPNorthboundAlarmExtendProductItem2	1.3.6.1.4.1.2011.2.15.2.4.3.3.32	Octet string	Whether the alarm is a root alarm. The options are as follows: • **0**: non-root alarm • **1**: root alarm
iMAPNorthboundAlarmExtendProductItem3	1.3.6.1.4.1.2011.2.15.2.4.3.3.33	Octet string	Information about an associated alarm group.
iMAPNorthboundAlarmExtendProductItem4	1.3.6.1.4.1.2011.2.15.2.4.3.3.34	Octet string	Time when an alarm arrives at the NMS.

Name in the MIB	OID	Type	Description
iMAPNorthboundAlarmExtendProductItem5	1.3.6.1.4.1.2011.2.15.2.4.3.3.35	Octet string	Name of the service affected by the alarm.
iMAPNorthboundAlarmExtendProductItem6	1.3.6.1.4.1.2011.2.15.2.4.3.3.36	Octet string	Alarm ID (character string type). It is recommended that this field be preferentially used as the alarm ID during the interconnection.
iMAPNorthboundAlarmExtendProductItem7	1.3.6.1.4.1.2011.2.15.2.4.3.3.37	Octet string	Alarm name.
iMAPNorthboundAlarmExtendProductItem8	1.3.6.1.4.1.2011.2.15.2.4.3.3.38	Octet string	Result of the alarm RCA.
iMAPNorthboundAlarmClearOperator	1.3.6.1.4.1.2011.2.15.2.4.3.3.46	Octet string	Operator who clears an alarm.
iMAPNorthboundAlarmObjectInstanceType	1.3.6.1.4.1.2011.2.15.2.4.3.3.47	Octet string	Type of an alarm object instance. This field is not in use, and the value **0** is always reported.
iMAPNorthboundAlarmClearCategory	1.3.6.1.4.1.2011.2.15.2.4.3.3.48	Octet string	Alarm clearance category, which can be set to: • 1: Alarms that can be cleared automatically. • 2: Alarms that cannot be cleared automatically.
iMAPNorthboundAlarmClearType	1.3.6.1.4.1.2011.2.15.2.4.3.3.49	Octet string	Alarm clearance type, which can be set to: • 0: Uncleared • 1: Normal Clear • 2: Restore Clear • 3: Manual Clear • 4: Configure Clear • 5: Co-relation Clear • 6: System Clear • 7: Synchronization Clear
iMAPNorthboundAlarmServiceAffectFlag	1.3.6.1.4.1.2011.2.15.2.4.3.3.50	Octet string	Whether a service is affected. • 1: Yes • 2: No

Name in the MIB	OID	Type	Description
iMAPNorthboundAlarmAddionalInfo	1.3.6.1.4.1.2011.2.15.2.4.3.3.51	Octet string	Additional information.

13.3.2 Alarm Synchronization Start Trap

The alarm synchronization start trap (**iMAPNorthboundFaultAlarmQueryBeginNotificationType**) informs the OSS that alarm synchronization has started.

Function

After the OSS sends alarm query requests, the SNMP NBI returns this type of trap to the OSS to indicate that alarm synchronization has started.

Trigger Condition

The OSS triggers the alarm synchronization. For details, see **9.2.3 Synchronizing Alarms**.

The OSS sets **iMAPNorthboundAlarmQuery** to **1**.

Definition

Name	ENTERPRISE	Type	Description
iMAPNorthboundFaultAlarmQueryBeginNotificationType	iMAPNorthboundFaultAlarmNotification	Trap/Inform	Alarm synchronization start trap.

VB List

None

13.3.3 Alarm Synchronization Result Trap

The alarm synchronization result trap (**iMAPNorthboundFaultAlarmQueryNotificationType**) carries information about alarms on NCE.

Function

After the OSS initiates the alarm synchronization, the SNMP NBI sends this type of traps to report required alarms on NCE to the OSS.

Trigger Condition

The OSS triggers the alarm synchronization. For details, see **9.2.3 Synchronizing Alarms**.

The OSS sets **iMAPNorthboundAlarmQuery** to **1**.

Definition

Name	ENTERPRISE	Type	Description
iMAPNorthboundFaultAlarmQuery-NotificationType	iMAPNorthboundFaultAlarmNotification	Trap/Inform	Alarm synchronization result.

VB List

The fields are the same as those of the real-time alarm trap.

NOTE

- The definitions of alarm fields in alarm synchronization result traps are the same as those in alarm notification traps. The only difference is that the former is NCE's response to the query of valid alarms, whereas the latter is actively reported by NCE.

13.3.4 Alarm Synchronization End Trap

The alarm synchronization end trap (**iMAPNorthboundFaultAlarmQueryEndNotificationType**) informs the OSS that alarm synchronization has ended.

Function

NCE sends this type of traps to inform the OSS of the end of alarm synchronization.

Trigger Condition

Alarm synchronization end traps are triggered when:

- All required alarms on NCE have been reported to the OSS in trap packets.
- The OSS stops the synchronization.

The OSS triggers the termination of synchronization. For details, see **9.2.3 Synchronizing Alarms**.

The OSS sets **iMAPNorthboundAlarmQuery** to **0**.

Definition

Name	ENTERPRISE	Type	Description
iMAPNorthboundFaultAlarmQueryEndNotificationType	iMAPNorthboundFaultAlarmNotification	Trap/Inform	Alarm synchronization end trap.

VB List

None

13.3.5 KeepAlive Info (Heartbeat) Trap

The heartbeat notification trap (**iMAPNorthboundHeartbeatNotificationType**) informs the OSS that it is properly communicating with NCE.

Function

NCE sends the KeepAlive info (heartbeat) to the OSS regularly each period. If the OSS receives the trap, the connection between the OSS and NCE works. If the OSS does not receive the trap in this period and the heartbeat is disabled, the OSS disconnects with NCE.

Trigger Condition

NCE sends the KeepAlive info (heartbeat) trap to the OSS regularly in the preset period.

Definition

Name	ENTERPRISE	Type	Description
iMAPNorthboundHeartbeatNotificationType	iMAPNorthboundHeartbeatNotification	Trap/Inform	Notification for the Keep Alive traps.

VB List

In the following table, listed data types are for SNMPv1. The data types complying with SNMPv2c and SNMPv3 are not described if they are the same as those complying with SNMPv1. For any differences, details will be described in brackets.

Name	OID	Data Type	Description
iMAPNorthboundHeartbeatSystem-Label	1.3.6.1.4.1.2011.2.15.2.1.2.1.1.1.1	OCTET STRING	NCE system ID.
iMAPNorthboundHeartbeatPeriod	1.3.6.1.4.1.2011.2.15.2.1.2.1.1.1.2	INTEGER (Integer32)	Heartbeat period in seconds (it must be greater than or equal to 3, and the maximum value is 3600).
iMAPNorthboundHeartbeatTimeStamp	1.3.6.1.4.1.2011.2.15.2.1.2.1.1.1.3	OCTET STRING	Timestamp, the time when the heartbeat notification trap is generated.

13.4 MIB2 Trap Sample

MIB2 supports five types of traps: alarm notification trap, alarm synchronization start trap, alarm synchronization result trap, alarm synchronization end trap, and heartbeat trap. The samples in this section use SNMPv1 as an example. SNMPv2c and SNMPv3 are similar to SNMPv1.

13.4.1 Alarm Notification Trap

```
12: Specific trap
iMAPNorthboundFaultAlarmNotification::iMAPNorthboundFaultAlarmReportNotificationType #1 trap(v1)
received from: 10.185.156.226 at 2017/7/17 16:55:55    Time stamp: 0 days 00h:06m:42s.19th    Agent
address: 10.185.156.226 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap    Manager address:
10.190.200.188 Port: 55559 Transport: IP/UDP    Community: ******    SNMPv1 agent address:
10.185.156.226    Enterprise: iMAPNorthboundFaultAlarmNotification    Specific Trap MIB Lookup
Results    Name: iMAPNorthboundFaultAlarmReportNotificationType, Module: IMAP_NORTHBOUND_MIB-
V1, Enterprise: iMAPNorthboundFaultAlarmNotification    Bindings (26)    Binding #1:
iMAPNorthboundAlarmCSN.0 *** (octets) 3    Binding #2: iMAPNorthboundAlarmCategory.0 *** (octets)
1    Binding #3: iMAPNorthboundAlarmOccurTime.0 *** (octets) 2017-07-17 05:23:27    Binding #4:
iMAPNorthboundAlarmMOName.0 *** (octets) OSS    Binding #5: iMAPNorthboundAlarmProductID.0 ***
(int32) omc(6)    Binding #6: iMAPNorthboundAlarmNEType.0 *** (octets) 100000    Binding #7:
iMAPNorthboundAlarmNEDevID.0 *** (octets) OS=1    Binding #8: iMAPNorthboundAlarmDevCsn.0 ***
(octets) 0    Binding #9: iMAPNorthboundAlarmID.0 *** (int32) 40    Binding #10:
iMAPNorthboundAlarmType.0 *** (int32) processingError(10)    Binding #11: iMAPNorthboundAlarmLevel.
0 *** (int32) major(2)    Binding #12: iMAPNorthboundAlarmRestore.0 *** (int32) uncleared(2)    Binding
#13: iMAPNorthboundAlarmConfirm.0 *** (int32) unacknowledged(2)    Binding #14:
iMAPNorthboundAlarmAckTime.0 *** (octets) (zero-length)    Binding #15:
iMAPNorthboundAlarmRestoreTime.0 *** (octets) (zero-length)    Binding #16:
```


iMAPNorthboundAlarmOperator.0 *** (octets) (zero-length) Binding #17: iMAPNorthboundAlarmExtendInfo.0 *** (octets) Active Server=linux-bbfw Binding #18: iMAPNorthboundAlarmProbablecause.0 *** (octets) The ESN of the server does not match that in the license file Binding #19: iMAPNorthboundAlarmProposedrepairactions.0 *** (octets) Apply for another license or contact customer service personnel. Binding #20: iMAPNorthboundAlarmSpecificproblems.0 *** (octets) The ESN of the server does not match that in the license file. Binding #21: iMAPNorthboundAlarmClearOperator.0 *** (octets) (zero-length) Binding #22: iMAPNorthboundAlarmObjectInstanceType.0 *** (octets) 0 Binding #23: iMAPNorthboundAlarmClearCategory.0 *** (octets) 1 Binding #24: iMAPNorthboundAlarmClearType.0 *** (octets) 0 Binding #25: iMAPNorthboundAlarmServiceAffectFlag.0 *** (octets) 0 Binding #26: iMAPNorthboundAlarmAdditionalInfo.0 *** (octets) The ESN of the server does not match that in the license file.

13.4.2 Alarm Synchronization Start Trap

After the OSS sends alarm synchronization requests, the SNMP NBI returns the start notification of alarm synchronization.

18: Specific trap iMAPNorthboundFaultAlarmNotification::iMAPNorthboundFaultAlarmQueryBeginNotificationType #2 trap(v1) received from: 10.185.156.226 at 2017/7/17 17:00:24 Time stamp: 0 days 00h:11m:11s.02th Agent address: 10.185.156.226 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap Manager address: 10.190.200.188 Port: 55559 Transport: IP/UDP Community: ****** SNMPv1 agent address: 10.185.156.226 Enterprise: iMAPNorthboundFaultAlarmNotification Specific Trap MIB Lookup Results Name: iMAPNorthboundFaultAlarmQueryBeginNotificationType, Module: IMAP_NORTHBOUND_MIB-V1, Enterprise: iMAPNorthboundFaultAlarmNotification Bindings (0) None.

13.4.3 Alarm Synchronization Result Trap

After the OSS sends alarm synchronization requests, the SNMP NBI will report the alarms meeting filter criteria to the OSS.

20: Specific trap iMAPNorthboundFaultAlarmNotification::iMAPNorthboundFaultAlarmQueryNotificationType #3 trap(v1) received from: 10.185.156.226 at 2017/7/17 17:00:24 Time stamp: 0 days 00h:11m:11s.12th Agent address: 10.185.156.226 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap Manager address: 10.190.200.188 Port: 55559 Transport: IP/UDP Community: ****** SNMPv1 agent address: 10.185.156.226 Enterprise: iMAPNorthboundFaultAlarmNotification Specific Trap MIB Lookup Results Name: iMAPNorthboundFaultAlarmQueryNotificationType, Module: IMAP_NORTHBOUND_MIB-V1, Enterprise: iMAPNorthboundFaultAlarmNotification Bindings (26) Binding #1: iMAPNorthboundAlarmCSN.0 *** (octets) 2 Binding #2: iMAPNorthboundAlarmCategory.0 *** (octets) 1 Binding #3: iMAPNorthboundAlarmOccurTime.0 *** (octets) 2017-07-17 05:23:27 Binding #4: iMAPNorthboundAlarmMOName.0 *** (octets) OSS Binding #5: iMAPNorthboundAlarmProductID.0 *** (int32) omc(6) Binding #6: iMAPNorthboundAlarmNEType.0 *** (octets) 100000 Binding #7: iMAPNorthboundAlarmNEDevID.0 *** (octets) OS=1 Binding #8: iMAPNorthboundAlarmDevCsn.0 *** (octets) 0 Binding #9: iMAPNorthboundAlarmID.0 *** (int32) 297 Binding #10: iMAPNorthboundAlarmType.0 *** (int32) processingError(10) Binding #11: iMAPNorthboundAlarmLevel.0 *** (int32) critical(1) Binding #12: iMAPNorthboundAlarmRestore.0 *** (int32) uncleared(2) Binding #13: iMAPNorthboundAlarmConfirm.0 *** (int32) unacknowledged(2) Binding #14: iMAPNorthboundAlarmAckTime.0 *** (octets) (zero-length) Binding #15: iMAPNorthboundAlarmRestoreTime.0 *** (octets) (zero-length) Binding #16: iMAPNorthboundAlarmOperator.0 *** (octets) (zero-length) Binding #17: iMAPNorthboundAlarmExtendInfo.0 *** (octets) ProductName=iMAP Binding #18: iMAPNorthboundAlarmProbablecause.0 *** (octets) The OSS License Expired Binding #19: iMAPNorthboundAlarmProposedrepairactions.0 *** (octets) Contact Huawei technical support engineers to apply for a new OSS license. Binding #20: iMAPNorthboundAlarmSpecificproblems.0 *** (octets) This alarm is generated when the OSS license expires. Binding #21: iMAPNorthboundAlarmClearOperator.0 *** (octets) (zero-length) Binding #22: iMAPNorthboundAlarmObjectInstanceType.0 *** (octets) 0 Binding


```
#23: iMAPNorthboundAlarmClearCategory.0 *** (octets) 1       Binding #24:
iMAPNorthboundAlarmClearType.0 *** (octets) 0       Binding #25:
iMAPNorthboundAlarmServiceAffectFlag.0 *** (octets) 0       Binding #26:
iMAPNorthboundAlarmAdditionalInfo.0 *** (octets) This alarm is generated when the OSS
license expires.
```

13.4.4 Alarm Synchronization End Trap

Alarm synchronization end traps are triggered when all required alarms have been reported to the OSS or the OSS automatically stops the synchronization.

Synchronization Stopped After Alarm Reporting Was Complete

After all required alarms are reported to the OSS, SNMP NBI sends traps through the SNMP NBI to inform the OSS of the stop of alarm reporting.

```
1335: Specific trap
hwNmNorthboundEventSynchronizationEnd::hwNmNorthboundEventSynchronizationEndNotify
#11 trap(v1) received from: 10.71.88.151 at 2010-11-24 15:57:45
  Time stamp: 0 days 00h:07m:25s.16th
  Agent address: 10.71.88.151 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.70.73.96 Port: 8888 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.71.88.151
  Enterprise: hwNmNorthboundEventSynchronizationEnd
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventSynchronizationEndNotify, Module: HW-
IMAPV1NORTHBOUND-TRAP-MIB, Enterprise: hwNmNorthboundEventSynchronizationEnd
  Bindings (2)
    Binding #1: hwNmNorthboundEventSynchronizationEndStatus.0 *** (int32) normalEnd(1)
    Binding #2: hwNmNorthboundEventSynchronizationEndStatusDetail.0 *** (octets) Sync End:
Successfully queried all alarms!
```

Synchronization Was Stopped by the OSS

The OSS can also stop the synchronization as required. The SNMP NBI then reports traps to inform the OSS of the stop of alarm synchronization, as a response to the request.

```
2420: Specific trap
hwNmNorthboundEventSynchronizationEnd::hwNmNorthboundEventSynchronizationEndNotify
#11 trap(v1) received from: 10.71.88.151 at 2010-11-24 16:04:01
  Time stamp: 0 days 00h:13m:40s.35th
  Agent address: 10.71.88.151 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.70.73.96 Port: 8888 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.71.88.151
  Enterprise: hwNmNorthboundEventSynchronizationEnd
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventSynchronizationEndNotify, Module: HW-
IMAPV1NORTHBOUND-TRAP-MIB, Enterprise: hwNmNorthboundEventSynchronizationEnd
  Bindings (2)
    Binding #1: hwNmNorthboundEventSynchronizationEndStatus.0 *** (int32) stopped(2)
    Binding #2: hwNmNorthboundEventSynchronizationEndStatusDetail.0 *** (octets) Sync
Stopped: The synchronization is stopped by the NMS's command!
```


Synchronization Was Stopped Unexpectedly

```
403: Specific trap
hwNmNorthboundEventSynchronizationEnd::hwNmNorthboundEventSynchronizationEndNotify
#11 trap(v1) received from: 10.71.224.13 at 2011-4-27 16:44:56
  Time stamp: 0 days 00h:03m:31s.64th
  Agent address: 10.71.224.13 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.70.71.97 Port: 6666 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.71.224.13
  Enterprise: hwNmNorthboundEventSynchronizationEnd
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventSynchronizationEndNotify, Module: HW-
IMAPV1NORTHBOUND-TRAP-MIB, Enterprise: hwNmNorthboundEventSynchronizationEnd
  Bindings (2)
    Binding #1: hwNmNorthboundEventSynchronizationEndStatus.0 *** (int32) error(3)
    Binding #2: hwNmNorthboundEventSynchronizationEndStatusDetail.0 *** (octets) Sync Error:
Query failed as Agent shutting down!
```

13.4.5 Heartbeat Trap

The SNMP NBI sends heartbeat traps to the OSS periodically. Based on the heartbeats, the OSS determines whether the connection with the SNMP NBI is proper.

NOTE

Two OIDs are supported.

hwNmAgent (Default)

```
795: Specific trap hwNmNorthboundEventKeepAliveInfo::hwNmNorthboundEventKeepAlive #2
trap(v1) received from: 10.71.88.151 at 2010-11-24 15:57:20
  Time stamp: 0 days 00h:07m:00s.12th
  Agent address: 10.71.88.151 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.70.73.96 Port: 8888 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.71.88.151
  Enterprise: hwNmNorthboundEventKeepAliveInfo
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventKeepAlive, Module: HW-IMAPV1NORTHBOUND-TRAP-MIB,
Enterprise: hwNmNorthboundEventKeepAliveInfo
  Bindings (1)
    Binding #1: hwNmAgent *** (octets) SNMP Agent
```

hwNmNorthboundKeepAlive (Configurable-1.3.6.1.4.1.2011.2.15.1.7.2.1)

```
8: Specific trap hwNmNorthboundEventKeepAliveInfo::hwNmNorthboundEventKeepAlive #2
trap(v1) received from: 10.67.192.220 at 2012/6/26 11:19:13
  Time stamp: 0 days 00h:00m:15s.04th
  Agent address: 10.67.192.220 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.66.102.169 Port: 6666 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.67.192.220
  Enterprise: hwNmNorthboundEventKeepAliveInfo
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventKeepAlive, Module: HW-IMAPV1NORTHBOUND-TRAP-MIB,
Enterprise: hwNmNorthboundEventKeepAliveInfo
  Bindings (1)
    Binding #1: hwNmNorthboundKeepAlive *** (octets) SNMP Agent
```


hwNmNorthboundKeepAlive (Configurable-1.3.6.1.4.1.2011.2.15.1.7.2.1.0)

```
3: Specific trap hwNmNorthboundEventKeepAliveInfo::hwNmNorthboundEventKeepAlive #2
trap(v1) received from: 10.78.219.70 at 2012/7/26 19:11:29
  Time stamp: 0 days 00h:01m:45s.11th
  Agent address: 10.78.219.70 Port: 6666 Transport: IP/UDP Protocol: SNMPv1 Trap
  Manager address: 10.66.103.78 Port: 6666 Transport: IP/UDP
Community: ******
  SNMPv1 agent address: 10.78.219.70
  Enterprise: hwNmNorthboundEventKeepAliveInfo
  Specific Trap MIB Lookup Results
    Name: hwNmNorthboundEventKeepAlive, Module: HW-IMAPV1NORTHBOUND-TRAP-MIB,
Enterprise: hwNmNorthboundEventKeepAliveInfo
  Bindings (1)
    Binding #1: hwNmNorthboundKeepAlive.0 *** (octets) SNMP Agent
```


14 MIB3

The MIB3 (T2000-NETMANAGEMENT-MIB) is mainly used for managing transport devices or upgrading the T2000.

MIB3 supports four types of traps: alarm notification trap, alarm synchronization start trap, alarm synchronization result trap, and alarm synchronization end trap. The samples in this section use SNMPv1 as an example. SNMPv2c and SNMPv3 are similar to SNMPv1.

14.1 MIB Description

The complete T2000-NETMANAGEMENT-MIB node is:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).huawei(2011).products(2).netManagement(15).nmAgent(1)

The MIB tree is shown as follows:

```
--- huawei(2011)
        |--- products(2)
            |--- netManagement(15)
                |--- nmAgent(1)
                    |---- nmNorthboundEvent(7)
```

nmNorthboundEvent defines the SNMP NBI of NCE.

For details about the function interfaces of MIB, see **9.3 MIB3 Subinterfaces**.

For details about the structure and detailed parameters of MIB, see *iMaster NCE SNMP NBI MIB File*.

NOTE

iMaster NCE SNMP NBI MIB File is available on the Huawei technical support website. To obtain this document, contact the local technical support.

14.2 Alarm Fields Reported by MIB3

MIB3 supports 36 alarm fields, and you can customize them.

When the MIB frame is set to **MIB3**, the SNMP NBI reports the alarm fields in the following table.

Name	Name in the MIB	Description	Value
EMS Name	northboundReportAlarmEmsName	EMS name. The value is always Huawei/NCE.	Octet string
Device Type	northboundReportAlarmManagedObjectClass	NE type. Example: OptiX 2500+	Octet string
Device Name	northboundReportAlarmManagedObjectInstance	Device name. Example: NE350	Octet string
NE Name	northboundReportAlarmNEName	NE name, which is the same as the device name. Example: NE350	Octet string
Rack Name	northboundReportAlarmRackName	Cabinet name. The value is always **1**.	Octet string
Subrack Name	northboundReportAlarmShelfName	Subrack name. In the WDM or OTN domain, the NE name is the name of an optical NE and the subrack name is the name of the subrack that belongs to the optical NE. In the SDH or other domains, the NE name is the subrack name. Example: NE350	Octet string
Physical Device Location	northboundReportAlarmDevLocation	Physical location of the device. This parameter is always left blank.	Octet string
Board Name	northboundReportAlarmBoardName	Board name. Example: PQ1	Octet string

Name	Name in the MIB	Description	Value
Port Type	northboundReportAlarmPortType	Port type. Example: SDH_TU	Octet string
Port Number	northboundReportAlarmPortNumber	Port number. Example: 1	Integer
Location of an Alarm Object	northboundReportAlarmLocation	Specific location of an alarm. Example: ne=590174/rack=1/shelf=1/slot=5/domain=sdh/port=1/highPath=1/lowPath=0/layer=5 The rules for assembling alarm location information for a PTN NE may be slightly different, for example: ne=3145796/rack=1/shelf=1/slot=4/domain=ptn/type=physical/port=1/location1=260/layer=15	Octet string
Alarm Type	northboundReportAlarmEventType	Alarm type. The options are as follows: • communicationsAlarm • qualityofServiceAlarm • equipmentAlarm • processingErrorAlarm • environmentalAlarm	Octet string
Alarm Occurrence Time	northboundReportAlarmEventTime	Time when an alarm is generated. Example: 2005-10-14,17:41:04.0 The option is always the local time.	Octet string

Name	Name in the MIB	Description	Value
Alarm Severity	northboundReportAlarmPerceived-Severity	Alarm severity. The options are as follows: • Critical • Major • Minor • Warning • Cleared • Indeterminate	Octet string
Possible Alarm Cause	northboundReportAlarmProbableCause	Possible causes of the alarm. Example: RAI	Octet string
Alarm Cause	northboundReportAlarmSpecificProblems	Alarm cause. For example, NE communication was lost.	Octet string
Affect Service	northboundReportAlarmOperationAffected	Affect Service The options are as follows: 0: The alarm does not affect services. 1: The alarm affects services.	Integer
Alarm ID	northboundReportAlarmID	Alarm ID. Example: 93	Integer
Alarm Name	northboundReportAlarmName	Alarm name. Example: LP_RDI	Octet string
Alarm troubleshooting suggestions.	northboundReportAlarmProposedRepairActions	Alarm troubleshooting suggestions. This parameter is always left blank.	Octet string
IP Address of the Object for Alarm Rising	northboundReportAlarmIPAddress	IP address of the device where an alarm is generated. This parameter is always left blank.	IP address
Alarm SN	northboundReportAlarmNotificationIdentifier	SN of an alarm. Example: 109	Integer

Name	Name in the MIB	Description	Value
ID of the Resource for Alarm Rising	northboundReportAlarmResourceID	ID of the resource where an alarm is generated. This parameter is always left blank.	Integer
Additional Information	northboundReportAlarmAdditionalText	Additional information. Example: Alarm Parameter II(hex) 0x02	Octet string
Clearance Alarm	northboundReportAlarmCleared	Whether it is a clear alarm. The options are as follows: **0**: non-clear alarm **1**: clear alarm	Integer
SN of an Alarm to Be Cleared	northboundReportAlarmCorrelatedNotifications	SN of an alarm to be cleared. The value of this parameter is the same as that of the **SN of an Alarm** parameter.	Integer
Additional Alarm Information (10 Fields)	northboundReportAlarmAdditionalVB	Additional information of an alarm. This parameter is always left blank.	Octet string

14.3 MIB3 Trap

The SNMP NBI supports the following traps when MIB3 is loaded.

- Active alarm notification trap: **northBoundReportAlarm**
- Alarm synchronization result trap: **northBoundSynchAlarm**
- Alarm synchronization start trap: **northBoundSynchAlarmStart**
- Alarm synchronization end trap: **northBoundSynchAlarmEnd**

14.3.1 Alarm Notification Trap

Function

When alarms are generated on NEs or NCE, the SNMP NBI automatically sends this type of traps to inform the OSS of real-time alarms.

Trigger Condition

When alarms are generated on NEs or NCE, alarm notification traps are triggered.

Definition

Name	ENTERPRISE	Type	Description
northBoundReportAlarm	northboundNotificationType	Trap	Real-time alarms are reported.

VB List

In the following table, listed data types are for SNMPv1. The data types complying with SNMPv2c and SNMPv3 are not described if they are the same as those complying with SNMPv1. For any differences, details will be described in brackets.

NOTE

The definitions of alarm fields in alarm synchronization result traps are the same as those in alarm notification traps. The only difference is that the former is NCE's response to the query of valid alarms, whereas the latter is actively reported by NCE.

Name in the MIB	OID	Type	Description
northboundReportAlarmManagedObjectClass	1.3.6.1.4.1.2011.2.15.1.7.3.1	OCTET STRING	NE type. Example: OptiX 2500+
northboundReportAlarmManagedObjectInstance	1.3.6.1.4.1.2011.2.15.1.7.3.2	OCTET STRING	Device name. Example: NE350
northboundReportAlarmEventType	1.3.6.1.4.1.2011.2.15.1.7.3.3	OCTET STRING	Alarm type. The options are as follows: • communicationsAlarm • qualityofServiceAlarm • equipmentAlarm • processingErrorAlarm • environmentalAlarm
northboundReportAlarmEventTime	1.3.6.1.4.1.2011.2.15.1.7.3.4	OCTET STRING	Time when an alarm is generated. Example: 2005-10-14,17:41:04.0 The option is always the local time.
northboundReportAlarmProbableCause	1.3.6.1.4.1.2011.2.15.1.7.3.5	OCTET STRING	Possible causes of the alarm. Example: RAI.

Name in the MIB	OID	Type	Description
northboundReportAlarmSpecificProblems	1.3.6.1.4.1.2011.2.15.1.7.3.6	OCTET STRING	Alarm cause. For example, NE communication was lost.
northboundReportAlarmPerceivedSeverity	1.3.6.1.4.1.2011.2.15.1.7.3.7	OCTET STRING	Alarm severity. The options are as follows: ● Critical ● Major ● Minor ● Warning ● cleared ● indeterminate
northboundReportAlarmNotificationIdentifier	1.3.6.1.4.1.2011.2.15.1.7.3.8	INTEGER	SN of an alarm. Example: 109
northboundReportAlarmCorrelatedNotifications	1.3.6.1.4.1.2011.2.15.1.7.3.9	INTEGER	SN of an alarm to be cleared. The value of this parameter is the same as the alarm SN.
northboundReportAlarmProposedRepairActions	1.3.6.1.4.1.2011.2.15.1.7.3.10	OCTET STRING	Alarm troubleshooting suggestions. This parameter is always left blank.
northboundReportAlarmAdditionalText	1.3.6.1.4.1.2011.2.15.1.7.3.11	OCTET STRING	Additional information. Example: Alarm Parameter II(hex) 0x02
northboundReportAlarmEmsName	1.3.6.1.4.1.2011.2.15.1.7.3.12	OCTET STRING	EMS name. The value is always **Huawei/NCE**.
northboundReportAlarmNEName	1.3.6.1.4.1.2011.2.15.1.7.3.13	OCTET STRING	NE name, which is the same as the device name. Example: NE350
northboundReportAlarmDevLocation	1.3.6.1.4.1.2011.2.15.1.7.3.14	OCTET STRING	Physical location of the device. This parameter is always left blank.

Name in the MIB	OID	Type	Description
northboundReportAlarmRackName	1.3.6.1.4.1.2011.2.15.1.7.3.15	OCTET STRING	Cabinet name. The value is always **1**.
northboundReportAlarmShelfName	1.3.6.1.4.1.2011.2.15.1.7.3.16	OCTET STRING	Subrack name. In the WDM or OTN domain, the NE name is the name of an optical NE and the subrack name is the name of the subrack that belongs to the optical NE. In the SDH or other domains, the NE name is the subrack name. Example: NE350
northboundReportAlarmBoardName	1.3.6.1.4.1.2011.2.15.1.7.3.17	OCTET STRING	Board name. Example: PQ1
northboundReportAlarmPortType	1.3.6.1.4.1.2011.2.15.1.7.3.18	OCTET STRING	Port type. Example: SDH_TU
northboundReportAlarmPortNumber	1.3.6.1.4.1.2011.2.15.1.7.3.19	INTEGER	Port number. Example: 1
northboundReportAlarmLocation	1.3.6.1.4.1.2011.2.15.1.7.3.20	OCTET STRING	Specific location of an alarm. Example: ne=590174/rack=1/shelf=1/slot=5/domain=sdh/port=1/highPath=1/lowPath=0/layer=5. The rules for assembling alarm location information for a PTN NE may be slightly different. ne=3145796/rack=1/shelf=1/slot=4/domain=ptn/type=physical/port=1/location1=260/layer=15
northboundReportAlarmOperationAffected	1.3.6.1.4.1.2011.2.15.1.7.3.21	OCTET STRING	Whether an alarm affects services. The options are as follows: 0: The alarm does not affect services. 1: The alarm affects services.

Name in the MIB	OID	Type	Description
northboundReportAlarmID	1.3.6.1.4.1.2011.2.15.1.7.3.22	INTEGER	Alarm ID. Example: 93
northboundReportAlarmName	1.3.6.1.4.1.2011.2.15.1.7.3.23	OCTET STRING	Alarm name. Example: LP_RDI
northboundReportAlarmIPAddress	1.3.6.1.4.1.2011.2.15.1.7.3.24	IpAddress	IP address of the device where an alarm is generated. This parameter is always left blank.
northboundReportAlarmResourceID	1.3.6.1.4.1.2011.2.15.1.7.3.25	INTEGER	ID of the resource where an alarm is generated. This parameter is always left blank.
northboundReportAlarmCleared	1.3.6.1.4.1.2011.2.15.1.7.3.26	INTEGER	Whether it is a clear alarm. The options are as follows: **0**: non-clear alarm **1**: clear alarm
northboundReportAlarmAdditionalVB1-VB10	1.3.6.1.4.1.2011.2.15.1.7.3.27	OCTET STRING	Additional alarm information (10 fields). northboundReportAlarmAdditionalVB1 indicates the alarm UUID of the physical resources (NEs, cards, and ports) in the IP domain. northboundReportAlarmAdditionalVB2-VB10 are always left blank.

14.3.2 Alarm Synchronization Start Trap

Function

After the OSS sends alarm query requests, the SNMP NBI returns this type of trap to the OSS to indicate that alarm synchronization has started.

Trigger Condition

The OSS triggers the alarm synchronization. For details, see **9.3.2 Synchronizing Alarms**.

The OSS sets **northBoundSynchAlarmCommand** to **1**.

NOTE

- 1: starts the alarm synchronization.
- 0: ends the alarm synchronization.

Definition

Name	ENTERPRISE	Type	Description
northBoundSynchAlarmStart	northboundNotificationType	Trap	Alarm synchronization start trap.

VB List

None

14.3.3 Alarm Synchronization Result Trap

Function

After the OSS initiates the alarm synchronization, the SNMP NBI sends this type of traps to report required alarms on NCE to the OSS.

Trigger Condition

The OSS triggers the alarm synchronization. For details, see **9.3.2 Synchronizing Alarms**.

The OSS sets **northBoundSynchAlarmCommand** to **1**.

NOTE

- 1: starts the alarm synchronization.
- 0: ends the alarm synchronization.

Definition

1. Definition of the alarm synchronization result trap

Name	ENTERPRISE	Type	Description
northBoundSynchAlarm	northboundNotificationType	Trap/Inform	Alarm synchronization start trap.

VB List

In the following table, listed data types are for SNMPv1. The data types complying with SNMPv2c and SNMPv3 are not described if they are the same as those complying with SNMPv1. For any differences, details will be described in brackets.

NOTE

The definitions of alarm fields in alarm synchronization result traps are the same as those in alarm notification traps. The only difference is that the former is NCE's response to the query of valid alarms, whereas the latter is actively reported by NCE.

Name in the MIB	OID	Type	Description
northboundReportAlarmManagedObjectClass	1.3.6.1.4.1.2011.2.15.1.7.3.1	OCTET STRING	NE type. Example: OptiX 2500+
northboundReportAlarmManagedObjectInstance	1.3.6.1.4.1.2011.2.15.1.7.3.2	OCTET STRING	Device name. Example: NE350
northboundReportAlarmEventType	1.3.6.1.4.1.2011.2.15.1.7.3.3	OCTET STRING	Alarm type. The options are as follows: ● communicationsAlarm ● qualityofServiceAlarm ● equipmentAlarm ● processingErrorAlarm ● environmentalAlarm
northboundReportAlarmEventTime	1.3.6.1.4.1.2011.2.15.1.7.3.4	OCTET STRING	Time when an alarm is generated. Example: 2005-10-14,17:41:04.0 The option is always the local time.
northboundReportAlarmProbableCause	1.3.6.1.4.1.2011.2.15.1.7.3.5	OCTET STRING	Possible causes of the alarm. Example: RAI
northboundReportAlarmSpecificProblems	1.3.6.1.4.1.2011.2.15.1.7.3.6	OCTET STRING	Alarm cause. For example, NE communication was lost.

Name in the MIB	OID	Type	Description
northboundReportAlarmPerceivedSeverity	1.3.6.1.4.1.2011.2.15.1.7.3.7	OCTET STRING	Alarm severity. The options are as follows: • Critical • Major • Minor • Warning • cleared • indeterminate
northboundReportAlarmNotificationIdentifier	1.3.6.1.4.1.2011.2.15.1.7.3.8	INTEGER	SN of an alarm. Example: 109
northboundReportAlarmCorrelatedNotifications	1.3.6.1.4.1.2011.2.15.1.7.3.9	INTEGER	SN of an alarm to be cleared. The value of this parameter is the same as the alarm SN.
northboundReportAlarmProposedRepairActions	1.3.6.1.4.1.2011.2.15.1.7.3.10	OCTET STRING	Alarm troubleshooting suggestions. This parameter is always left blank.
northboundReportAlarmAdditionalText	1.3.6.1.4.1.2011.2.15.1.7.3.11	OCTET STRING	Additional information. Example: Alarm Parameter II(hex) 0x02
northboundReportAlarmEmsName	1.3.6.1.4.1.2011.2.15.1.7.3.12	OCTET STRING	EMS name. The value is always **Huawei/NCE**.
northboundReportAlarmNEName	1.3.6.1.4.1.2011.2.15.1.7.3.13	OCTET STRING	NE name, which is the same as the device name. Example: NE350
northboundReportAlarmDevLocation	1.3.6.1.4.1.2011.2.15.1.7.3.14	OCTET STRING	Physical location of the device. This parameter is always left blank.
northboundReportAlarmRackName	1.3.6.1.4.1.2011.2.15.1.7.3.15	OCTET STRING	Cabinet name. The value is always **1**.

Name in the MIB	OID	Type	Description
northboundReportAlarmShelfName	1.3.6.1.4.1.2011.2.15.1.7.3.16	OCTET STRING	Subrack name. In the WDM or OTN domain, the NE name is the name of an optical NE and the subrack name is the name of the subrack that belongs to the optical NE. In the SDH or other domains, the NE name is the subrack name. Example: NE350
northboundReportAlarmBoardName	1.3.6.1.4.1.2011.2.15.1.7.3.17	OCTET STRING	Board name. Example: PQ1
northboundReportAlarmPortType	1.3.6.1.4.1.2011.2.15.1.7.3.18	OCTET STRING	Port type. Example: SDH_TU
northboundReportAlarmPortNumber	1.3.6.1.4.1.2011.2.15.1.7.3.19	INTEGER	Port number. Example: 1
northboundReportAlarmLocation	1.3.6.1.4.1.2011.2.15.1.7.3.20	OCTET STRING	Specific location of an alarm. Example: ne=590174/rack=1/shelf=1/slot=5/domain=sdh/port=1/highPath=1/lowPath=0/layer=5. The rules for assembling alarm location information for a PTN NE may be slightly different. ne=3145796/rack=1/shelf=1/slot=4/domain=ptn/type=physical/port=1/location1=260/layer=15
northboundReportAlarmOperationAffected	1.3.6.1.4.1.2011.2.15.1.7.3.21	OCTET STRING	Whether an alarm affects services. The options are as follows: 0: The alarm does not affect services. 1: The alarm affects services.
northboundReportAlarmID	1.3.6.1.4.1.2011.2.15.1.7.3.22	INTEGER	Alarm ID. Example: 93

Name in the MIB	OID	Type	Description
northboundReportAlarmName	1.3.6.1.4.1.2011.2.15.1.7.3.23	OCTET STRING	Alarm name. Example: LP_RDI
northboundReportAlarmIPAddress	1.3.6.1.4.1.2011.2.15.1.7.3.24	IpAddress	IP address of the device where an alarm is generated. This parameter is always left blank.
northboundReportAlarmResourceID	1.3.6.1.4.1.2011.2.15.1.7.3.25	INTEGER	ID of the resource where an alarm is generated. This parameter is always left blank.
northboundReportAlarmCleared	1.3.6.1.4.1.2011.2.15.1.7.3.26	INTEGER	Whether it is a clear alarm. The options are as follows: **0**: non-clear alarm **1**: clear alarm
northboundReportAlarmAdditionalVB1-VB10	1.3.6.1.4.1.2011.2.15.1.7.3.27	OCTET STRING	Additional alarm information (10 fields). northboundReportAlarmAdditionalVB1 indicates the alarm UUID of the physical resources (NEs, cards, and ports) in the IP domain. northboundReportAlarmAdditionalVB2-VB10 are always left blank.

14.3.4 Alarm Synchronization End Trap

Function

NCE sends this type of traps to inform the OSS of the end of alarm synchronization.

Trigger Condition

Alarm synchronization end traps are triggered when:

- All required alarms on NCE have been reported to the OSS in trap packets.
- The OSS stops the synchronization.

The OSS triggers the termination of synchronization. For details, see **9.3.2 Synchronizing Alarms**.

The OSS sets **northBoundSynchAlarmCommand** to **0**.

NOTE

- 1: starts the alarm synchronization.
- 0: ends the alarm synchronization.

Definition

Table 14-1 Definition of the alarm synchronization end trap

Name	ENTERPRISE	Type	Description
northBoundSynchAlarmEnd	northboundNotificationType	Trap/Inform	Alarm synchronization end trap.

VB List

In the following table, listed data types are for SNMPv1. The data types complying with SNMPv2c and SNMPv3 are not described if they are the same as those complying with SNMPv1. For any differences, details will be described in brackets.

VB	OID	Data Type	Description
northBoundSynchAlarmEndStatus	1.3.6.1.4.1.2011.2.15.1.7.4.3	INTEGER	Alarm synchronization result. 0: indicates that the synchronization was complete. 1: indicates that the OSS stopped the synchronization. 2: indicates that the synchronization was stopped unexpectedly.

14.4 MIB3 Trap Sample

MIB3 supports four types of traps: alarm notification trap, alarm synchronization start trap, alarm synchronization result trap, and alarm synchronization end trap. The samples in this section use SNMPv1 as an example. SNMPv2c and SNMPv3 are similar to SNMPv1.

NOTE

MIB3 does not support heartbeat traps.

14.4.1 Alarm Notification Trap

When an alarm is generated on a device or NCE, the SNMP NBI will report the alarm to the OSS. MIB3 supports 36 VBs and you cannot customize them.


```
4: Specific trap northboundNotificationType::northBoundSynchAlarm #2 trap(v1) received from:
10.71.226.158 at 2011-3-10 10:52:50     Time stamp: 0 days 00h:05m:24s.43th     Agent address:
10.71.226.158 Port: 982 Transport: IP/UDP Protocol: SNMPv1 Trap     Manager address:
10.70.71.97 Port: 6666 Transport: IP/UDP     Community: ******     SNMPv1 agent address:
10.71.226.158     Enterprise: northboundNotificationType     Specific Trap MIB Lookup
Results     Name: northBoundSynchAlarm, Module: T2000-NETMANAGEMENT-MIB, Enterprise:
northboundNotificationType     Bindings (36)     Binding #1:
northboundReportAlarmManagedObjectClass.0 *** (octets) (zero-length)     Binding #2:
northboundReportAlarmManagedObjectInstance.0 *** (octets) Huawei/NCE     Binding #3:
northboundReportAlarmEventType.0 *** (octets) processingErrorAlarm     Binding #4:
northboundReportAlarmEventTime.0 *** (octets) 2010-11-29,23:31:54.0     Binding #5:
northboundReportAlarmProbableCause.0 *** (octets) When the database usage is larger than
the threshold for the critical severity, the NMS generates this alarm. When the database usage
is smaller than the threshold for the critical severit ...     Binding #6:
northboundReportAlarmSpecificProblems.0 *** (octets) (zero-length)     Binding #7:
northboundReportAlarmPerceivedSeverity.0 *** (octets) Critical     Binding #8:
northboundReportAlarmNotificationIdentifier.0 *** (int32) 20     Binding #9:
northboundReportAlarmCorrelatedNotifications.0 *** (int32) 20     Binding #10:
northboundReportAlarmProposedRepairActions.0 *** (octets) (zero-length)     Binding #11:
northboundReportAlarmAdditionalText.0 *** (octets) (zero-length)     Binding #12:
northboundReportAlarmEmsName.0 *** (octets) Huawei/NCE     Binding #13:
northboundReportAlarmNEName.0 *** (octets) Huawei/NCE     Binding #14:
northboundReportAlarmDevLocation.0 *** (octets) (zero-length)     Binding #15:
northboundReportAlarmRackName.0 *** (octets) 1     Binding #16:
northboundReportAlarmShelfName.0 *** (octets) (zero-length)     Binding #17:
northboundReportAlarmBoardName.0 *** (octets) (zero-length)     Binding #18:
northboundReportAlarmPortType.0 *** (octets) (zero-length)     Binding #19:
northboundReportAlarmPortNumber.0 *** (int32) 0     Binding #20:
northboundReportAlarmLocation.0 *** (octets) EMS System     Binding #21:
northboundReportAlarmOperationAffected.0 *** (int32) 0     Binding #22:
northboundReportAlarmID.0 *** (int32) 103     Binding #23: northboundReportAlarmName.0
*** (octets) The Database Usage Is Too High (Critical)     Binding #24:
northboundReportAlarmIPAddress.0 *** (octets) (zero-length)     Binding #25:
northboundReportAlarmResourceID.0 *** (octets) (zero-length)     Binding #26:
northboundReportAlarmCleared.0 *** (int32) 0     Binding #27:
northboundReportAlarmAdditionalVB1.0 *** (octets) (zero-length)     Binding #28:
northboundReportAlarmAdditionalVB2.0 *** (octets) (zero-length)     Binding #29:
northboundReportAlarmAdditionalVB3.0 *** (octets) (zero-length)     Binding #30:
northboundReportAlarmAdditionalVB4.0 *** (octets) (zero-length)     Binding #31:
northboundReportAlarmAdditionalVB5.0 *** (octets) (zero-length)     Binding #32:
northboundReportAlarmAdditionalVB6.0 *** (octets) (zero-length)     Binding #33:
northboundReportAlarmAdditionalVB7.0 *** (octets) (zero-length)     Binding #34:
northboundReportAlarmAdditionalVB8.0 *** (octets) (zero-length)     Binding #35:
northboundReportAlarmAdditionalVB9.0 *** (octets) (zero-length)     Binding #36:
northboundReportAlarmAdditionalVB10.0 *** (octets) (zero-length)
```

14.4.2 Alarm Synchronization Start Trap

After the OSS sends alarm synchronization requests, the SNMP NBI returns the start notification of alarm synchronization.

```
54: Specific trap northboundNotificationType::northBoundSynchAlarmStart #3 trap(v1) received
from: 10.71.226.158 at 2011-3-10 10:53:04     Time stamp: 0 days 00h:05m:38s.06th     Agent
address: 10.71.226.158 Port: 982 Transport: IP/UDP Protocol: SNMPv1 Trap     Manager address:
10.70.71.97 Port: 6666 Transport: IP/UDP     Community: ******     SNMPv1 agent address:
10.71.226.158     Enterprise: northboundNotificationType     Specific Trap MIB Lookup
Results     Name: northBoundSynchAlarmStart, Module: T2000-NETMANAGEMENT-MIB,
Enterprise: northboundNotificationType     Bindings (1)     Binding #1:
northboundNotificationType.0.4 *** (int32) 0
```


14.4.3 Alarm Synchronization Result Trap

After the OSS sends alarm synchronization requests, the SNMP NBI will report the alarms meeting filter criteria to the OSS.

```
55: Specific trap northboundNotificationType::northBoundSynchAlarm #2 trap(v1) received
from: 10.71.226.158 at 2011-3-10 10:53:04     Time stamp: 0 days 00h:05m:38s.25th     Agent
address: 10.71.226.158 Port: 982 Transport: IP/UDP Protocol: SNMPv1 Trap     Manager address:
10.70.71.97 Port: 6666 Transport: IP/UDP     Community: ******     SNMPv1 agent address:
10.71.226.158     Enterprise: northboundNotificationType     Specific Trap MIB Lookup
Results     Name: northBoundSynchAlarm, Module: T2000-NETMANAGEMENT-MIB, Enterprise:
northboundNotificationType     Bindings (36)     Binding #1:
northboundReportAlarmManagedObjectClass.0 *** (octets) (zero-length)     Binding #2:
northboundReportAlarmManagedObjectInstance.0 *** (octets) Huawei/NCE     Binding #3:
northboundReportAlarmEventType.0 *** (octets) processingErrorAlarm     Binding #4:
northboundReportAlarmEventTime.0 *** (octets) 2008-09-21,15:29:56.0     Binding #5:
northboundReportAlarmProbableCause.0 *** (octets) SFTP server fault     Binding #6:
northboundReportAlarmSpecificProblems.0 *** (octets) SFTP server fault     Binding #7:
northboundReportAlarmPerceivedSeverity.0 *** (octets) Major     Binding #8:
northboundReportAlarmNotificationIdentifier.0 *** (int32) 2     Binding #9:
northboundReportAlarmCorrelatedNotifications.0 *** (int32) 2     Binding #10:
northboundReportAlarmProposedRepairActions.0 *** (octets) (zero-length)     Binding #11:
northboundReportAlarmAdditionalText.0 *** (octets) (zero-length)     Binding #12:
northboundReportAlarmEmsName.0 *** (octets) Huawei/NCE     Binding #13:
northboundReportAlarmNEName.0 *** (octets) Huawei/NCE     Binding #14:
northboundReportAlarmDevLocation.0 *** (octets) (zero-length)     Binding #15:
northboundReportAlarmRackName.0 *** (octets) 1     Binding #16:
northboundReportAlarmShelfName.0 *** (octets) (zero-length)     Binding #17:
northboundReportAlarmBoardName.0 *** (octets) (zero-length)     Binding #18:
northboundReportAlarmPortType.0 *** (octets) (zero-length)     Binding #19:
northboundReportAlarmPortNumber.0 *** (int32) 0     Binding #20:
northboundReportAlarmLocation.0 *** (octets) EMS System     Binding #21:
northboundReportAlarmOperationAffected.0 *** (int32) 0     Binding #22:
northboundReportAlarmID.0 *** (int32) 60002     Binding #23: northboundReportAlarmName.
0 *** (octets) SFTP server fault     Binding #24: northboundReportAlarmIPAddress.0 *** (octets)
(zero-length)     Binding #25: northboundReportAlarmResourceID.0 *** (octets) (zero-
length)     Binding #26: northboundReportAlarmCleared.0 *** (int32) 0     Binding #27:
northboundReportAlarmAdditionalVB1.0 *** (octets) (zero-length)     Binding #28:
northboundReportAlarmAdditionalVB2.0 *** (octets) (zero-length)     Binding #29:
northboundReportAlarmAdditionalVB3.0 *** (octets) (zero-length)     Binding #30:
northboundReportAlarmAdditionalVB4.0 *** (octets) (zero-length)     Binding #31:
northboundReportAlarmAdditionalVB5.0 *** (octets) (zero-length)     Binding #32:
northboundReportAlarmAdditionalVB6.0 *** (octets) (zero-length)     Binding #33:
northboundReportAlarmAdditionalVB7.0 *** (octets) (zero-length)     Binding #34:
northboundReportAlarmAdditionalVB8.0 *** (octets) (zero-length)     Binding #35:
northboundReportAlarmAdditionalVB9.0 *** (octets) (zero-length)     Binding #36:
northboundReportAlarmAdditionalVB10.0 *** (octets) (zero-length)
```

14.4.4 Alarm Synchronization End Trap

Alarm synchronization end traps are triggered when all required alarms have been reported to the OSS or the OSS automatically stops the synchronization.

Synchronization Stopped After Alarm Reporting Was Complete

After all required alarms are reported to the OSS, SNMP NBI sends traps through the SNMP NBI to inform the OSS of the stop of alarm reporting.

```
101: Specific trap northboundNotificationType::northBoundSynchAlarmEnd #4 trap(v1) received
from: 10.71.226.158 at 2011-3-10 10:53:08     Time stamp: 0 days 00h:05m:42s.27th     Agent
```


address: 10.71.226.158 Port: 982 Transport: IP/UDP Protocol: SNMPv1 Trap Manager address: 10.70.71.97 Port: 6666 Transport: IP/UDP Community: ****** SNMPv1 agent address: 10.71.226.158 Enterprise: northboundNotificationType Specific Trap MIB Lookup Results Name: northBoundSynchAlarmEnd, Module: T2000-NETMANAGEMENT-MIB, Enterprise: northboundNotificationType Bindings (1) Binding #1: northBoundSynchAlarmEndStatus.0 *** (int32) 0

Synchronization Was Stopped by the OSS

The OSS can also stop the synchronization as required. The SNMP NBI then reports traps to inform the OSS of the stop of alarm synchronization, as a response to the request.

101: Specific trap northboundNotificationType::northBoundSynchAlarmEnd #4 trap(v1) received from: 10.71.226.158 at 2011-3-10 10:53:08 Time stamp: 0 days 00h:05m:42s.27th Agent address: 10.71.226.158 Port: 982 Transport: IP/UDP Protocol: SNMPv1 Trap Manager address: 10.70.71.97 Port: 6666 Transport: IP/UDP Community: ****** SNMPv1 agent address: 10.71.226.158 Enterprise: northboundNotificationType Specific Trap MIB Lookup Results Name: northBoundSynchAlarmEnd, Module: T2000-NETMANAGEMENT-MIB, Enterprise: northboundNotificationType Bindings (1) Binding #1: northBoundSynchAlarmEndStatus.0 *** (int32) 1

Synchronization Was Stopped Unexpectedly

58: Specific trap northboundNotificationType::northBoundSynchAlarmEnd #4 trap(v1) received from: 10.71.224.13 at 2011-4-27 17:15:52 Time stamp: 0 days 00h:22m:37s.33th Agent address: 10.71.224.13 Port: 982 Transport: IP/UDP Protocol: SNMPv1 Trap Manager address: 10.70.71.97 Port: 6666 Transport: IP/UDP Community: ****** SNMPv1 agent address: 10.71.224.13 Enterprise: northboundNotificationType Specific Trap MIB Lookup Results Name: northBoundSynchAlarmEnd, Module: T2000-NETMANAGEMENT-MIB, Enterprise: northboundNotificationType Bindings (1) Binding #1: northBoundSynchAlarmEndStatus. 0 *** (int32) 2

A Acronyms and Abbreviations

This part lists the acronyms and abbreviations in this document.

E	
EMS	element management system
I	
IP	Internet Protocol
M	
MC	monitor center
MIB	management information base
N	
NBI	northbound interface
NE	network element
NMC	network management center
NMS	network management system
P	
PDU	Protocol Data Unit
S	
SMI	structure of management information
SNMP	Simple Network Management Protocol
T	
TCP	Transmission Control Protocol
TMN	Telecommunication Management Network
V	
VB	variable binding

