

MiVoice MX-ONE SNMP Support, Alarm Notification and Emergency Call Events

OPERATIONAL DIRECTIONS



NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2017, Mitel Networks Corporation

All rights reserved

1

GENERAL

Note: MiVoice MX-ONE supports SNMPv1, SNMPv2c and SNMPv3 MIBs for monitoring and traps. The MX-ONE SNMP agent does not include provisioning or configuration from an NMS. Provisioning of MX-ONE shall be accomplished using Provisioning Manager and Service Node Manager or alternatively via an SSL CLI interface.

The MX-ONE Service Node can be supervised from a Simple Network Management Protocol (SNMP) management system and configured to send alarm notifications by snmp traps or optionally by e-mail or text messaging using Short Messaging Service (SMS).

This document describes the MX-ONE Service Node SNMP support and how the basic configuration of alarm notification is set up.

There are three snmp MIB implementations available in the service node, the old deprecated Ericsson MIB and the Mitel MIB for monitoring status and alarms, and the Mitel ERN MIB for emergency call events.

You can monitor MX-ONE Service Node from an SNMP management system, using one or all tree of them.

The SNMP implementation in the MX-ONE Service Node is based on *net-snmp*. More documentation can be found in the */usr/share/doc/packages/net-snmp* directory or at <http://www.net-snmp.org>.

Net-snmp is one of the packages installed along with the operating system on the MX-ONE Service Node. During installation, the net-snmp daemon is configured to use the AGENT_X protocol.

Note: The programs ALSNMP (Ericsson MIB) and AALSNMP (Mitel Status MIB) and ESNMP (Mitel emergency notification MIB) are part of the telephony system, and communicate with the snmp daemon via the AGENT_X protocol. The ALSNMP and ESNMP are not loaded by default, and needs to be loaded using the `pu_add` command, if the Ericsson MIB format or the Mitel emergency notifications are used.

The snmp daemon (snmpd) is installed in each LIM (node) of the MX-ONE. Consequently, the network management systems needs to get traps from all nodes individually to get the complete system view.

In the normal setup each node sends traps directly to network management systems but may be configured to route traps through a proxy to the network management systems. The snmpd daemon has a default setup and is operational after installation, but requires additional configuration for the traps to be sent to the management system.

The snmptrapd daemon is also be used for additional features like proxy agent for traps and to log traps to local disk. These features needs additional configuration.

The snmptrapd daemon program is installed, but is not activated as default, thus to enable e-mail, SMS or other features additional configuration is required.

2

PREREQUISITES

The MiVoice MX-ONE system must run.

Since the legacy Ericsson MIB SNMP format, and Mitel emergency notifications are regarded as an optional functions, the ALSNMP or ESNMP SW programs must be manually loaded before using the functionality desired. Only the Mitel status MIB (AALSNMP) is automatically loaded at installation.

See the ADMINISTRATOR USER'S GUIDE, and the INSTALLING AND CONFIGURING MIVOICE MX-ONE, section Optional programs.

3

SNMP INTRODUCTION

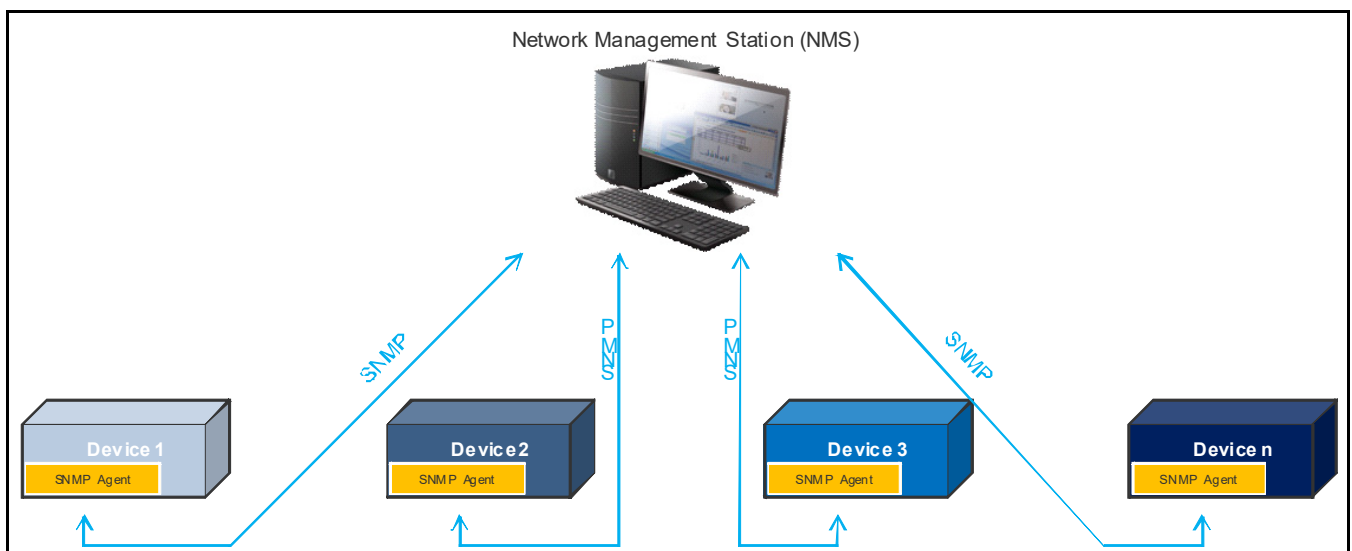
The SNMP (Simple Network Management Protocol) is an Internet-standard protocol used to manage devices on IP networks.

As defined in the RFC 1157, "Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements."

SNMP is composed by three components:

- Managed device or network elements
- Agent - software that runs on managed device that defines what can be monitored and controlled.
- Network Management Station (NMS) - software that runs on management system that are responsible for polling (query) and receiving traps from agents, process the received information and take the proper action.

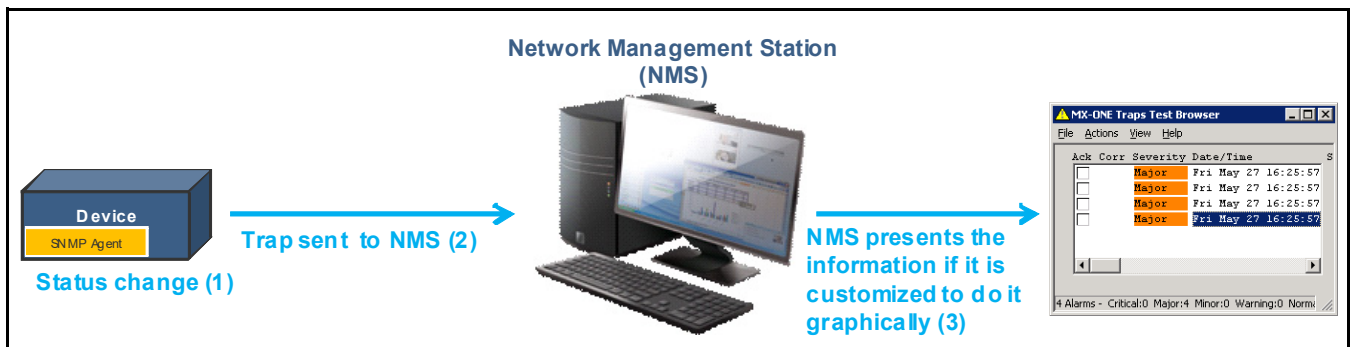
SNMP protocol is used to exchange information between the monitored device and NMS.



Basically, there are two methods that SNMP agents can communicate with Network Management Station, receiving a Trap or requesting information via Queries.

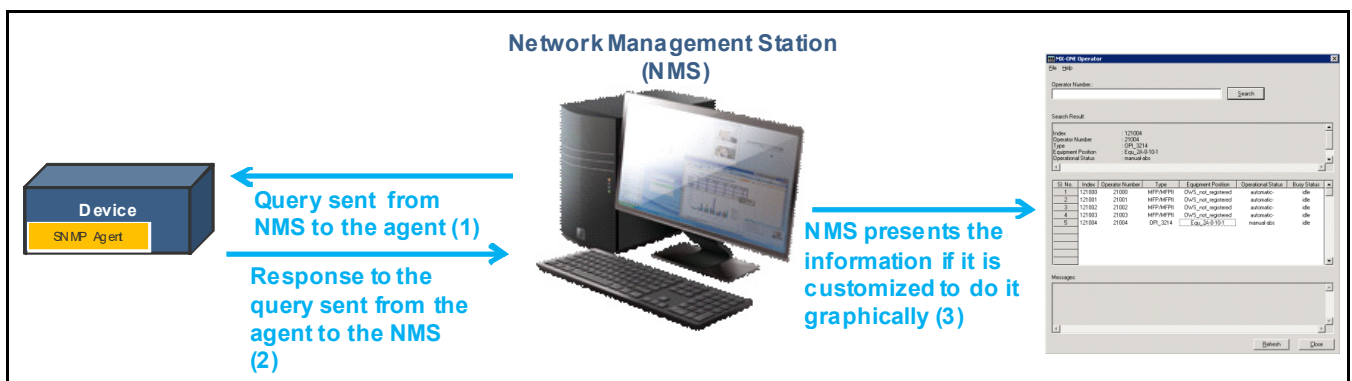
Trap

The agent sends Traps when occurs status change in the monitored device. The Trap is received by Network Management Station (NMS) that can present the information in a graphical format, if properly configured, as shown in the figure below.



Query

A query can be requested from the NMS, for example from a MIB Browser to collect data from the monitored device.



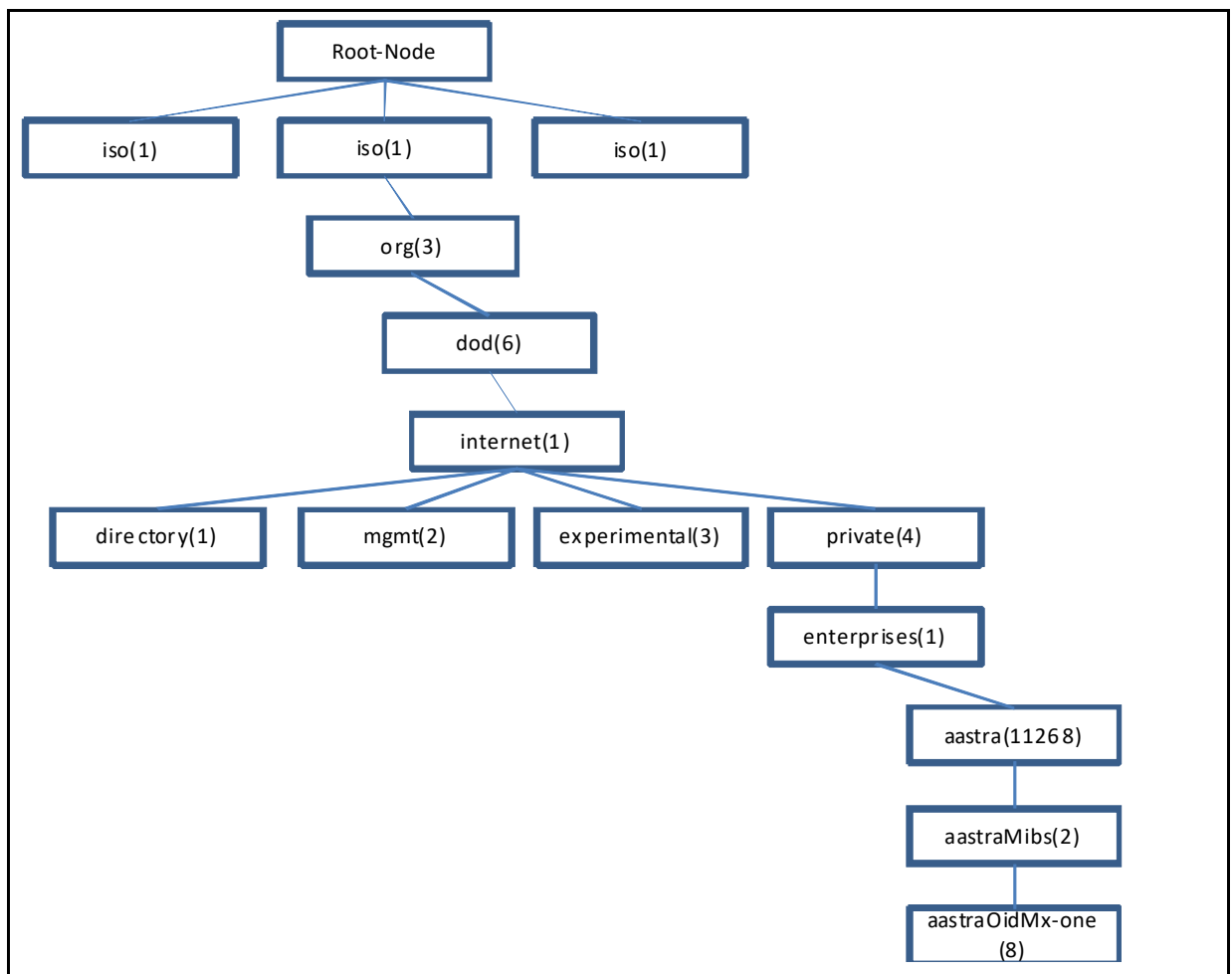
The SNMP protocol does not define which information a managed device should provide. Indeed, SNMP uses management information bases (MIBs) to define the available information. MIBs is described as a database of managed objects where monitored information such as interface status, etc is defined.

MIBs use a hierarchical tree-structured database. The Structure of Management Information Version 1 (SMIv1) defines how managed objects are named and specifies their associated information.

A unique name or object identifier (OID) is used to identify a managed object, where each has a numerical OID and an associated textual name, as the following example:

OID Name	aastraOidMxone (8)
Numerical	.1.3.6.1.4.1.11268.2.8
Textual	.iso.org.dod.internet.private.enterprises.aastra.aastraMibs.aastraOidMx-one
	or
	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).aastra(11268).aastraMibs(2).aastraOidMx-one(8).

The figure below shows the SMI representation for the Mitel's aastraOidMxone OID.



The supplier of the monitored device needs to provide a MIB (Management information base) file that defines what information is available from that specific device.

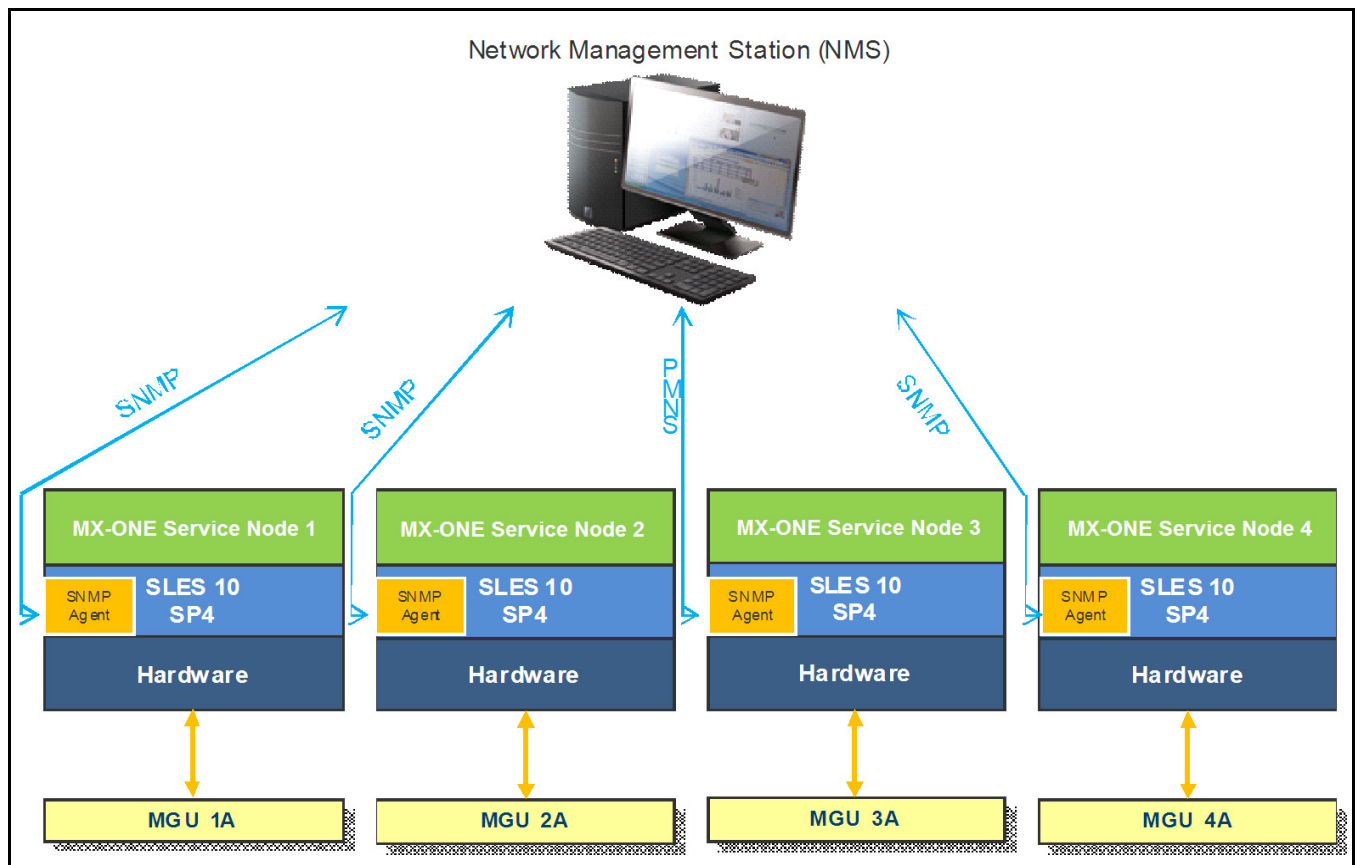
4 MIVOICE MX-ONE SNMP

4.1 SNMP IMPLEMENTATION

MX-ONE is a device running on IP networks supports SNMP that means the MX-ONE Service Node is supervised by a SNMP network management station or network node manager.

MX-ONE Service Node can be configured to send alarm notifications by SNMP traps or optionally by e-mail or text messaging using Short Messaging Service (SMS).

The SNMP implementation in the MX-ONE Service Node is based on net-snmp. Net-snmp is one of the packages installed along with the operating system on the MX-ONE Service Node. During installation, the net-snmp daemon is configured to use the AGENT_X protocol. The program AALSNMP (Mitel MIB) is part of the telephony system and communicates with the SNMP daemon via the AGENT_X protocol. The SNMP daemon (snmpd) is installed in each server (node) of the MX-ONE. Consequently, the network management station needs to get traps from all nodes individually in order to get the complete system view.



4.2

DIFFERENCE BETWEEN SNMP IMPLEMENTATION IN MIVoice MX-ONE V.4.1 AND MIVoice MX-ONE 5.0/6.0

4.2.1

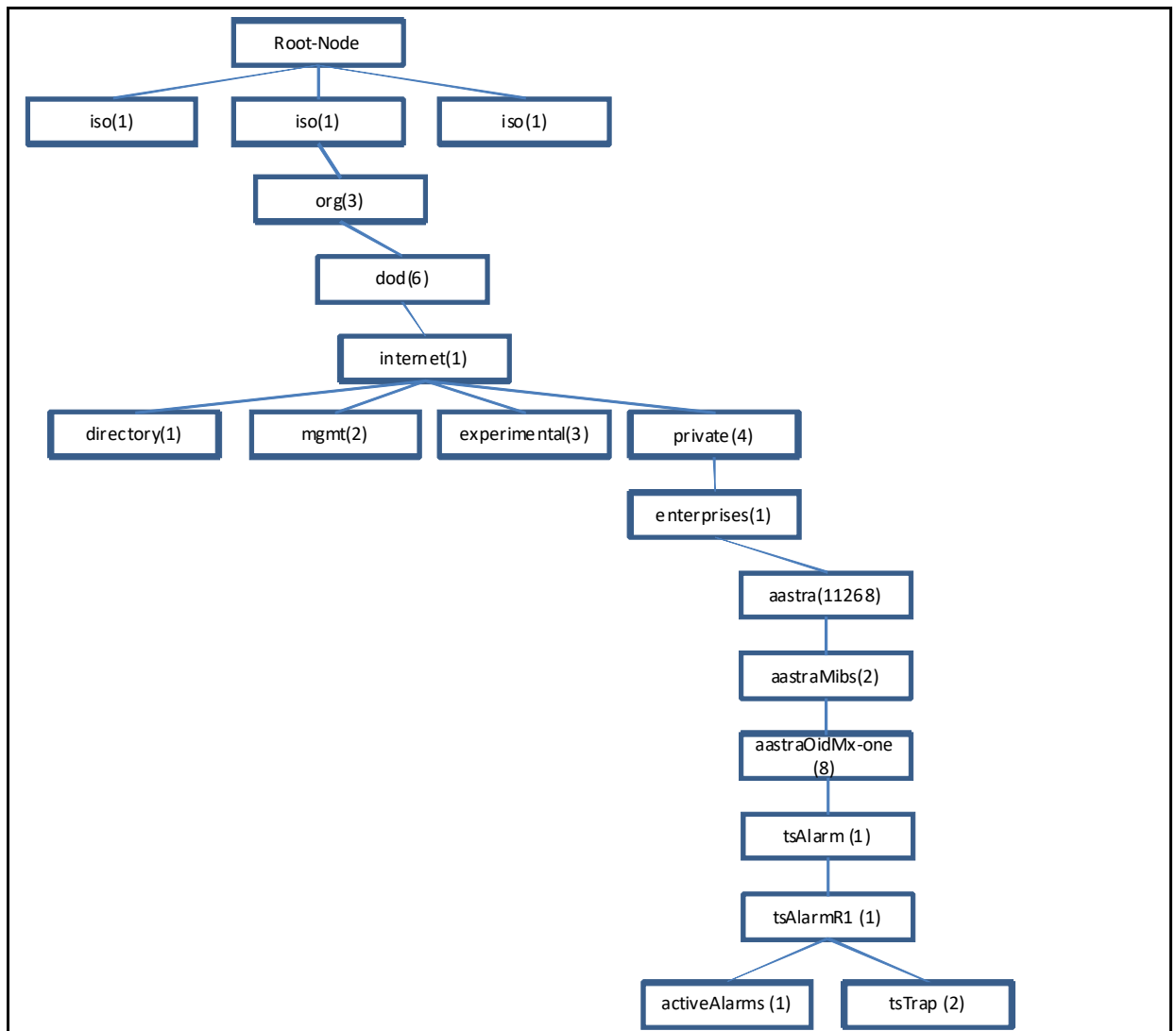
MIVoice MX-ONE

The SNMP MIB available in MX-ONE implements system alarms objects.

In short, up to MX-ONE 4.1, only system alarms were supported by the MX-ONE SNMP MIB.

The OID that represents MX-ONE system alarms is the following:

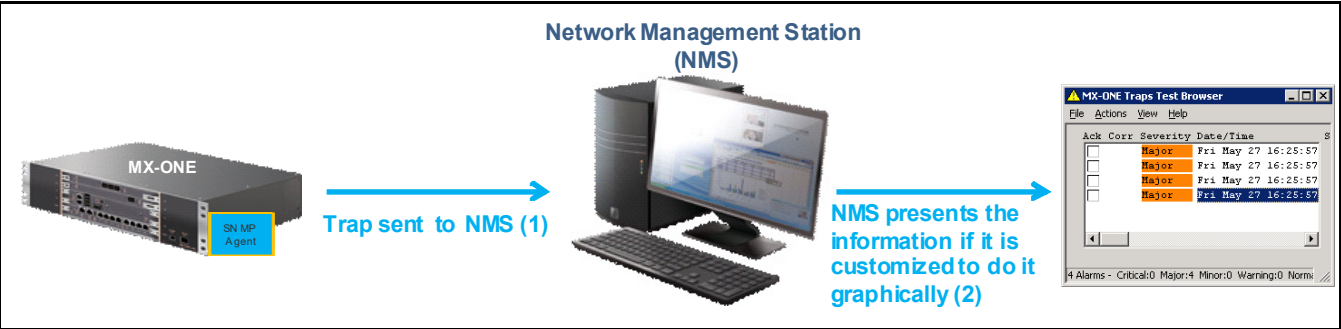
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).aastra(11268).aastraMibs(2).aastraOidMx-one(8).tsAlarm(1).tsAlarmR1(1)



MX-ONE SNMP agent sends system alarms traps to a NMS when an alarm occurs in the system if it configured properly.

The Network Management System is customized to understand the information provided by MX-ONE SNMP agent.

You can use query to fetch alarm information from MX-ONE Service Node.



The figure below is an example of MX-ONE Alarms in one Network Management system that is customized to work with MX-ONE.

The screenshot shows the 'MX-ONE TS Alarms Browser' window. It contains a table with columns: Ack, Corr, Severity, Date/Time, OAD-Name, Source, and Message. The table lists several alarms, including 'Warning', 'CRITICAL', and 'Normal' severity levels. The status bar at the bottom indicates '11 Alarms - Critical:3 Major:0 Minor:0 Warning:1 Normal:7'.

Ack	Corr	Severity	Date/Time	OAD-Name	Source	Message
<input type="checkbox"/>		Warning	Tue 11 25 18:21:02	192.168.26.110	rack	No info detected alarm: test
<input type="checkbox"/>		CRITICAL	Tue 11 25 19:00:54	192.168.26.110	LIM rack 1	detected alarm: Local
<input type="checkbox"/>		Normal	Tue 11 25 19:00:54	192.168.26.110		Alarm status has been changed from
<input type="checkbox"/>		Normal	Tue 11 25 19:00:59	192.168.26.110	LIM rack 1	detected alarm ceased:
<input type="checkbox"/>		Normal	Tue 11 25 19:00:59	192.168.26.110		Alarm status has been changed from
<input type="checkbox"/>		CRITICAL	Tue 11 25 19:00:59	192.168.26.110	LIM rack 1	detected alarm: Broken
<input type="checkbox"/>		Normal	Tue 11 25 19:00:59	192.168.26.110		Alarm status has been changed from
<input type="checkbox"/>		CRITICAL	Tue 11 25 19:00:59	192.168.26.110	LIM rack 1	detected alarm: Broken
<input type="checkbox"/>		Normal	Tue 11 25 19:01:04	192.168.26.110	LIM rack 1	detected alarm ceased:
<input type="checkbox"/>		Normal	Tue 11 25 19:01:04	192.168.26.110	LIM rack 1	detected alarm ceased:
<input type="checkbox"/>		Normal	Tue 11 25 19:01:04	192.168.26.110		Alarm status has been changed from

Note: NMS is customized to display MX-ONE information. The SNMP Plug-in for HP Openview 7.53 Windows version was customized for it.

4.2.2

MIVOICE MX-ONE 5.0 & 6.0 SNMP IMPLEMENTATION

If you want to retrieve information from active LIMs in a system where the connection to one or more other LIMs is lost, the request for information from the SNMP manager cannot use **getnext** (SNMP-walk). Therefore, when reading data in the LIM data table, the SNMP-walk stops and does not continue to the next table.

Instead requests for specific data has to be made on a per LIM basis, one at a time.

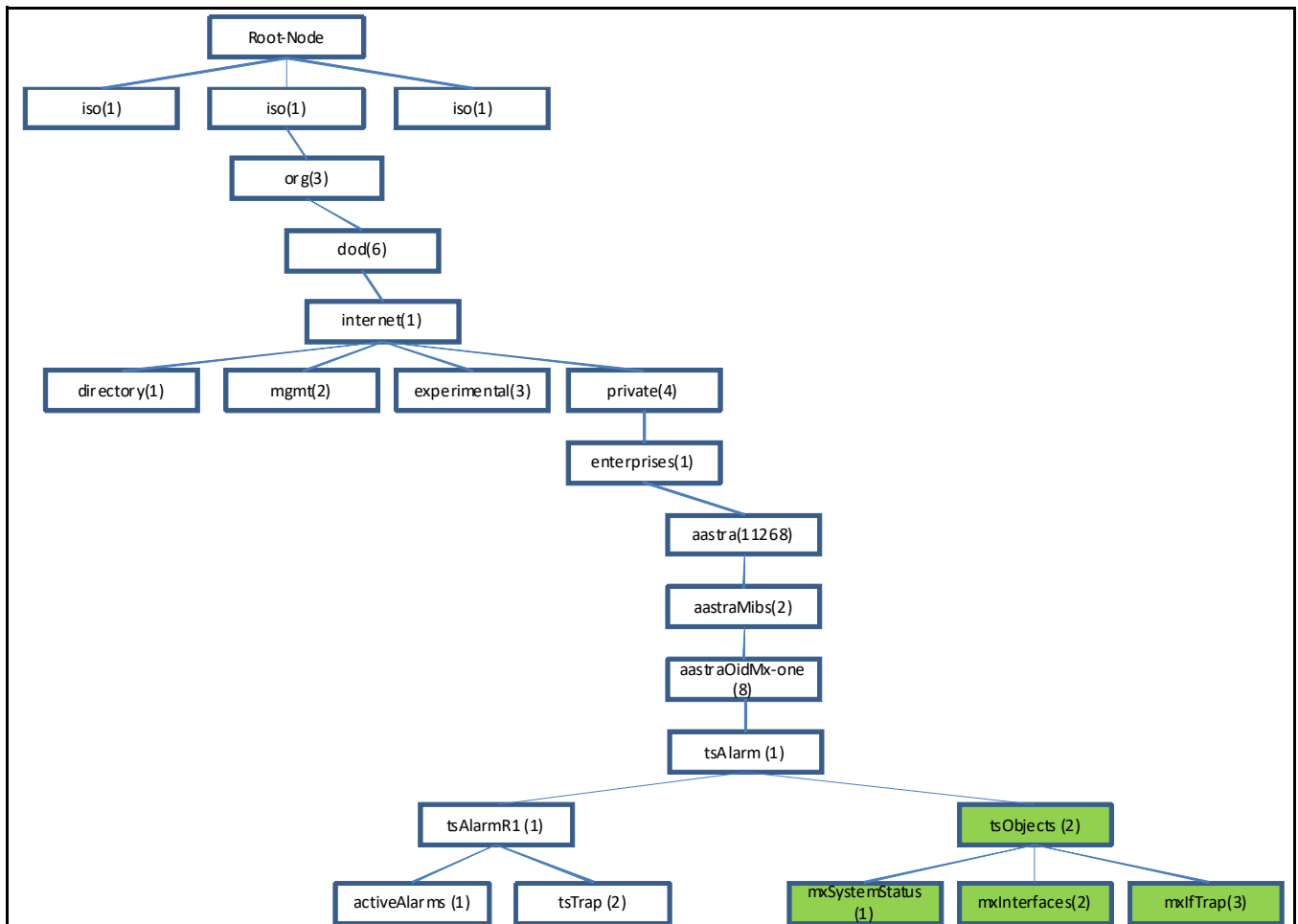
The device MIB must use an initial scan of the whole tree. The SNMP station, then stores the information tree in a map. This tree is then used to fetch status of the devices and store the status in the map. If new devices are then added or removed in this MIB, a TRAP message alerts that the tree has changed, which causes the SNMP station to update the map. Therefore, you need to update only the status of the mapped devices. You may do a complete scan only when the sync between the tree and the map is lost.

When you create a map of devices, it normally shows LIMs, MGUs, boards, and so on. The alarm status of the devices (from the other MIB) should be assigned and be visible in the map. If the alarm status in the LIM, MGU or device is critical, the traffic status is irrelevant because the device might probably be offline.

In MX-ONE 5.0 a new group of objects were implemented to monitor MX-ONE functions and devices. These objects also exist in MX-ONE 6.0.

These news objects are represented by the OID Objects.

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).aastra(11268).aastraMibs(2).aastraOidMx-one(8).tsAlarm(1).tsObjects(2)



The additional information in 5.0/6.0 is the tsObject MIB:

MxSystemStatus and mxInterfaces, provides MX-ONE information regarding the items below. NNM can query this information. They are read-only.

mxSystemStatus(1)

- MX-ONE Release
- System Status
 - Number of Servers, IPs, Backup Status and Info, GSM Sync info, MX-ONE Service Node Status.

mxInterfaces(2)

- Trunk
 - Type, Description, Bearer Cap, Route number, Trunk Identification (TRU), EQU, Status.
- Operator
 - Directory Number, Type, EQU, Operation and Busy Status.
- Call Information Logging
 - Output, Type, Subtype, Dbname, Server, Operational Status.
- Computer Telephony Integration phase 3
 - CTI Group, Server, IP, Operational Status.
- Computer Telephony Integration phase 1
 - CTI Group, Server, IP, Operational Status.
- Interception Computer, ICU

- Individual, Type, Interface, Server Number, Information, Operational Status.
- Gateway
 - Type, Identification, Description, Operational Status, IP.
- Media Gateways
 - Type, Identification, Description, Operational Status, IP.
- Inter Server Signaling
 - GJU side: Type, Identification, Remote Side, Description, Status.
 - GSM side: Identification, Synchronism, Operational Status A and B, Active side.
- CAS Boards
 - Type, Identification, Description, Operational Status.

MIB Trap, when there is a change on the status of the following items MX-ONE Service Node sends a trap to the NNM.

mxTrap(3)

- Trunk
- Operator
- Call Information Logging
- Computer Telephony Integration 1
- Computer Telephony Integration 3
- Interception Computer
- Gateway
- Media Gateway
- Inter Server Signaling
- Voice Cards
- CAS Boards

4.2.3

MIVOICE MX-ONE 5.0/6.0 SNMP LICENSE MECHANISM

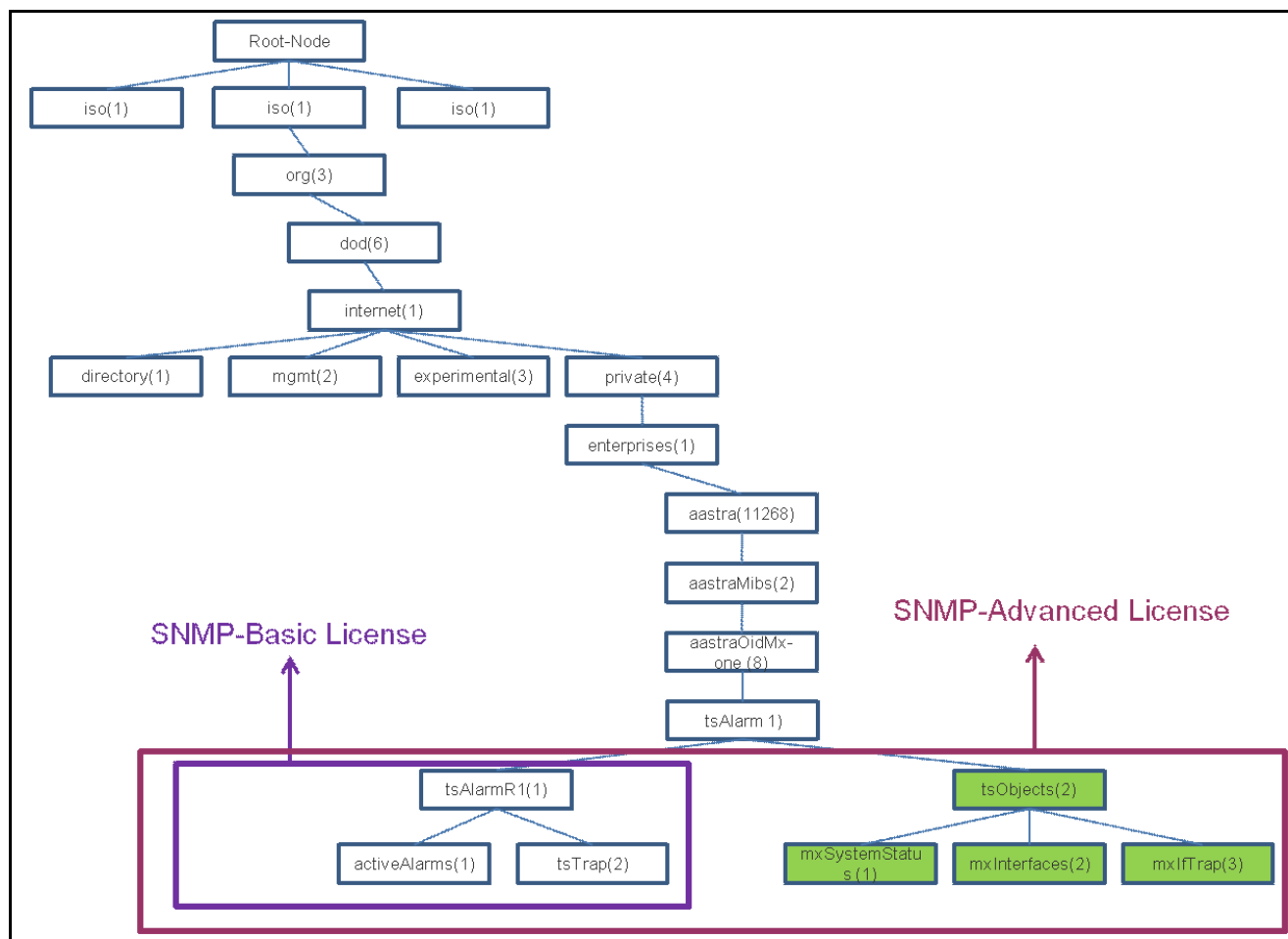
The SNMP license in MX-ONE 5.0/6.0 is divided in two parts and they are called basic and advanced:

Basic

It allows MX-ONE to send alarm information via traps to a NMS and the system administrator can query the system to get some alarm information (tsAlarmR1 in the screen below).

Advanced

It allows MX-ONE to send alarm and object information via trap to a NMS and the system administrator can query the system to get some alarm/object information (tsAlarmR1 and tsObjects in the screen below).



5 MIB SUPPORT

5.1 INITIAL MIB SUPPORT

- MIB-2 – General network statistics (RFC 1213).
- Net-snmp agent extensions – Processes, disks, memory, load average, shell commands, and error handling.
- SNMPv3 MIBS (RFC 2571-6).
- Partial support of Ericsson-MD110-SNMP-MIB, using ALSNMP.
- Full support of Mitel MX-ONE-TS-ALARM-MIB, using AALSNMP.

The administrator can add additional MIBs, but it must be configured separately.

5.2 PARTIAL SUPPORT OF ERICSSON MIBS

The definitions are found in an installed system at:
/usr/share/snmp/mibs/Ericsson-DNA-SNMP-MIB.txt and
/usr/share/snmp/mibs/Ericsson-MD110-SNMP-MIB.txt.

Implementation in program unit ASNMP.

5.2.1 SUPPORTED OBJECTS IN DEPRECATED ERICSSON MD110 SNMP MIB

In the MX-ONE Service Node, only the following objects in the MD110 SNMP MIB are supported with read-only access:

	OID	Description
md110Release	.1.3.6.1.4.1.193.8.1.1	
mdAlarmStatus	.1.3.6.1.4.1.193.8.1.3.1.2	
activeAlarms	.1.3.6.1.4.1.193.8.1.3.2.1.1.1-10000	

5.2.2 SUPPORTED TRAPS IN DEPRECATED ERICSSON MD110 SNMP MIB

	OID	Description
mdAlarmCritical	.1.3.6.1.4.1.193.8.1.0.1	
mdAlarmMajor	.1.3.6.1.4.1.193.8.1.0.2	
mdAlarmMinor	.1.3.6.1.4.1.193.8.1.0.3	
mdAlarmWarning	.1.3.6.1.4.1.193.8.1.0.4	
mdAlarmCease	.1.3.6.1.4.1.193.8.1.0.5	
mdAlarmStatusChange	.1.3.6.1.4.1.193.8.1.0.2000	

5.3

FULL SUPPORT OF MX-ONE-TS-ALARM-MIBS

The definitions are found in an installed system at:
 /usr/share/snmp/mibs/MX-ONE-TS-ALARM-MIB.txt or in Operational directions
 MX-ONE TS Alarm MIB.

Implementation in program unit AASNMP.

5.3.1

SUPPORTED OBJECTS IN MX-ONE-TS-ALARM-MIB

Table 1 Alarm OIDs

	OID	Description
tsAlarmR1	.1.3.6.1.4.1.11268.2.8.1.1	
activeAlarms	.1.3.6.1.4.1.11268.2.8.1.1.1	
mxalStatus	.1.3.6.1.4.1.11268.2.8.1.1.1.1	See below *)
activeAlarmTable	.1.3.6.1.4.1.11268.2.8.1.1.1.2	A table of active alarms in the MX-ONE node.
ActiveAlarmEntry	.1.3.6.1.4.1.11268.2.8.1.1.1.2.1	
mxalHandle	.1.3.6.1.4.1.11268.2.8.1.1.1.2.1.1	Handle of an MX-ONE alarm. An alarm instance is identified by its handle and the lim number.
mxalFrom	.1.3.6.1.4.1.11268.2.8.1.1.1.2.1.2	Sending lim (and unit) related to the alarm.
mxalFaultCode	.1.3.6.1.4.1.11268.2.8.1.1.1.2.1.3	Fault Code of an MX-ONE alarm. Indicates type of alarm. Fault code is domain:code (within domain). Example: Fault code 5:8.
mxalSeverity	.1.3.6.1.4.1.11268.2.8.1.1.1.2.1.4	See below *)
mxalWhere	.1.3.6.1.4.1.11268.2.8.1.1.1.2.1.5	Faulty unit etc related to the alarm.
mxalExplanation	.1.3.6.1.4.1.11268.2.8.1.1.1.2.1.6	Textual description associated with the alarm.
mxalNoticed	.1.3.6.1.4.1.11268.2.8.1.1.1.2.1.7	Indicates if the alarm is noticed. May indicate that someone is working on the problem.
mxalNoticedNote	.1.3.6.1.4.1.11268.2.8.1.1.1.2.1.8	Comment added to the alarm when noticed.

*) The current alarm status of the MX-ONE node

- Indeterminate - Status unknow
- Critical - Any active alarms with severity 4,
- Major - Any active alarms with severity 3,
- Minor - Any active alarms with severity 2,
- Warning - Any active alarms with severity 1,
- Normal - Any active alarms with severity 0, or no active alarms.

5.3.2

SUPPORTED TRAPS IN MX-ONE-TS-ALARM-MIB

Table 2 Trap OIDs

	OID	Description
tsTrap	.1.3.6.1.4.1.11268.2.8.1.1.2	
tsTrapV2	.1.3.6.1.4.1.11268.2.8.1.1.2.0	
mxAlarmCritical	.1.3.6.1.4.1.11268.2.8.1.1.2.0.1	This trap is sent when an MX-ONE alarm with severity 4 is detected.
mxAlarmMajor	.1.3.6.1.4.1.11268.2.8.1.1.2.0.2	This trap is sent when an MX-ONE alarm with severity 3 is detected.

	OID	Description
mxAlarmMinor	.1.3.6.1.4.1.11268.2.8.1.1.2.0.3	This trap is sent when an MX-ONE alarm with severity 2 is detected.
mxAlarmWarning	.1.3.6.1.4.1.11268.2.8.1.1.2.0.4	This trap is sent when an MX-ONE alarm with severity 1 is detected.
mxAlarmSysClear	.1.3.6.1.4.1.11268.2.8.1.1.2.0.5	This trap is sent when an MX-ONE alarm is cleared by the system.
mxAlarmOpClear	.1.3.6.1.4.1.11268.2.8.1.1.2.0.6	This trap is sent when an MX-ONE alarm is cleared by the operator.
mxAlarmStatusChange	.1.3.6.1.4.1.11268.2.8.1.1.2.0.2000	This trap is sent when the alarm status of the lim is changed.

5.4 MIVOICE MX-ONE 5.0/6.0 SNMP MIB DETAIL DESCRIPTION

The definitions are found in an installed system at:
/usr/share/snmp/mibs/MX-ONE-TS-ALARM-MIB.txt.

Implementation in program unit ESNMP.

5.4.1 SYSTEM STATUS

5.4.1.1 System Status Information

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).aastra(11268).aastra-Mibs(2).aastraOidMx-one(8).tsAlarm(1).tsObjects(2).mxSystemStatus(1)

	OID	Description
mxSystemStatus	.1.3.6.1.4.1.11268.2.8.1.2.1	
mxRelease	.1.3.6.1.4.1.11268.2.8.1.2.1.1.0	Indicates MX-ONE software release. This data is provided from the software interface and cannot be changed.
mxLimTable	.1.3.6.1.4.1.11268.2.8.1.2.1.2	A table with data for the interfaces.
mxLimEntry	.1.3.6.1.4.1.11268.2.8.1.2.1.2.1	Internal use. No information is provided.
mxLimIndex	.1.3.6.1.4.1.11268.2.8.1.2.1.2.1.1	Defines the MX-ONE Service Node number.
mxLimWhere	.1.3.6.1.4.1.11268.2.8.1.2.1.2.1.2	Presents MX-ONE Service Node host name, if defined in the DNS.
mxLimIp	.1.3.6.1.4.1.11268.2.8.1.2.1.2.1.3	The currently IP address in use by the MX-ONE Service Node.
mxLimBackupStatus	.1.3.6.1.4.1.11268.2.8.1.2.1.2.1.4	MX-ONE Service Node backup operational status.
mxLimBackupInfo	.1.3.6.1.4.1.11268.2.8.1.2.1.2.1.5	Additional information regarding MX-ONE Service Node backup. Date and hour of the current backup, if it is valid.
mxLimCCLInfo	.1.3.6.1.4.1.11268.2.8.1.2.1.2.1.6	Synchronization data in the MX-ONE Service Node if MD 110 Group Switch is presented in the MX-ONE. Unknown is displayed if GSM is not present in the system (migration customer only).
mxLimStatus	.1.3.6.1.4.1.11268.2.8.1.2.1.2.1.7	MX-ONE Service Node operational state (running, manual-blocked,system-blocked,blocked,unknown). Unknown result if the MX-ONE Service Node connected to is isolated.

	OID	Description
mxObjectStatus	.1.3.6.1.4.1.11268.2.8.1.2.1.3.0	The traffic state of the object.

5.4.2 INTERFACES

5.4.2.1 Route and Trunk information

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).astra(11268).astra-Mibs(2).astraOidMx-one(8) tsAlarm(1).tsObjects(2).mxInterfaces(2).mxIfTrunk(2)

	OID	Description
mxInterfaces	.1.3.6.1.4.1.11268.2.8.1.2.1	
mxIfTrunk	.1.3.6.1.4.1.11268.2.8.1.2.2.2	Indicates MX-ONE software release. This data is provided from the software interface and cannot be changed.
mxRouteTable	.1.3.6.1.4.1.11268.2.8.1.2.2.2.1	A table with Route information.
mxRouteEntry	.1.3.6.1.4.1.11268.2.8.1.2.2.2.1.1	Internal use. No information is provided.
mxRouteIndex	.1.3.6.1.4.1.11268.2.8.1.2.2.2.1.1.1	The route number.
mxRouteType	.1.3.6.1.4.1.11268.2.8.1.2.2.2.1.1.2	Type of route, public or tie-line. Signalling system used. Example: Public route, signal system = ISDN.
mxRouteDescr	.1.3.6.1.4.1.11268.2.8.1.2.2.2.1.1.3	Route type. See MML TYPE of interface.
mxRouteBearerCap	.1.3.6.1.4.1.11268.2.8.1.2.2.2.1.1.4	Bearer capabilities of the route Corresponds to the route parameter BCAP. The positions is a string of 0 and 1. Each position of the string corresponds to a Bearer capability attribute, A position set to 1 means that the corresponding capability is provided. pos 1 :64 kbps Unrestricted pos 2 :64 kbps Restricted pos 3 :3.1 kHz Audio pos 4 :Speech pos 5 :7 kHz Audio pos 6 :16 kbit/s unrestr. digital
mxTrunkTable	.1.3.6.1.4.1.11268.2.8.1.2.2.2.2	A table with trunk interfaces data.
mxTrunkEntry	.1.3.6.1.4.1.11268.2.8.1.2.2.2.2.1	Internal use. No information is provided.
mxTrunkIndex	.1.3.6.1.4.1.11268.2.8.1.2.2.2.2.1.1	A unique value for each interface. Its value is calculated as: X=route number, Y=lim number, Z=trunk individual within lim and route. $mxTrunkIndex = (X * 2097152) + (Y * 4096) + Z$
mxTrunkId	.1.3.6.1.4.1.11268.2.8.1.2.2.2.2.1.2	Trunk line number. Server and sequence number for the external line.
mxTrunkRouteNo	.1.3.6.1.4.1.11268.2.8.1.2.2.2.2.1.3	The route number. Linkin to mxRouteTable.
mxTrunkWhere	.1.3.6.1.4.1.11268.2.8.1.2.2.2.2.1.4	EQU position. Note that EQU is not presented to SIP trunks.
mxTrunkDescr	.1.3.6.1.4.1.11268.2.8.1.2.2.2.2.1.5	Trunk type. See MML TYPE of interface.
mxTrunkAddDescr	.1.3.6.1.4.1.11268.2.8.1.2.2.2.2.1.6	Future development. A textual string containing information about the remote end.

	OID	Description
mxTrunkOperStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.2.1.7	The traffic state of the interface (idle, busy, blocked, unknown).

5.4.2.2 Operator or attendant information

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).aastra(11268).aastraMibs(2).aastraOidMx-one(8).tsAlarm(1).tsObjects(2).mxlInterfaces(2).mxlfOperator(3)

	OID	Description
mxlfOperator	.1.3.6.1.4.1.11268.2.8.1.2.2.3	
mxOpiTable	.1.3.6.1.4.1.11268.2.8.1.2.2.3.1	A table with attendant / operator data.
mxOpiEntry	.1.3.6.1.4.1.11268.2.8.1.2.2.3.1.1	Internal use. No information is provided.
mxOpiIndex	.1.3.6.1.4.1.11268.2.8.1.2.2.3.1.1.1	A unique value for each Attendant / Operator.
mxOpiDirno	.1.3.6.1.4.1.11268.2.8.1.2.2.3.1.1.2	A textual string displaying the directory number.
mxOpiType	.1.3.6.1.4.1.11268.2.8.1.2.2.3.1.1.3	Operator console type, see Type Parameter in CPI PBX Operator Traffic, OP document.
mxOpiWhere	.1.3.6.1.4.1.11268.2.8.1.2.2.3.1.1.4	Port identity, EQU position or IP address.
mxOpiDescr	.1.3.6.1.4.1.11268.2.8.1.2.2.3.1.1.5	Future development. A textual string containing information about the interface.
mxOpiAddDescr	.1.3.6.1.4.1.11268.2.8.1.2.2.3.1.1.6	Future development. A textual string containing information about the interface.
mxOpiOperStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.3.1.1.7	The operational state of the attendant (manual-absent(1), automatic-absent(2), present(3), blocked(4), unknown(5))
mxOpiBusyStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.3.1.1.8	The traffic state of the attendant (idle, busy or unknown).

5.4.2.3 Call Information Logging

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).aastra(11268).aastraMibs(2).aastraOidMx-one(8).tsAlarm(1).tsObjects(2).mxlInterfaces(2).mxlfCil(5)

	OID	Description
mxlfCil	.1.3.6.1.4.1.11268.2.8.1.2.2.5	
mxCilTable	.1.3.6.1.4.1.11268.2.8.1.2.2.5.1	A table with CIL output data.
mxCilEntry	.1.3.6.1.4.1.11268.2.8.1.2.2.5.1.1	Internal use. No information is provided.
mxCilIndex	.1.3.6.1.4.1.11268.2.8.1.2.2.5.1.1.1	A unique value for each output.
mxCilOutput	.1.3.6.1.4.1.11268.2.8.1.2.2.5.1.1.2	A unique value for each output. Its value is a string in format XXX-Y. XXX = MX-ONE Service Node number, Y =output number.
mxCilType	.1.3.6.1.4.1.11268.2.8.1.2.2.5.1.1.3	Type of storage.
mxCilSubtype	.1.3.6.1.4.1.11268.2.8.1.2.2.5.1.1.4	Subtype of storage.
mxCilDbName	.1.3.6.1.4.1.11268.2.8.1.2.2.5.1.1.5	Path or device for the storage.
mxCilServer	.1.3.6.1.4.1.11268.2.8.1.2.2.5.1.1.6	Storage server information.

	OID	Description
mxCilOperStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.5.1.1.7	The operational state of the interface (up, down or unknown). The unknown(3) state indicates that the agent can't get the status of the interface. The interface can then be either up or down.

5.4.2.4

CSTA I and CSTA III information

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).aastra(11268).aastra-Mibs(2).aastraOidMx-one(8).tsAlarm(1).tsObjects(2).mxInterfaces(2).mxIfCsta(6)

	OID	Description
mxIfCsta	.1.3.6.1.4.1.11268.2.8.1.2.2.6	
mxCti1Table	.1.3.6.1.4.1.11268.2.8.1.2.2.6.1	A table with CSTA I data.
mxCti1Entry	.1.3.6.1.4.1.11268.2.8.1.2.2.6.1.1	Internal use. No information is provided
mxCti1Index	.1.3.6.1.4.1.11268.2.8.1.2.2.6.1.1.1	A unique value for each link group.
mxCti1Group	.1.3.6.1.4.1.11268.2.8.1.2.2.6.1.1.2	CSTA group name.
mxCti1Lim	.1.3.6.1.4.1.11268.2.8.1.2.2.6.1.1.3	MX-ONE Service Node number where the interface is initiated.
mxCti1Ip	.1.3.6.1.4.1.11268.2.8.1.2.2.6.1.1.4	MX-ONE Service Node IP address where CSTA is initiated.
mxCti1OperStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.6.1.1.5	The operational state of the interface (up, down, faulty, unknown). The unknown state indicates that the agent can't get the status of the interface. The interface can then be either up or down
mxCti3Table	.1.3.6.1.4.1.11268.2.8.1.2.2.6.2	A table with CSTA III data
mxCti3Entry	.1.3.6.1.4.1.11268.2.8.1.2.2.6.2.1	Internal use. No information is provided.
mxCti3Index	.1.3.6.1.4.1.11268.2.8.1.2.2.6.2.1.1	Internal use. No information is provided.
mxCti3Type	.1.3.6.1.4.1.11268.2.8.1.2.2.6.2.1.2	Information of type of protocol used for this interface. ASN1 or XML.
mxCti3Lim	.1.3.6.1.4.1.11268.2.8.1.2.2.6.2.1.3	MX-ONE Service Node number where the interface is initiated.
mxCti3Ip	.1.3.6.1.4.1.11268.2.8.1.2.2.6.2.1.4	IP address, only presented if the Service is up.
mxCti3Port	.1.3.6.1.4.1.11268.2.8.1.2.2.6.2.1.5	Port number.
mxCti3OperStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.6.2.1.6	The operational state of the interface (UnInitialized, Initialized, Enabled, Disabled, NotExist) . The unknown state indicates that the agent can't get the status of the interface. The interface can then be either up or down

5.4.2.5

System Computer information (ICU):

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).aastra(11268).aastra-Mibs(2).aastraOidMx-one(8).tsAlarm(1).tsObjects(2).mxInterfaces(2).mxIfGici(7)

	OID	Description
mxIfGici	.1.3.6.1.4.1.11268.2.8.1.2.2.7	

	OID	Description
mxIcuTable	.1.3.6.1.4.1.11268.2.8.1.2.2.7.1	A table with Information System Computer connections.
mxIcuEntry	.1.3.6.1.4.1.11268.2.8.1.2.2.7.1.1	Internal use. No information is provided.
mxIcuIndex	.1.3.6.1.4.1.11268.2.8.1.2.2.7.1.1.1	A unique value for each information system.
mxIculfclnd	.1.3.6.1.4.1.11268.2.8.1.2.2.7.1.1.2	Information computer individual (Ifcind).
mxIcuType	.1.3.6.1.4.1.11268.2.8.1.2.2.7.1.1.3	Information of type of interface (IFC-initiated, ICS, VS-F, EM, ACD-MIS, ANCD, Unknown).
mxIcuInterface	.1.3.6.1.4.1.11268.2.8.1.2.2.7.1.1.4	Type of interface. e.g. V.24 or Ethernet.
mxIcuLim	.1.3.6.1.4.1.11268.2.8.1.2.2.7.1.1.5	MX-ONE Service Node number where the information system computer is connected. Not used =0.
mxIcuInfo	.1.3.6.1.4.1.11268.2.8.1.2.2.7.1.1.6	IP address, port number or V.24 data.
mxIcuOperStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.7.1.1.7	The operational state of the interface. The unknown(3) state indicates that the agent can't get the status of the interface. The interface can then be either up or down, also used for generic type.

5.4.2.6

Gateways Information

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).aastra(11268).aastra-Mibs(2).aastraOidMx-one(8).tsAlarm(1).tsObjects(2).mxInterfaces(2).mxIfSwitch(9)

	OID	Description
mxIfSwitch	.1.3.6.1.4.1.11268.2.8.1.2.2.9	
mxMgwTable	.1.3.6.1.4.1.11268.2.8.1.2.2.9.1	A table with Information System Computer connections.
mxMgwEntry	.1.3.6.1.4.1.11268.2.8.1.2.2.9.1.1	Internal use. No information is provided.
mxMgwIndex	.1.3.6.1.4.1.11268.2.8.1.2.2.9.1.1.1	A unique value for each information system.
mxMgwWhere	.1.3.6.1.4.1.11268.2.8.1.2.2.9.1.1.2	Information computer individual (Ifcind).
mxMgwType	.1.3.6.1.4.1.11268.2.8.1.2.2.9.1.1.3	Information of type of interface (IFC-initiated, ICS, VS-F, EM, ACD-MIS, ANCD, Unknown).
mxMgwDescr	.1.3.6.1.4.1.11268.2.8.1.2.2.9.1.1.4	Type of interface. e.g. V.24 or Ethernet.
mxMgwOperStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.9.1.1.5	The operational state of the interface. The unknown(3) state indicates that the agent can't get the status of the interface. The interface can then be either up or down.
mxGateWayTable	.1.3.6.1.4.1.11268.2.8.1.2.2.9.2	A table with media gateway data.
mxGateWayEntry	.1.3.6.1.4.1.11268.2.8.1.2.2.9.2.1	Internal use. No information is provided.
mxGateWayIndex	.1.3.6.1.4.1.11268.2.8.1.2.2.9.2.1.1	A unique value for each interface.
mxGateWayType	.1.3.6.1.4.1.11268.2.8.1.2.2.9.2.1.2	Information of type of interface for this interface, e.g. MGU, LSU_E or MS.
mxGateWayWhere	.1.3.6.1.4.1.11268.2.8.1.2.2.9.2.1.3	IPLU Board position (EQU) is presented when Type = LSU_E. If MGU or MS is used NO_LS_MULTIPLE is presented.
mxGateWayDescr	.1.3.6.1.4.1.11268.2.8.1.2.2.9.2.1.4	IP address of the gateway board.

	OID	Description
mxGateWayOperStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.9.2.1.5	The operational state of the interface. The unknown(3) state indicates that the agent can't get the status of the interface. The interface can then be either up or down.

5.4.2.7

Group Switch Information

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).aastra(11268).aastra-Mibs(2).aastraOidMx-one(8).tsAlarm(1).tsObjects(2).mxInterfaces(2).mxIfInterlim(10)

	OID	Description
mxIfInterlim	.1.3.6.1.4.1.11268.2.8.1.2.2.10	
mxGjuTable	.1.3.6.1.4.1.11268.2.8.1.2.2.10.1	A table with GJU data.
mxGjuEntry	.1.3.6.1.4.1.11268.2.8.1.2.2.10.1.1	Internal use. No information is provided.
mxGjuIndex	.1.3.6.1.4.1.11268.2.8.1.2.2.10.1.1.1	A unique value for each interface. Format XXXYYYYY, where XXXX = Telephony Server, YYYYY =switchposition
mxGjuType	.1.3.6.1.4.1.11268.2.8.1.2.2.10.1.1.2	Information of type of both local and remote end e.g. GJU-L to GJU-L, GJU-L to GJU-G or GJU-L not connected.
mxGjuWhere	.1.3.6.1.4.1.11268.2.8.1.2.2.10.1.1.3	Board position of GJU-L.
mxGjuRemote	.1.3.6.1.4.1.11268.2.8.1.2.2.10.1.1.4	Remote end position.
mxGjuAddDescr0	.1.3.6.1.4.1.11268.2.8.1.2.2.10.1.1.5	A textual string containing information about the interface connection side 0.
mxGjuAddDescr1	.1.3.6.1.4.1.11268.2.8.1.2.2.10.1.1.6	A textual string containing information about the interface connection side 1.
mxGjuOperStatus0	.1.3.6.1.4.1.11268.2.8.1.2.2.10.1.1.7	A textual string containing information about the status of the interface side 0.
mxGjuOperStatus1	.1.3.6.1.4.1.11268.2.8.1.2.2.10.1.1.8	A textual string containing information about the status of the interface side 1.
mxGsmTable	.1.3.6.1.4.1.11268.2.8.1.2.2.10.2	A table with GSM data.
mxGsmEntry	.1.3.6.1.4.1.11268.2.8.1.2.2.10.2.1	Internal use. No information is provided.
mxGsmIndex	.1.3.6.1.4.1.11268.2.8.1.2.2.10.2.1.1	A unique value for each GSM starts at 1.
mxGsmWhere	.1.3.6.1.4.1.11268.2.8.1.2.2.10.2.1.2	GSM number.
mxGsmSyncCtrl	.1.3.6.1.4.1.11268.2.8.1.2.2.10.2.1.3	Clock status of GSM.
mxGsmAStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.10.2.1.4	Operational state of the group Switch side A
mxGsmBStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.10.2.1.5	Operational state of the group Switch side B
mxGsmActiveSide	.1.3.6.1.4.1.11268.2.8.1.2.2.10.4.0	The active side of a group Switch -side0 or side1.

5.4.2.8

CAS Boards information

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).aastra(11268).aastraMibs(2).aastraOidMx-one(8).tsAlarm(1).tsObjects(2).mxInterfaces(2).mxIfCasBoards(12)

	OID	Description
mxIfCasboards	.1.3.6.1.4.1.11268.2.8.1.2.2.12	

	OID	Description
mxCasBoardTable	.1.3.6.1.4.1.11268.2.8.1.2.2.12.1	A table with CAS boards data.
mxCasBoardEntry	.1.3.6.1.4.1.11268.2.8.1.2.2.12.1.1	Internal use. No information is provided.
mxCasBoardIndex	.1.3.6.1.4.1.11268.2.8.1.2.2.12.1.1.1	A unique value for each interface.
mxCasBoardData	.1.3.6.1.4.1.11268.2.8.1.2.2.12.1.1.2	Type of configuration, corresponds to the EL7 ICAT configuration see command EXTEI.
mxCasBoardWhere	.1.3.6.1.4.1.11268.2.8.1.2.2.12.1.1.3	The equipment position of the CAS board.
mxCasBoardDirno	.1.3.6.1.4.1.11268.2.8.1.2.2.12.1.1.4	A textual string directory number.
mxCasBoardOperStatus	.1.3.6.1.4.1.11268.2.8.1.2.2.12.1.1.5	The operational state of the interface (idle, busy, blocked, unknown). The unknown(3) state indicates that the agent can't get the status of the interface. The interface can then be either up or down.

5.4.3

TRAPS

The table below shows the IODs that are available in the mxTraps.

One trap is sent when MX-ONE status for one of these objects is changed.

	OID	Description
mxIfTrap	.1.3.6.1.4.1.11268.2.8.1.2.3	
mxObjectBackupStatusChange	.1.3.6.1.4.1.11268.2.8.1.2.3.1	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxLimBackupStatus, *)
mxObjectTrunkChange	.1.3.6.1.4.1.11268.2.8.1.2.3.2	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxTrunkIndex, *)
mxObjectOpiChange	.1.3.6.1.4.1.11268.2.8.1.2.3.3	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxOpilIndex, *)
mxObjectCilChange	.1.3.6.1.4.1.11268.2.8.1.2.3.4	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxCilIndex, *)
mxObjectCti1Change	.1.3.6.1.4.1.11268.2.8.1.2.3.5	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxCti1Index, *)
mxObjectCti3Change	.1.3.6.1.4.1.11268.2.8.1.2.3.6	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxCti3Index, *)
mxObjectlcuChange	.1.3.6.1.4.1.11268.2.8.1.2.3.7	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxlculIndex, *)

	OID	Description
mxObjectMgwChange	.1.3.6.1.4.1.11268.2.8.1.2.3.8	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxMgwIndex, *)
mxObjectGatewayChange	.1.3.6.1.4.1.11268.2.8.1.2.3.9	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxGateWayIndex, *)
mxObjectGjuChange	.1.3.6.1.4.1.11268.2.8.1.2.3.10	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxGjuIndex, *)
mxObjectGsmChange	.1.3.6.1.4.1.11268.2.8.1.2.3.11	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxGsmIndex, *)
mxObjectGsmSideChange	.1.3.6.1.4.1.11268.2.8.1.2.3.12	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxGsmActiveSide, *)
mxObjectVcuChange	.1.3.6.1.4.1.11268.2.8.1.2.3.13	Obsolete, VCU is not supported. This trap was sent when MX-ONE status for this object was changed. The following information was presented: mxVcuIndex, *)
mxObjectCasBoardChange	.1.3.6.1.4.1.11268.2.8.1.2.3.14	This trap is sent when MX-ONE status for this object is changed. The following information is presented: mxCasBoardIndex, *)

*) Additionally, the following information is also presented mxObjectStatus, mxal-Handle, mxalFrom, mxalFaultCode, mxalSeverity, mxalWhere, mxalExplanation, mxal-Noticed, mxalNoticedNote.

5.5 SUPPORT OF MITEL ERN MIB

The definitions are found in an installed system at:

/usr/share/snmp/mibs/MITEL-MIB.txt and /usr/share/snmp/mibs/MITEL-ERN-MIB.txt.

Implementation in program unit ESNMP.

5.5.1 SYSTEM STATUS

5.5.1.1 Supported Objects in MITEL ERN MIB

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).mitel(1027). mitelProprietary (4). mitelPropApplications (1). mitelAppCallServer(1)

	OID	Description
mitelCsEmergencyResponse	1.3.6.1.4.1.1027.4.1.1.3	The branch to support ER Adviser.

	OID	Description
mitelCsErSeqNumber	.1.3.6.1.4.1.1027.4.1.1.3.1	Sequence number, assigned for each new emergency call since last (re-)start.
mitelCsErCallType	.1.3.6.1.4.1.1027.4.1.1.3.2	Always 1.
mitelCsErDetectTime	.1.3.6.1.4.1.1027.4.1.1.3.3	Time of the emergency call in local time.
mitelCsErCallingDN	.1.3.6.1.4.1.1027.4.1.1.3.4	The DN of the device used to place the emergency call.
mitelCsErCallingPNI	.1.3.6.1.4.1.1027.4.1.1.3.5	The Primary Node ID for the caller. E.g "Lim x", where x is the service node number.
mitelCsErCesidDigits	.1.3.6.1.4.1.1027.4.1.1.3.6	The ELIN/CESID from the calling device if applicable.
mitelCsErDialledDigits	.1.3.6.1.4.1.1027.4.1.1.3.7	The number dialed, typically 911 is the US.
mitelCsErRegistrationDN	.1.3.6.1.4.1.1027.4.1.1.3.8	Extension number of the device that made the call.
mitelCsErUnackTableIndex	.1.3.6.1.4.1.1027.4.1.1.3.9.1	The index of the row for the Manager to acknowledge the notification.
mitelCsErUnackTableToken	.1.3.6.1.4.1.1027.4.1.1.3.9.2	The status of this row. Normally 1.

5.5.2 TRAPS

	OID	Description
mitelCsErNotification	.1.3.6.1.4.1.1027.4.1.1.3.401	A new trap is sent for each new emergency call, and repeated every two minutes, for two hours, if not cleared. In the trap following data is presented: mitelCsErSeqNumber, mitelCsErCallType, mitelCsErDetectTime, mitelCsErCallingDN, mitelCsErCallingPNI, mitelCsErCesidDigits, mitelCsErDialledDigits, mitelCsErRegistrationDN, mitelCsErUnackTableIndex, mitelCsErUnackTableToken.

5.5.3 SUPPORTED WRITEABLE OBJECTS IN MITEL ERN MIB

In the MX-ONE Service Node, following objects in the MITEL ERN MIB are supported with write-only access.

	OID	Description
mitelCsErUnackTable	.1.3.6.1.4.1.1027.4.1.1.3.9.1.2.0	
mitelCsErUnackTableToken	.1.3.6.1.4.1.1027.4.1.1.3.9.1.2.0-63	Remove repetitive sending of emergency traps, by writing the integer received by the NMS in the mitelCsErSeqNumber in the mitelCsErNotification trap.

6

CONFIGURATION

SNMP is preconfigured at installation and can be reconfigured by editing the configuration files in the */etc/snmp* directory, or by the tools provided in the distribution (*/usr/bin/snmpconf*).

Configurations file are found at path: */etc/snmp/*

Example files are found at path: */opt/eri_sn/etc/templates*

Other binary files: */opt/eri_sn/bin/snmpAction.pl*

Optional binary file: */usr/bin/traptoemail*

6.1

CONFIGURATION OF THE SNMP DAEMON

The SNMP agent used in the MX-ONE Service Node is a daemon called *snmpd*, the associated configuration file is */etc/snmp/snmpd.conf*.

The *snmpd* agent must be forced to reread the configuration file after it has been updated by command ***/etc/init.d/snmpd reload***.

6.1.1

SYSTEM INFORMATION

The agent is configured to fit the installation by editing the configuration file. At a minimum, the following entries should be updated in every LIM:

- *syslocation* – Physical location of the system
- *syscontact* – Contact information for the administrator of the system

6.1.2

COMMUNITY SETTINGS

In most cases the default community settings should be changed to prevent easy access to the net-snmp agent.

- *rwcommunity* – The community name to allow write access
- *rocommunity* – The community name to allow read access

6.1.3

ADDITIONAL TRAP-SENDING CONFIGURATION

If external trap monitoring is required, change the configuration file as follows:

- *trap2sink* – More than one trap monitoring system can be defined (one per line).
- *trapsink* – More than one trap monitoring system can be defined (one per line).
- *trapcommunityname* – The community name that will accompany the sent trap.

At installation the default *trap2sink* is defined to *localhost*, thus, sending all traps to the *snmptrapd* running on the same MX-ONE node.

If the *snmptrapd* functionality to send mail or SMS is not required (as mentioned below), then delete the default line containing *localhost*.

Additional *trap2sinks* may be added to send information to several trap monitors or management systems. This is done by adding one line for each new trap monitor or management system.

If the system needs to have a common trap sender set the `trap2sink` in all lims to the same address, e.g.: `lim 1`. Then let the `snmptrapd` daemon in `lim 1` forward (proxy) the traps to network management centre.

6.1.4 ADDITIONAL SNMP TRAPS

The default setup of the `net-snmp` daemon sends a trap at startup (cold start), and traps if authentication fails.

Additional traps like disk monitoring can be enabled by changing the configuration by editing the `/etc/snmp/snmpd.conf` file, see manual pages `man snmpd.conf`.

6.2 CONFIGURATION OF ALARM NOTIFICATION USING E-MAIL AND SMS

The MX-ONE Service Node can be configured to send alarm notifications by e-mail or directly or via Short Messaging Service (SMS). The notices are based on the SNMP daemon `snmptrapd`. The daemon receives and logs SNMP TRAP messages, then translates them into an e-mail format. A public e-mail to SMS server can be used to forward the notification to a mobile phone using SMS.

6.3 ENABLING MAIL FROM SNMP TRAPS

Mail notification is configured by editing the `/etc/snmp/snmptrapd.conf` file. Enter the destination e-mail address(es) for the notifications after uncommenting the desired trap(s).

For additional information regarding configuration of this feature, type: `man snmptrapd.conf`.

To start the daemon run `chkconfig snmptrapd on` to enable service to be started at next boot, and use command `/etc/init.d/snmptrapd start` to start the service after configuration is complete.

6.4 PROXY TRAPS TO THE SAME DESTINATION

If network management centre requires only one trappingsender from the system use the `snmptrapd` proxy functionality.

Set the `trap2sink` in all lims to `lim 1` address in the `/etc/snmp/snmpd.conf` file.

Configure the `/etc/snmp/snmptrapd.conf` file in `lim 1` to include "forward default DESTINATION". DESTINATION is the address of the network management centre.

Disable the `snmptrapd` daemon in all lims except in `lim 1`.

6.5 DISABLING TRAP DAEMON

If the `snmptrapd` functionality to send mail or SMS is not required, then delete any line in the `trap2sink` section, containing `localhost` in the `/etc/snmp/snmptrapd.conf` file.

Stop the service by `chkconfig snmptrapd off`, and `/etc/init.d/snmptrapd stop`.

6.6

RESTART TRAP DAEMON

Use command `/etc/init.d/snmptrapd restart` to restart the service when reconfiguration is done.

7

VERIFY THE INSTALLATION

1. Verify that these files exist depending on what MIBs are used:
2. Alarms using Ericsson MIBs.
`/usr/share/snmp/mibs/Ericsson-DNA-SNMP-MIB.txt`
`/usr/share/snmp/mibs/Ericsson-MD110-SNMP-MIB.txt`
3. Alarm and status using Mitel (Aastra) alarm MIBs.
`/usr/share/snmp/mibs/MX-ONE-TS-ALARM-MIB.txt`
4. Emergency call events using Mitel ERN MIBs.
`/usr/share/snmp/mibs/MITEL-MIB.txt`
`/usr/share/snmp/mibs/MITEL-ERN-MIB.txt`
5. Verify the `/etc/snmp/snmp.conf` file:
 Check that the following entries are present.
`mibs +Ericsson-DNA-SNMP-MIB:Ericsson-MD110-SNMP-MIB`
`mibs +MX-ONE-TS-ALARM-MIB`
`mibs +MITEL-MIB`
`mibs +MITEL-ERN`
6. Verify started net-snmp daemons.
 Check status of the daemons
`# chkconfig snmp`
`# chkconfig snmptrap`
 If a daemon is not running use command `chkconfig xxxx on` to enable service to be started at next boot, and use `command /etc/init.d/xxxx start` to start the service.

8

USING NET-SNMP TOOLS TO CHECK ALARMS

By use of command **snmpwalk**, you can perform a check to see if the daemon is running and in contact with the ALSNMP/AALSNMP program(s).

8.1

VERIFYING THE DEPRECATED ERICSSON MIB

Use command *alarm -i* to create a test alarms with different severities.

E.g. *alarm -i -C 666 -D 1 --alarm-severity 4 --alarm-text "Test alarm"\
--faulty-lim 1 --add-text "I did this"*

snmpwalk -v 2c -c public -m all localhost 1.3.6.1.4.1.193.8

At least the *md110Release* and *mdAlarmStatus* objects should be printed, and optionally any *activeAlarms* object.

Use command *alarm -e* to remove alarm when ready.

E.g. *alarm -e -C 666 -D 1*

8.2

VERIFYING THE MITEL ALARM AND STATUS MIB

Use command *alarm -i* to create a test alarms with different severities.

E.g. *alarm -i -C 666 -D 1 --alarm-severity 4 --alarm-text "Test alarm"\
--faulty-lim 1 --add-text "I did this"*

Use command *alarm -e -C 666 -D 1*

snmpwalk -v 2c -c public -m all localhost 1.3.6.1.4.1.11268.2.8.1.1.1 will only print active alarms.

Use command *alarm -e* to remove alarm when ready.

E.g. *alarm -e -C 666 -D 1*

See also the commands: **snmpget**, **snmpgetnext**, and **snmptable**.

8.3

VERIFYING ALARM AND STATUS TRAP SENDING

To verify that the alarms are forwarded you may use alarm commands to create, change and remove alarm.

Hints where to check:

- /var/log/messages*
- /var/log/net-snmp.log*
- /var/log/mail*

8.3.1

EXAMPLE

Use command *alarm -i* to create a test alarms with different severities.

alarm -i -C 666 -D 1 --alarm-severity 4 --alarm-text "Test alarm"

```
--faulty-lim 1 --add-text "I did this"
```

Use command *alarm -p* to verify that the alarm exist, and to get the alarm handle.

```
alarm -p -C 666 -D 1
```

Check that a trap was sent to management system and/or mail system.

Use command *alarm_noticed --alarm-handle XX* to change noticed state of the alarm.

```
alarm_noticed --alarm-handle XX
```

Check that a trap was sent to management system and/or mail system.

Use command *alarm -e --alarm-handle XX* to remove alarm.

```
alarm -e --alarm-handle XX
```

Check that a trap was sent to management system and/or mail system.

8.4

VERIFYING EMERGENCY CALL EVENT TRAP SENDING

You may need to start the snmptrapd daemon to get the traps printed to the net-snmp.log.

Hints where to check: /var/log/net-snmp.log

8.4.1

EXAMPLE

Make an emergency call (E.g. 112 or 911 call).

You may need to initiate an alternative destination with a different number to test the feature.

Be sure that the destination is initiated with the ADC D26=1 set to trigger the emergency call event trap sending.

Check that a trap was received at the management system and/or mail system.

Use command: "*diagnostic_print -lim ALL -unit ESNMP -request 2*" to print the list of emergency events to verify that the call is in the list.

Use command: "*snmpset -v1 -c <auth> <pbx-ip>*

.1.3.6.1.4.1.1027.4.1.1.3.9.1.2.<mitelCsErUnackTableIndex> i <mitelCsErSeqNumber>" to remove one entry from the list.

Use command: "*diagnostic_print -lim ALL -unit ESNMP -request 2*" to print the list of emergency events to verify the removed entry is gone.

Additional tests with calls should be done per lim.

Also check that the repetition is done by delaying the snmpset command.

Remove the entry from the list by procedure in the NMS application.