Configuring RMON and SNMP

SYSTEM ADMINISTRATOR GUIDE

Copyright

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.
NetOp	is a trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 About SNMP

The Simple Network Management Protocol (SNMP) allows you to monitor network devices from a central location. This section provides an overview of SNMP.

SNMP defines the standards used to monitor one or more network devices.

An SNMP management system contains the following parts:

- One or more SNMP agents
- SNMP Manager (entity containing command generator or notification receiver applications)
- Protocol to communicate information between the SNMP agent and manager entities.

  The following are examples of protocols SNMP uses to communicate between entities:

  - Trap notifications—for example, traps and events
  - Get requests
  - Set requests
  - Management Information Bases (MIBs)

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **`Product Overview`** folder of this Customer Product Information library.

1.1 MIBs

The Management Information Base (MIB) is a virtual database of defined objects used to manage network devices. MIB objects are organized hierarchically and each object has a unique object identifier (OID). You can read and write objects to obtain information about a network by using a network-management protocol, such as SNMP. For a list of SNMP standards, see the SNMP Management Framework and RFCs section. For information about Standard MIB support, see *Standard SNMP MIBs*.

The SmartEdge router supports enterprise-specific MIBs and standard MIBs defined by Ericsson and standard MIBs defined by standards bodies, such as the Internet Engineering Task Force (IETF), International Telecommunications Union (ITU), and Institute of Electrical and Electronics Engineers, Inc. (IEEE). For information about the enterprise-specific MIBs (including the OIDs), see *Enterprise MIBs*.

OIDs are identifiable by numbers. These numbers represent the hierarchy of the object in the MIB. For example, all Ericsson proprietary MIBs start with the OID syntax 1.3.6.1.4.1.2352.2.***xyz***. This syntax indicates that .xyz is located in the MIB hierarchy in the following way (numbers in parentheses show their placement in the MIB hierarchy; however, in the system, MIB OIDs are displayed as numbers only):

The following example shows the hierarchy of the MIB.

```
iso(1).org(3).dod(6).internet(1).private(4).enterprises
(1).redBackNetworks(2352).rbnMgmt(2).xyz
```

You can also identify an object by its object name. For example, ifNumber in IF-MIB can be identified by its object name (iso.org.dod.internet.mgmt.enterprises.interfaces.ifNumber) or OID (1.3.6.1.2.1.2.1). This document identifies OIDs by object names and numerical format.

1.2 Capability Statements

Enterprise MIBs updates are documented in capability statements (CAP files), organized by software release (similar to a revision history). Standard MIB CAP files are identified as RBN-IETF-<name>-CAP.my.

1.3 Notifications

An SNMP agent sends notifications to a network manager when certain system events occur. A standard or proprietary MIB defines these notifications, also called traps or events. Notifications are defined in various standard and enterprise-specific MIB modules. For more information about notifications used in the SmartEdge router, see *SNMP MIB Notifications.*

Examples of notifications that can occur in the SmartEdge router include:

- A card restarts
- An XCRP is replaced

- The system reaches too high a temperature

See Configure SNMPv1 and SNMPv2 or Configure SNMPv3 for instructions on how to enable notifications on the SmartEdge router . Use the **`snmp-server host`** command to specify whether to send SNMP notifications as traps or informs (informational notifications).

1.4 SNMP Management Framework and RFCs

The following components and standards documents define the SNMP management framework:

- Overall architecture—Described in RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*

- Mechanisms for describing and naming objects and events for the purpose of management:

  The first version, Structure of Management Information (SMIv1) as described in:

  - STD 16, RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*
  - STD 15, RFC 1157, *A Simple Network Management Protocol (SNMP)*
  - STD 16, RFC 1212, *Concise MIB Definitions*
  - RFC 1215, *Convention for Defining Traps for Use with the SNMP*

  The second version, SMIv2, as described in:

  - STD 58, RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
  - STD 58, RFC 2579, *Textual Conventions for SMIv2*
  - STD 58, RFC 2580, *Conformance Statements for SMIv2*
  - RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*
  - RFC 1901, *Introduction to Community-based SNMPv2*

  SNMP Version 3 (SNMPv3):

  - STD 62, RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*
  - RFC 3411, *An Architecture for Describing SNMP Management Frameworks*

  - RFC 3412 *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*

  - RFC 3413 *SNMPv3 Applications*

  - RFC 3414 *User-based Security Model (USM) for version 33 of the Simple Network Management Protocol (SNMPv3)*

  - RFC 3415 *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

  - RFC 3416 *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

  - RFC 3417 *Transport Mappings for the Simple Network Management Protocol (SNMP)*

  - RFC 3418 *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

  - STD 62, RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework*

The SmartEdge router supports the User-Based Security Model (USM) and the following applications specific to RFC 3413 and RFC 3414:

- Command Responder—The SmartEdge router accepts SNMP read-class and write-class requests, performs the appropriate protocol operation, and generates a response message.

- Notification Originator—The SmartEdge router monitors the system for particular events and conditions and generates notification-class messages based on these events or conditions.

Managed objects are accessed through a virtual information store, the Management Information Base (MIB). MIB objects are defined using the mechanisms set out in the Structure of Management Information (SMI); for more information, see the MIBs section.

Other supported RFCs are:

- RFC 1155 *Structure and Identification of Management Information for TCP/IP-based Internets*

- RFC 2790 *Host Resources MIB*

- RFC 4113 *Management Information Base for the User Datagram Protocol (UDP)*

1.5 SNMP Versions

The SmartEdge router supports SNMP Version 1 (SNMPv1), Version 2c (SNMPv2), and Version 3 (SNMPv3).

There are several differences between configuring SNMPv1 and SNMPv2, and configuring SNMPv3:

- With SNMPv1 and 2c, communities are created to control access to MIB information. You can configure these communities to meet management requirements. For instance, you can set up the automatic generation of community strings for all managed Ericsson contexts. This automatically creates a group with the same name as the community string.
- With SNMPv3, groups and users (instead of communities) are manually configured to control access to MIB information. Privacy and encryption options ensure a high level of configurable security.
- SNMPv3 uses engine IDs to provide additional security.

2 Configuring RMON

To configure RMON, perform the tasks in the following sections.

2.1 Configuring RMON Features

To configure RMON features, perform the tasks described in Table 1; enter all commands in global configuration mode.

Note: You must first enable the SNMP server before you can configure RMON features.

Table 1 Configure RMON Features

#	Task	Root Command
1.	Define an RMON alarm.	*rmon alarm*
2.	Define an RMON event.	*rmon event*

2.2 Displaying RMON Information

Table 2 lists the operations tasks for SNMP and Remote Monitoring (RMON). Enter the **`show`** commands in any mode; enter all other commands in exec mode.

Table 2 SNMP Operations Tasks

Task	Root Command
Display RMON information.	*show rmon*

3 Configuring SNMP

To configure SNMP, perform the tasks in the following sections.

3.1 Configuring SNMPv1 and SNMPv2

To configure SNMPv1 and SNMPv2 for SNMP target management stations, such as the NetOp Element Management System (EMS) server, perform the tasks described in Table 3; enter all commands in global configuration mode unless otherwise noted.

Table 3 Configure SNMPv1 and SNMPv2

#	Task	Root Command	Notes
1.	Enable the SNMP server and access SNMP server configuration mode.	*snmp server*	
2.	Specify operational attributes for the server:		
	Enable or disable per-context filtering of SNMP reporting.	*context-filter ifmib*	Enter this command in SNMP server configuration mode.
	Enable or disable linkUp and linkDown notifications for Cisco High-Level Data Link Control (HDLC), Point-to-Point Protocol (PPP), and Frame Relay encapsulation layers, IP layers, or Layer 2 Tunneling Protocol (L2TP) tunnels.	*traps (SNMP server configuration)*	Enter this command in SNMP server configuration mode.
	Create additional SNMP MIB views.	*snmp view*	
	Create SNMP community strings.	*snmp community*	Enter this command multiple times to create multiple community strings.
	Configure an SNMP target management station to receive SNMP notifications, and optionally specify the context from which notifications are sent.	*snmp target*	

Table 4 lists the operations tasks for SNMP and Remote Monitoring (RMON). Enter the **show** commands in any mode; enter all other commands in exec mode.

Table 4 SNMP Operations Tasks

Task	Root Command
Display SNMP configuration.	*show configuration snmp*

3.2 Example: Using SNMPv2

In the following SNMPv2 example, the view **Inet-View** includes all objects in the Internet object identifier (OID) tree. The **Admin** community allows read access to the **Inet-View** view, and then the SmartEdge router is configured to send traps to a system, **NM-Station1**, with an IP address of **198.164.190.110:**

```
[local]Redback(config)#snmp server
[local]Redback(config-snmp-server)#traps ifmib encaps
[local]Redback(config-snmp-server)#exit
[local]Redback(config)#snmp view Inet-View internet included
[local]Redback(config)#snmp community Admin view Inet-View read-only
[local]Redback(config)#snmp target NM-Station1 198.164.190.110
security-name Admin version 2c view Inet-View trap
[local]Redback(config)#end
```

3.3 Configuring SNMPv3

Follow these guidelines to maximize security and ensure proper configuration of SNMPv3 for SNMP target management stations such as the NetOp EMS server:

- Define unique engine IDs—Do not define the engine ID value in a configuration file that will be applied to multiple systems.
- Protect configuration files—If you create configuration files that contain security information, such as authorization passwords and keys, the files should be stored on a secured system.
- Do not use saved configurations on multiple systems—SNMP security data is system-dependent. You compromise security if the same SNMP security data is assigned to multiple systems.

To configure SNMPv3, perform the tasks described in Table 5; enter all commands in global configuration mode, unless otherwise noted.

Table 5 Configure SNMPv3

#	Task	Root Command	Notes
1.	Enable the SNMP server and access SNMP server configuration mode.	*snmp server*	
2.	Specify operational attributes for the server:		
	Enable or disable per-context filtering of SNMP reporting.	*context-filter ifmib*	Enter this command in SNMP server configuration mode.
	Enable linkUp and linkDown notifications for Cisco HDLC, PPP, and Frame Relay encapsulation layers, IP layers, or L2TP tunnels.	*traps (SNMP server configuration)*	Enter this command in SNMP server configuration mode.
	Specify a unique engine ID for local or remote systems.	*snmp engine-id*	A remote engine ID is required to identify an SNMP target when using SNMPv3.
	Create additional SNMP MIB views.	*snmp view*	
3.	Create an SNMP group.	*snmp group*	Enter this command multiple times to create multiple groups.
4.	Create an SNMP user.	*snmp user*	Enter this command multiple times to create multiple users.
5.	Configure an SNMP target management station, and optionally specify the context from which notifications are sent:[1]		
	- Option 1	*snmp target*	
	- Option 2	*snmp notify*	
		snmp notify-filter	

Table 5 Configure SNMPv3

#	Task	Root Command	Notes
		snmp target-parameters	
		snmp notify-target	You must enter the first three commands before you enter the **snmp notify-target** command.

*(1) Option 1 and Option 2 are mutually exclusive. The **snmp target** command is equivalent to the set of commands of Option 2, but only if, in step 3, the SNMP group was created without a notification view identified (the **snmp group** command with the **notifynotify-view** construct).*

3.4 Example: Using SNMPv3

The following SNMPv3 example configures the **Inet-View** view to include all objects in the Internet MIB tree. It also configures an authenticated group, **Group4**, to allow read and notify access to the **Inet-View** view, and a user, **Admin**, who is part of **Group4**, with an encoded authorization password. It also configures the SmartEdge router to send inform notifications from the **Inet-View** view to a system, **Nm-Station1** (IP address **10.3.4.5**), excluding the **rbnSRMIBNotifications** trap:

```
[local]Redback(config)#snmp server
[local]Redback(config-snmp-server)#traps ifmib encaps
[local]Redback(config-snmp-server)#exit
[local]Redback(config)#snmp engine-id local AA:00:00:00:01
[local]Redback(config)#snmp view Inet-View internet included
[local]Redback(config)#snmp group Group4 security-model usm auth read
Inet-View notify Inet-View
[local]Redback(config)#snmp user Admin group Group4 security-model usm
md5 key encoded base64 L1sR+UKZj4PqeRodf3zqTg==
[local]Redback(config)#snmp notify Notify-Inform Tag-Inform inform
[local]Redback(config)#snmp notify-filter Filter-incInet 1.3.*.4 included
[local]Redback(config)#snmp notify-filter Filter-NOrbnSRMIB
rbnSRMIBNotifications excluded
[local]Redback(config)#snmp target-parameters Param2 security-name
Admin version 3 security-level auth
[local]Redback(config)#snmp notify-target Nm-Station1 10.3.4.5/24 tag
Inet-Informs parameters Param2 filter Filter-NOrbnSRMIB
```

3.5 Displaying SNMP Statistics

Table 6 lists the operations tasks for SNMP and RMON. Enter the **`show`** commands in any mode; enter all other commands in exec mode.

Table 6 SNMP and RMON Operations Tasks

Task	Root Command
Enable the generation of SNMP debug messages.	*debug snmp*
Display commands for the SNMP.	*show configuration snmp*
Display RMON information.	*show rmon*
Display SNMP statistics, including usage, configured contexts, communities, notifications, SNMP daemon status, targets, and views.	*show snmp*

3.6 Generating SNMP Debug Messages

Table 7 lists the operations tasks for SNMP and Remote Monitoring (RMON). Enter the **`show`** commands in any mode; enter all other commands in exec mode.

Table 7 SNMP Operations Tasks

Task	Root Command
Enable the generation of SNMP debug messages.	*debug snmp*

3.7 Example: Setting SNMP Command Privileges

The following example assigns the minimum privilege level to all commands that start with the **`snmp`** keyword to **12:**

```
[local]Redback(config)#privilege config inherit level 12 snmp
```

4 Configuring MIB Information to Display OIDs in Human-Readable Form

Note: You must enable SNMP before you can perform this procedure.

To configure MIB information to display Object Identifiers (OIDs) in human-readable form, perform the following tasks. This procedure provides a general overview of how to complete this task using any MIB browser. Refer to the documentation for your MIB browser for specific details on how to perform this procedure:

1. Download and install a MIB browser.
2. Download and save the MIB definition file.
3. Add the MIB files to the MIB browser.
4. Open a MIB object to see the human-readable form of the OID.