

Configuring Communications with the NetOp EMS

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2010. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

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	Introduction	1
2	Setting Up Administrator Accounts on the Node	1
3	Configuring the Ethernet Management Port	3
4	Configuring SSL Encryption Between the Node and the NetOp EMS Server	3
5	Enabling the SSH Protocol on the Node	4
6	Enabling Communication Between the Node and the NetOp EMS Software	5
7	Enabling or Suppressing SNMP Trap Forwarding	5
8	Configuring a Node to Support Automatic Node Discovery	7
	Glossary	9





1 Introduction

In this document, SmartEdge® routers are known as "nodes."

This document describes how to configure communication settings on a node that uses the SmartEdge OS to enable remote access by the NetOp™ Element Management System (EMS) software. Communication settings must be configured on each node in your network that you want managed by the NetOp EMS software. After communications are configured and enabled, the NetOp EMS server can remotely access the node through the appropriate node proxy, and you can manage the node by using the NetOp client.

Remote access to a node is disabled by default. To enable remote access, you must modify the node configuration file. To modify the node configuration file, you must connect a terminal to the console port of the node, and open a local console session to access the SmartEdge OS Command-Line Interface (CLI).

For more information see the:

- “Connections for Management Access” section in the *SmartEdge 100 Router Hardware Guide*.
- “Access During the Initial Startup and Reload” section in the *SmartEdge 400 Router Hardware Guide*, *SmartEdge 600 Router Hardware Guide*, *SmartEdge 800 Router Hardware Guide*, or *SmartEdge 1200 Router Hardware Guide*, as appropriate.

Except where explicitly stated, this document makes the following assumptions:

- The current settings of each node corresponds to the factory settings.
To reset a previously configured node to the factory settings, remove the standard configuration file and reload the node operating system software.
- The NetOp EMS server and node proxies are installed and running.

2 Setting Up Administrator Accounts on the Node

For communication between the NetOp EMS server and a node, a dedicated administrator account must be set up on the node for the node proxy to use. To



allow remote access to the SmartEdge OS CLI to privileged users of the NetOp client, you must set up additional administrator accounts.

Use the following guidelines when setting up the administrator account for the node proxy on a node:

- The account must exist in the local context.
- If you use node groups in the NetOp EMS software to ensure consistent communications settings, use the same administrator account name and password for all nodes in the same node group.

Note: Node groups ensure consistent settings among nodes of the same type that use the same version of node operating system software. You can configure node groups before or after you configure nodes to communicate with the NetOp EMS software; for information, see “Node Group Configuration” in *NetOp EMS Software Configuration* or “Add a New Node Group” in *NetOp EMS Initial Configuration*.

Administrator accounts for privileged users of the NetOp client, to allow remote access to the SmartEdge OS CLI on the node, can be restricted by context and privilege level.

The following example displays how to set up an unrestricted administrator account `netop` with password `admin_5` in the local context and save it to the node configuration file:

```
[local]Ericsson>enable
[local]Ericsson#configure
Enter configuration commands, one per line, 'end' to exit
[local]Ericsson(config)#context local
[local]Ericsson(config-ctx)#administrator netop password admin_5
[local]Ericsson(config-administrator)#privilege start 15
[local]Ericsson(config-administrator)#commit
Transaction committed.
[local]Ericsson(config-administrator)#end
[local]Ericsson#save configuration
```

For more information on these commands, see *Command List* and *Configuring Contexts and Interfaces*.

If the node is a member of a node group, you must define the administrative account for the node proxy identically for all nodes in the same node group. For each node, record the IP address of the node, and the name and password for each administrative user account you configure. You need this information to add the node to the NetOp EMS database; see “Managing Node Inventory” in *Inventory Management* in the NetOp EMS library.



3 Configuring the Ethernet Management Port

Node software maintenance operations supported by the NetOp EMS software are managed through the Ethernet management port. In addition, the Telnet or Secure Shell (SSH) session that is initiated in the NetOp client's CLI panel is connected to this port.

The management port is configured in the local context. First you create an interface for the port to use. In this interface, you identify the IP address of the node and the route to the network gateway to the NetOp EMS server. Next, you define the port and bring up the port. Then you bind the interface to the context, which creates a logical connection that enables the physical connection through the port using the route defined by the interface.

The following example displays a management port configuration for a node:

```
[local]Ericsson>enable
[local]Ericsson#configure
Enter configuration commands, one per line, 'end' to exit
[local]Ericsson(config)#context local
[local]Ericsson(config-ctx)#interface mgmt
[local]Ericsson(config-if)#ip address 192.168.1.5/24
[local]Ericsson(config-if)#ip route 0.0.0.0/0 192.168.1.254
[local]Ericsson(config-ctx)#port ethernet 7/1
[local]Ericsson(config-port)#no shutdown
[local]Ericsson(config-port)#bind interface mgmt local
[local]Ericsson(config-port)#end
[local]Ericsson#save configuration
```

Note: 192.168.1.5 is the IP address of the node. 192.168.1.254 is the IP address of the network gateway to the NetOp EMS server.

For more information on configuring the Ethernet management port and binding an IP address to it, see *Command List* and *Configuring Contexts and Interfaces* or *Performing Basic Configuration Tasks*.

4 Configuring SSL Encryption Between the Node and the NetOp EMS Server

The connection between the NetOp EMS server and the node is secured with SSL encryption by default.



You configure the SSL encryption protocol on a node by issuing the **connection-mode** command (in netop configuration mode) with the **tls** keyword and then saving the configuration. The **unencrypted** keyword allows unencrypted connections, while the **tls** keyword allows Transport Level Security (TLS) connections. For more information about the **connection-mode** command, see *Command List*.

The following example shows how to enable the SSL protocol on a node:

```
[local]Ericsson>enable
[local]Ericsson#configure
Enter configuration commands, one per line, 'end' to exit
[local]Ericsson(config-netop)#connection-mode tls
[local]Ericsson(config-netop)#save configuration
```

The following example shows how to display whether SSL encryption is enabled on the connection between the NetOp EMS server and the node:

```
[local]Ericsson>enable
[local]Ericsson#configure
[local]Ericsson(config)#netop
[local]Ericsson(config-netop)#show netop connection-mode
```

The following example shows how to allow both SSL encrypted and unencrypted connections between the NetOp EMS server and the node:

```
[local]Ericsson>enable
[local]Ericsson#configure
[local]Ericsson(config)#netop
[local]Ericsson(config-netop)#connection-mode tls unencrypted
[local]Ericsson(config-netop)#end
[local]Ericsson#save configuration
```

The following example shows how to return to the default condition on the connection between the NetOp EMS server and the node:

```
[local]Ericsson>enable
[local]Ericsson#configure
[local]Ericsson(config)#netop
[local]Ericsson(config-netop)#no connection-mode
[local]Ericsson(config-netop)#end
[local]Ericsson#save configuration
```

5 Enabling the SSH Protocol on the Node

You enable the SSH protocol on a node by generating an SSH key on the node. Issue the **ssh server-keygen** command (in global configuration mode) and then save the configuration. For more information about the **ssh server-keygen** command, see *Command List*.



The following example displays how to enable the SSH protocol on a node:

```
[local]Ericsson#ssh server-keygen
```

6 Enabling Communication Between the Node and the NetOp EMS Software

You enable communication to the NetOp EMS software by issuing the `netop` command (in global configuration mode), and then saving the configuration. The `netop` command starts the node's NetOp EMS daemon (`netopd`), which communicates with the appropriate node proxy. To disable communication between the node and the NetOp EMS software, issue the `no netop` form of the command to shut down the `netopd` process on the node. For more information about the `netop` command, see *Command List*.

Note: If the node is rebooted, the NetOp EMS daemon is automatically restarted if you save the configuration. If you do not save the configuration, you must manually restart the NetOp EMS daemon in the local console session.

The following example displays how to enable communication between a node and the NetOp EMS software:

```
[local]Ericsson>enable
[local]Ericsson#configure
Enter configuration commands, one per line, 'end' to exit
[local]Ericsson(config)#netop
[local]Ericsson(config-netop)#end
[local]Ericsson#save configuration
```

7 Enabling or Suppressing SNMP Trap Forwarding

You enable Simple Network Management Protocol (SNMP) communication between a node and the NetOp EMS software by issuing the `snmp server` command (in global configuration mode), and then saving the configuration.



The **snmp server** command starts an SNMP server on the node that forwards SNMP traps from the node to the appropriate node proxy.

The following example enables the forwarding of SNMP traps from the node to the NetOp EMS software:

```
[local]Ericsson>enable
[local]Ericsson#configure
Enter configuration commands, one per line, 'end' to exit
[local]Ericsson(config)#snmp server
[local]Ericsson(config-snmp-server)#end
[local]Ericsson#save configuration
```

To disable SNMP communication between the node and the NetOp EMS software, issue the **no snmp** form of the command to shut down the node's SNMP server.

For more information about the **snmp server** command, see *Command List*.

By default, the node forwards SNMP Version 2c (SNMPv2c) traps. You can reconfigure the node to forward SNMP Version 1, (SNMP) or SNMP Version 3 (SNMPv3) traps instead.

To reconfigure the node to forward SNMP or SNMPv3 traps after starting the SNMP server, use the **snmp version?** command (in netop configuration mode). When prompted for the SNMP version, enter the version and save the configuration.

The following example shows how to change the version of SNMP that the node forwards to the NetOp EMS software to SNMPv3:

```
[local]Ericsson>enable
[local]Ericsson#configure
[local]Ericsson(config)#netop
[local] (config-netop)#snmp version?
  1 SNMP Protocol Version 1
  2c SNMP Protocol Version 2c (default)
  3 SNMP Protocol Version 3
[local]Ericsson(config-netop)#3
[local]Ericsson(config-netop)#end
[local]Ericsson#save configuration
```

For more information about the **snmp version** command, see *Command List*.

SNMP trap notifications are enabled by default. To suppress the forwarding of SNMP trap notifications from the node to the NetOp EMS server, use the **no snmp traps** command (in netop configuration mode) and save the configuration. The **snmp traps** command reactivates trap notifications.

The following example shows how to suppress SNMP trap forwarding from the node to the NetOp EMS server:



```
[local]Ericsson>enable
[local]Ericsson#configure
[local]Ericsson(config)#netop
[local]Ericsson(config-netop)#no snmp traps
[local]Ericsson(config-netop)# end
[local]Ericsson# save configuration
```

For more information about the `snmp traps` command, see *Command List*.

To configure SNMP using the:

- SmartEdge OS CLI , see *Configuring RMON and SNMP*.
- NetOp client, see “SNMP Configuration” in *SmartEdge and SM Node Configuration* in the NetOp EMS library.

8 Configuring a Node to Support Automatic Node Discovery

After you configure the node to communicate with the NetOp EMS software, you can also configure it to support the NetOp EMS software to discover the node automatically. You configure automatic node discovery with the `advertise` command through the CL in netop configuration mode, which enables the sending of advertisement packets from the node to the NetOp EMS server.

Note: You must also enable support for the automatic node discovery in the NetOp EMS software. For instructions, see “Automatic Node Discovery Configuration” in *NetOp EMS Software Configuration* in the NetOp EMS library.

The following example displays how to enable a node to send advertisement packets every 30 seconds to the NetOp EMS server with the IP address 192.168.1.1 and to assign it to the node group NodeGroup01:

```
[local]Ericsson>enable
[local]Ericsson#configure
[local]Ericsson(config)#netop
Enter configuration commands, one per line, 'end' to exit
[local]Ericsson(config-netop)#advertise 192.168.1.1 interval 30 node-group NodeGroup01 port 6580
[local]Ericsson(config-netop)#commit
```

When the NetOp EMS server receives a packet from the node, the NetOp EMS server connects to the node and applies the communications settings defined for the node group associated with the SmartEdge OS running on the node. The node then stops sending advertise packets. For more information about the `advertise` command, see the *Command List*.



If the configuration is reloaded, the node starts sending advertise packets again unless you issue the `no` form of the command.

Note: To view the advertisement settings, issue the `show netop advertise` command.



Glossary

CLI

Command-Line Interface

EMS

Element Management System

SNMP

Simple Network Management Protocol

SNMPv2c

SNMP Version 2c

SNMPv3

SNMP Version 3

SSH

Secure Shell

TLS

Transport Level Security