Configuring TACACS+

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 Contents of This Document

This document provides an overview of the Terminal Access Controller Access Control System Plus (TACACS+) features supported on the SmartEdge router, describes TACACS+ Attribute-Value Pairs, and describes the tasks used to configure, monitor, and administer TACACS+. This document also provides a configuration example of TACACS+.

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.

2 Overview

The TACACS+ protocol enables building a system that secures remote access to networks and network services. TACACS+ is based on a client/server architecture. When configured with the IP address or hostname of a TACACS+ server, the SmartEdge router can act as a TACACS+ client. TACACS+ servers are configured on a per-context basis, with a limit of six servers in each context.

The SmartEdge router supports the TACACS+ features of One-Time Passwords in Everything (OPIE), S/Key, and SecurID, if they are supported by and enabled on the TACACS+ server. These functions are limited to Telnet sessions only.

The SmartEdge router uses Simple Network Management Protocol (SNMP) notifications when the SmartEdge router has difficulty communicating with a TACACS+ server and declares it down and also when communication to the server is restored.

Configurable options for a TACACS+ server include:

- Time-out interval, maximum number of retries, deadtime interval
- Domain stripping of structured user names
- Authenticating of administrators and authorizing the use of specific command-line interface (CLI) commands
- Sending of accounting messages for administrator sessions and CLI command accounting records to TACACS+ servers

To enable authentication and accounting features, you must also configure authentication, authorization, and accounting (AAA). For information about AAA tasks and commands, see *Configuring Authentication, Authorization, and Accounting*.

To enable administrator authentication through TACACS+, enter the **`aaa authentication administrator`** command (in context configuration mode). To configure CLI authorization, enter the **`aaa authorization commands`** command (in context configuration mode). To enable accounting messages to be sent to a TACACS+ server, enter the **`aaa accounting administrators`** and **`aaa accounting commands`** commands (in context configuration mode).

3 Configuration and Operations Tasks

The sections that follow provide information for configuring and operating TACACS.

3.1 Configuring TACACS+

Note: In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see *Command List*.

The SmartEdge router supports up to six TACACS+ servers in each context. Servers are assigned priority based on the order in which they are configured in the operating system. The first configured server is used first. If the first server becomes unavailable or unreachable, the second server is used, and so on.

By default, the local IP address for the interface on which TACACS+ is transmitted is included in packets sent by the SmartEdge router. To not publish the IP address to the TACACS+ server, you must configure a loopback interface to appear to be the source address for TACACS+ packets. The interface must be reachable by the TACACS+ server; for details about this command, see *Configuring Contexts and Interfaces*.

To configure a TACACS+ server, perform the tasks described in Table 1; enter all commands in context configuration mode, unless otherwise noted.

Table 1 Configure a TACACS+ Server

Task	Root Command	Notes
Configure the IP address or hostname of a TACACS+ server.	*tacacs+ server*	
Optional. Configure server parameters, using one or more of the following tasks:		
Modify the interval during which the SmartEdge router is to treat a nonresponsive TACACS+ server as dead, and try instead to reach another configured server.	*tacacs+ deadtime*	
Modify the number of retransmission attempts to open a TCP connection to the TACACS+ server in the event that no response is received from the server within the time-out period.	*tacacs+ max-retries*	

Table 1 Configure a TACACS+ Server

Task	Root Command	Notes
Strip the domain portion of a structured username before relaying an authentication, authorization, or accounting request.	*tacacs+ strip-domain*	
Modify the time-out value.	*tacacs+ timeout*	
Configure an IP source address.	*ip source-address*	Enter this command in interface configuration mode and specify the `tacacs+` keyword.

For information about configuring interfaces and the `ip source-address` command (in interface configuration mode), see *Configuring Contexts and Interfaces*.

3.2 Operations Tasks

To monitor and troubleshoot TACACS+ servers, perform the appropriate TACACS+ operations tasks described in Table 2. Enter the `debug` command in exec mode; enter the `show` command in any mode.

Table 2 TACACS+ Operations Tasks

Task	Root Command
Enable the generation of TACACS+ debug messages.	*debug aaa tacacs+*
Display configuration information for one or all TACACS+ servers in the current context.	*show tacacs+ server*

4 Configuration Examples

The following example configures a TACACS+ server IP address, **10.43.32.56**, with the key, **Secret**. The SmartEdge router will attempt to open a TCP connection to the TACACS+ server up to **5** times when no response is received within **30** seconds:

```
[local]Redback(config-ctx)#tacacs+ server 10.43.32.56 key Secret

[local]Redback(config-ctx)#tacacs+ max-retries 5

[local]Redback(config-ctx)#tacacs+ timeout 30

[local]Redback(config-ctx)#tacacs+ strip-domain
```

5 TACACS+ Attribute-Value Pairs

Terminal Access Controller Access Control System Plus (TACACS+) attribute-value pairs (AVPs) are used to define specific administrator and command-line interface (CLI) command authentication, authorization, and accounting (AAA) elements for user profiles that are stored on a TACACS+ server.

5.1 TACACS+ Authentication and Authorization AVPs

Table 3 describes TACACS+ authentication and authorization AVPs supported by the SmartEdge router.

Table 3 TACACS+ Authentication and Authorization AV Pairs

Attribute	**Description**
cmd=x	Administrator shell command. Indicates the command name for the command to be issued. This attribute can only be specified if service=shell.
cmd-arg=x	Argument used with an administrator shell command. Indicates the argument name to be used with the command. Multiple cmd-arg attributes can be specified and cmd-arg attributes are order dependent.
priv-lvl=x	When received in an administrator authorization response from the server, sets the starting privilege level for the administrator.
service=x	Service used by the administrator.

5.2 TACACS+ Administrator Accounting AVPs

Table 4 describes the TACACS+ administrator accounting AVPs supported by the SmartEdge router.

Table 4 TACACS+ Administrator Accounting AV Pairs

Attribute	**Description**
service=shell	Service used by the administrator.
start_time=x	Time at which the administrator logged onto the SmartEdge router. The format is in number of seconds since 12:00 a.m. January 1, 1970.
stop_time=x	Time at which the administrator logged off the SmartEdge router. The format is in number of seconds since 12:00 a.m., January 1, 1970.

Table 4 TACACS+ Administrator Accounting AV Pairs

Attribute	Description
task_id=x	Start and stop records for the same event must have matching (unique) task ID numbers.
timezone=x	Time zone abbreviation for all time stamps included in this packet.

5.3 TACACS+ Command Accounting AVPs

Table 5 describes the TACACS+ command accounting AVPs supported by the SmartEdge router.

Table 5 TACACS+ Command Accounting AV Pairs

Attribute	Description
cmd=x	Command issued by the administrator. Includes all supported CLI commands.
priv-lvl=x	Privilege level associated with the command being issued.
start_time=x	Time at which the command is issued.
service=shell	Service used by the administrator.
task_id=x	Start and stop records for the same event must have matching (unique) task ID numbers.
timezone=x	Time zone abbreviation for all timestamps included in this packet.