JUNIPER NETWORKS

JunosE™ Software for E Series™ Broadband Services Routers

TACACS+ Server

Release
14.3.x

Published: 2013-07-15

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

JunosE™ Software for E Series™ Broadband Services Routers TACACS+ Server
Release 14.3.x

Revision History
July 2013—FRS JunosE 14.3.x

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Tables

About the Documentation

E Series and JunosE Documentation and Release Notes

For a list of related JunosE documentation, see http://www.juniper.net/techpubs/software/index.html.

If the information in the latest release notes differs from the information in the documentation, follow the *JunosE Release Notes.*

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Audience

This guide is intended for experienced system and network specialists working with Juniper Networks E Series Broadband Services Routers in an Internet access environment.

E Series and JunosE Text and Syntax Conventions

Table 1 on page viii defines notice icons used in this documentation.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page viii defines text and syntax conventions that we use throughout the E Series and JunosE documentation.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents commands and keywords in text.	• Issue the **clock source** command. • Specify the keyword **exp-msg**.
Bold text like this	Represents text that the user must type.	**host1(config)#traffic class low-loss1**

`Fixed-width text like this`	Represents information as displayed on your terminal's screen.	**host1#show ip ospf 2**
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an Area Border Router (ABR)`

Italic text like this	• Emphasizes words. • Identifies variables. • Identifies chapter, appendix, and book names.	• There are two levels of access: *user* and *privileged*. • *clusterId, ipAddress.* • *Appendix A, System Specifications*
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
Italic text like this	Represents variables.	*mask*, *accessListName*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic | line
[ ] (brackets)	Represent optional keywords or variables.	[internal | external]
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
{ } (braces)	Represent required keywords or variables.	{ permit | deny } { in | out } { *clusterId* | *ipAddress* }

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the Technical Documentation page on the Juniper Networks Web site at http://www.juniper.net/.

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the Portable Libraries page at

http://www.juniper.net/techpubs/resources/index.html

Copies of the Management Information Bases (MIBs) for a particular software release are available for download in the software image bundle from the Juniper Networks Web site athttp://www.juniper.net/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

How TACACS+ Works

Understanding TACACS+

With the increased use of remote access, the need for managing more network access servers (NAS) has increased. Additionally, the need for control access on a per-user basis has escalated, as has the need for central administration of users and passwords.

Terminal Access Controller Access Control System (TACACS) is a security protocol that provides centralized validation of users who are attempting to gain access to a router or NAS. TACACS+, a more recent version of the original TACACS protocol, provides separate authentication, authorization, and accounting (AAA) services.

NOTE: **TACACS+ is a completely new protocol and is not compatible with TACACS or XTACACS.**

The TACACS+ protocol provides detailed accounting information and flexible administrative control over the authentication, authorization, and accounting process. The protocol allows a TACACS+ client to request detailed access control and allows the TACACS + process to respond to each component of that request. TACACS+ uses Transmission Control Protocol (TCP) for its transport.

TACACS+ provides security by encrypting all traffic between the NAS and the process. Encryption relies on a secret key that is known to both the client and the TACACS+ process.

Table 3 on page 3 describes terms that are frequently used in this chapter.

Table 3: TACACS-Related Terms

Term	Description
NAS	Network access server. A device that provides connections to a single user, to a network or subnetwork, and to interconnected networks. In reference to TACACS+, the NAS is the E Series router.

Table 3: TACACS-Related Terms *(continued)*

Term	Description
TACACS+ process	A program or software running on a security server that provides AAA services using the TACACS+ protocol. The program processes authentication, authorization, and accounting requests from an NAS. When processing authentication requests, the process might respond to the NAS with a request for additional information, such as a password.
TACACS+ host	The security server on which the TACACS+ process is running. Also referred to as a TACACS+ server.

AAA Overview

TACACS+ allows effective communication of AAA information between NASs and a central server. The separation of the AAA functions is a fundamental feature of the TACACS+ design:

- Authentication—Determines who a user is, then determines whether that user should be granted access to the network. The primary purpose is to prevent intruders from entering your networks. Authentication uses a database of users and passwords.
- Authorization—Determines what an authenticated user is allowed to do. Authorization gives the network manager the ability to limit network services to different users. Also, the network manager can limit the use of certain commands to various users. Authorization cannot occur without authentication.
- Accounting—Tracks what a user did and when it was done. Accounting can be used for an audit trail or for billing for connection time or resources used. Accounting can occur independent of authentication and authorization.

Central management of AAA means that the information is in a single, centralized, secure database, which is much easier to administer than information distributed across numerous devices. Both RADIUS and TACACS+ protocols are client-server systems that allow effective communication of AAA information.

For information about RADIUS, see *RADIUS Overview*.

Administrative Login Authentication

Fundamentally, TACACS+ provides the same services as RADIUS. Every authentication login attempt on an NAS is verified by a remote TACACS+ process.

TACACS+ authentication uses three packet types. Start packets and Continue packets are always sent by the user. Reply packets are always sent by the TACACS+ process.

TACACS+ sets up a TCP connection to the TACACS+ host and sends a Start packet. The TACACS+ host responds with a Reply packet, which either grants or denies access, reports an error, or challenges the user.

TACACS+ might challenge the user to provide username, password, passcode, or other information. Once the requested information is entered, TACACS+ sends a Continue

packet over the existing connection. The TACACS+ host sends a Reply packet. Once the authentication is complete, the connection is closed. Only three login retries are allowed.

To enable login authentication through both TACACS+ and RADIUS servers, use the **aaa new-model** command to specify AAA authentication for Telnet sessions.

Privilege Authentication

The privilege authentication process determines whether a user is allowed to use commands at a particular privilege level. This authentication process is handled similarly to login authentication, except that the user is limited to one authentication attempt. An empty reply to the challenge forces an immediate access denial. The **aaa authentication enable default** command allows you to set privilege authentication for users.

Login Authorization

To allow login authorization through the TACACS+ server, you can use the following commands: **aaa authorization**, **aaa authorization config-commands**, and **authorization**. For information about using these commands, see the *Passwords and Security* chapter in *JunosE System Basics Configuration Guide*.

Accounting

The TACACS+ accounting service enables you to create an audit trail of User Exec sessions and command-line interface (CLI) commands that have been executed within these sessions. For example, you can track user CLI connects and disconnects, when configuration modes have been entered and exited, and which configuration and operational commands have been executed.

You configure TACACS+ accounting in the JunosE Software by defining accounting method lists and then associating consoles and lines with the method lists. You define an accounting method list with a service type, name, accounting mode, and method:

- service type—Specifies the type of information being recorded
- name—Uniquely identifies an accounting method list within a service type
- accounting mode—Specifies what type of accounting records will be generated
- method—Specifies the protocol for sending the accounting records to a security server

You can then configure consoles and lines with an accounting method list name for each service type:

- Method list—A specified configuration that defines how the NAS performs the AAA accounting service. A service type can be configured with multiple method lists with different names, and a method list name can be used for different service types. Initially, no accounting method list is defined; therefore TACACS+ accounting is disabled.
  - Default method list—Configuration used by consoles and lines when no named method list is assigned. You enable TACACS+ accounting by defining default accounting method lists for each service type.
  - Named method list—Assigned to a console, specific line, or group of lines; overrides the default method list.

- Service type—Specifies the type of information provided by the TACACS+ accounting service:
  - Exec—Provides information about User Exec terminal sessions, such as telnet, Local Area Transport (LAT), and rlogin, on the NAS.
  - Commands <0-15>—Provides information about User Exec mode CLI commands for a specified privilege level that are being executed on the NAS. Each of the sixteen command privilege levels is a separate service type. Accounting records are generated for commands executed by users, CLI scripts, and macros.
- Accounting mode—Specifies the type of accounting records that are recorded on the TACACS+ server. Accounting records track user actions and resource usage. You can analyze and use the records for network management, billing, and auditing purposes.
  - start-stop—A start accounting record is generated just before a process begins, and a stop accounting record is generated after a process successfully completes. This mode is supported only for the Exec service type.
  - stop-only—A stop accounting record is generated after a process successfully completes. This mode is supported only for the Commands service types.

The NAS sends TACACS+ accounting packets to the TACACS+ host. The accounting packets contain data in the packet header, packet body, and attribute-value pairs (AVPs). Table 4 on page 6 provides descriptions of the TACACS+ accounting data.

Table 4: TACACS+ Accounting Information

Field/Attribute	Location	Description
major_version	Packet header	Major TACACS+ version number
minor_version	Packet header	Minor TACACS+ version number
type	Packet header	Type of the AAA service: Accounting
flags	Packet body	Bitmapped flags representing the record type: start accounting record or stop accounting record
priv-level	Packet body	Privilege level of the user executing the Exec session or CLI command: 0 - 15
user	Packet body	Name of user running the Exec session or CLI command
port	Packet body	NAS port used by the Exec session or CLI command
rem-addr	Packet body	User's remote location; either an IP address or the caller ID
service	AVP	User's primary service: Shell
cmd	AVP	CLI command that is to be executed: specified for Command-level accounting only

Table 4: TACACS+ Accounting Information *(continued)*

Field/Attribute	Location	Description
task_id	AVP	Unique sequential identifier used to match start and stop records for a task
elapsed_time	AVP	Elapsed time in seconds for the task execution: specified for Exec-level accounting stop records only
timezone	AVP	Time zone abbreviation used "Monitoring TACACS+ Statistics" on page 33for all timestamps

Related Documentation

- Configuring TACACS+ on page 13
- Monitoring TACACS+ Statistics on page 33
- Monitoring TACACS+ Information on page 35

TACACS+ References

For additional information about the TACACS+ protocol, see the following resources:

- The TACACS+ Protocol, Version 1.78—draft-grant-tacacs-02.txt (January 1997 expiration)
- RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)

NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at http://www.ietf.org for the latest drafts.

Related Documentation

- Understanding TACACS+ on page 3

TACACS+ Platform Considerations

TACACS+ is supported on all E Series routers. For information about the modules supported on E Series routers:

- See the *ERX Module Guide* for modules supported on ERX7xx models, ERX14xx models, and the ERX310 Broadband Services Router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 and E320 Broadband Services Routers.

Related Documentation

- Understanding TACACS+ on page 3

CHAPTER 2

Interoperation with Packet Mirroring

Using TACACS+ and Vty Access Lists to Secure Packet Mirroring

This procedure uses TACACS+ and vty access lists to manage the users who have access to the **mirror-enable** command. An authorized user who issues the **mirror-enable** command then gains access to the packet mirroring CLI commands and information.

This technique enables you to restrict the visibility and use of packet mirroring commands to a controlled, authorized group of users.

1. Configure TACACS+ authorization for the access level of the **mirror-enable** command (level 12 by default).

   Configure the router either to allow or disallow authorization when the TACACS+ servers are not available.

2. Configure all vty lines and the console to use the TACACS+ authorization configuration from Step 1 for access level 12 commands.

This procedure ensures that packet mirroring commands are never sent out of the E Series router—only the **mirror-enable** command is sent. The packet mirroring configuration and all information about mirrored interfaces and subscribers are available only to users who are authorized for the packet mirroring CLI commands on the router.

Related Documentation

- *CLI-Based Packet Mirroring Overview*
- *Configuring CLI-Based Packet Mirroring*
- *Using Vty Access Lists to Secure Packet Mirroring*
- *mirror-enable*

PART 2

Configuration

CHAPTER 3

Configuring TACACS+ Server, Authentication, and Accounting

Configuring TACACS+

Terminal Access Controller Access Control System (TACACS) is a security protocol that provides centralized validation of users who are attempting to gain access to a router or NAS. TACACS+, a more recent version of the original TACACS protocol, provides separate authentication, authorization, and accounting (AAA) services. This topic includes the following tasks:

Configuring TACACS+ Support

Before you begin to configure TACACS+, you must determine the following for the TACACS+ authentication and accounting servers:

- IP addresses
- TCP port numbers
- Secret keys

To use TACACS+, you must enable AAA. To configure your router to support TACACS+, perform the following tasks. Some of the tasks are optional. Once you configure TACACS+ support on the router, you can configure TACACS+ authentication, authorization, and accounting independent of each other.

You can configure the TACACs+ server only on default virtual routers. If you attempt to configure TACACS+ server settings on VRs other than the default VR or in a VRF, an error message is displayed.

1. Specify the names of the IP host or hosts maintaining a TACACS+ server. Optionally, you can specify other parameters, such as port number, timeout interval, and key.

   host1(config)#tacacs-server host 192.168.1.27 port 10 timeout 3 key your_secret primary

2. (Optional) Set the authentication and encryption key value shared by all TACACS+ servers that do not have a server-specific key set up by the **tacacs-server host** command.

   host1(config)#tacacs-server key " &#889P^"

3. (Optional) Set alternative source addresses to be used for TACACS+ server communications.

   host1(config)#tacacs-server source-address 192.168.134.63

4. (Optional) Set the timeout value for all TACACS+ servers that do not have a server-specific timeout set up by the **tacacs-server host** command.

   host1(config)#tacacs-server timeout 15

5. (Optional) Set the retry value for a TACACS+ client. The maximum retry attempt for a request is five. By default, the retry value is two.

   host1(config)#tacacs-server retransmit-retries 4

Configuring Authentication

Once TACACS+ support is enabled on the router, you can configure TACACS+ authentication. Perform the following steps:

1. Specify AAA new model as the authentication method for the vty lines on your router.

   host1(config)#aaa new-model

2. Specify AAA authentication by defining an authorization methods list.

   host1(config)#aaa authentication login tac tacacs+ radius enable

3. Specify the privilege level by defining a methods list that uses TACACS+ for authentication.

   host1(config)#aaa authentication enable default tacacs+ radius enable

4. Configure vty lines.

   host1(config)#line vty 0 4

5. Apply an authentication list to the vty lines you specified on your router.

   host1(config-line)#login authentication tac

Configuring Accounting

Once TACACS+ support is enabled on the router, you can configure TACACS+ accounting. Perform the following steps:

1. Specify AAA new model as the accounting method for your router.

   host1(config)#aaa new-model

2. Enable TACACS+ accounting on the router, and configure accounting method lists. For example:

   host1(config)#aaa accounting exec default start-stop tacacs+
   host1(config)#aaa accounting commands 0 listX stop-only tacacs+

```
host1(config)#aaa accounting commands 1 listX stop-only tacacs+
host1(config)#aaa accounting commands 13 listY stop-only tacacs+
host1(config)#aaa accounting commands 14 default stop-only tacacs+
host1(config)#aaa accounting commands 15 default stop-only tacacs+
```

3. (Optional) Specify that accounting records are not generated for users without explicit user names.

```
host1(config)#aaa accounting suppress null-username
```

4. Apply accounting method lists to a console or lines. For example:

```
host1(config)#line console 0
host1(config-line)#accounting commands 0 listX
host1(config-line)#accounting commands 1 listX
host1(config-line)#accounting commands 13 listY
host1(config-line)#exit
host1(config)#line vty 0 4
host1(config-line)#accounting commands 13 listY
```

Note that Exec accounting and User Exec mode commands accounting for privilege levels 14 and 15 are now enabled for all lines and consoles with the creation of their default method list, as shown in Step 2.

Related Documentation

- aaa accounting commands on page 18
- aaa accounting exec on page 19
- *aaa accounting suppress null-username*
- aaa authentication enable default on page 21
- aaa authentication login on page 22
- aaa new-model on page 20
- line on page 23
- login authentication on page 24
- tacacs-server host on page 25
- tacacs-server key on page 26
- tacacs-server source-address on page 28
- tacacs-server timeout on page 29

CHAPTER 4

Configuration Commands

aaa accounting commands

Syntax aaa accounting commands *level* { default | *listName* } stop-only tacacs+

no aaa accounting commands *level listName*

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables AAA accounting for TACACS+ to be captured for a specific user privilege level and creates accounting method lists. The **no** version deletes the accounting method list.

Options

- *level*—Privilege level of user commands for which accounting information is captured; in the range 0–15
- default—Specifies that the default method list is used to specify how accounting is performed
- *listName*—Named method list used to specify how accounting is performed
- stop-only—Sends a stop accounting notice at the end of a process

Mode Global Configuration

Related Documentation

- Understanding TACACS+ on page 3
- Configuring TACACS+ on page 13

aaa accounting exec

Syntax aaa accounting exec { default | *listName* } start-stop tacacs+

no aaa accounting exec *listName*

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables AAA accounting for TACACS+ to be captured for User Exec terminal sessions, and creates accounting method lists. The **no** version deletes the accounting method list.

Options

- exec—Specifies that accounting information is captured for User Exec terminal sessions
- default—Specifies that the default method list is used to specify how accounting is performed
- *listName*—Named method list used to specify how accounting is performed
- start-stop—Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a successful process

Mode Global Configuration

aaa new-model

Syntax [no] aaa new-model

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies AAA authentication for Telnet sessions. It is also used to specify AAA new model as the authentication method for the vty lines on your router. If you specify AAA new model and you do not create an authentication list, users will not be able to access the router through a vty line. The **no** version restores simple authentication (login and password).

Mode Global Configuration

aaa authentication enable default

Syntax aaa authentication enable default *authenticator* [*authenticator*]*

no aaa authentication enable default

Release Information Command introduced before JunosE Release 7.1.0.

Description Allows privilege determination to be authenticated through the authenticator(s) you specify (TACACS+ or RADIUS server). This command specifies a list of authentication methods that are used to determine whether a user is granted access to the privilege command level. This authentication is applied to vty users. Requests sent to a TACACS+ or RADIUS server include the username that is entered for login authentication. If the authentication method list is empty, the local **enable** password is used. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line. The **no** version removes the authentication settings.

Options

- *authenticator*—Authentication method:
  - enable—Use the enable password
  - line—Use the line password
  - none—Use no authentication
  - radius—Use RADIUS authentication
  - tacacs+—Use TACACS+ authentication
  - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

aaa authentication login

Syntax aaa authentication login { default | *authListName* } *authenticator* [*authenticator*]*

no aaa authentication login *authListName*

Release Information Command introduced before JunosE Release 7.1.0.

Description Creates an authentication list and the criteria for login. This authentication is applied to vty users. After you have specified **aaa new-model** as the authentication method for vty lines, an authentication list called default is automatically assigned to the vty lines. To allow users to access the vty lines, you must create an authentication list and either:

- Name the list default.
- Assign a different name to the authentication list, and assign the new list to the vty line using the **login authentication** command.

The system traverses the list of authentication methods to determine whether a user is allowed to start a Telnet session. If a specific method is available but the user information is not valid (such as an incorrect password), the system does not continue to traverse the list and denies the user a session. If a specific method is unavailable, the system continues to traverse the list. For example, if **tacacs+** is the first authentication type element on the list and the TACACS+ server is unreachable, the system attempts to authenticate with the next authentication type on the list, such as **radius**. The system assumes an implicit denial of service if it reaches the end of the authentication list without finding an available method. The **no** version disables AAA authentication.

Options

- default—Specifies the use of the default login for authentication
- *authListName*—Existing authentication list name (created using the **login authentication** command); a string of 1–32 characters
- *authenticator*—Authentication method:
  - line—Use the line password for authentication
  - none—Use no authentication
  - radius—Use RADIUS authentication
  - tacacs+—Use TACACS+ authentication
- *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

line

Syntax line { console *lineNumber* | vty *lineRangeStart* [*lineRangeEnd*] }

no line vty *lineNumber*

Release Information Command introduced before JunosE Release 7.1.0.

Description Opens virtual terminal lines or the console line and allows you to configure the lines. By default five vty lines (0–4) are open. The **no** version removes a vty line or a range of lines from your configuration; users will not be able to run Telnet, SSH, or FTP to lines that you remove. When you remove a vty line, the router removes all lines above that line. For example, **no line vty 6** causes the router to remove lines 6 through 29. You cannot remove lines 0 through 4.

NOTE: Once lines are open, login is enabled by default. Before users can access the lines, you must configure a password, disable login using the **no login** command, or configure AAA authentication on the line.

Options

- console—Specifies the console line
- vty—Specifies vty lines
- *lineNumber*—Number of a single line; 0 for the console line
- *lineRangeStart*—Start of the vty line range; a number from 0–29
- *lineRangeEnd*—End of the vty line range; a number from 0–29

Mode Global Configuration

login authentication

Syntax login authentication *authListName*

no login authentication

Release Information Command introduced before JunosE Release 7.1.0.

Description Applies an AAA authentication list to the vty sessions that you specified for AAA authentication. The **no** version removes all authentication methods, which means the router accepts Telnet sessions without challenge.

Options

- *authListName*—Authentication list name of up to 32 characters

Mode Line Configuration

tacacs-server host

Syntax tacacs-server host *ipAddress* [port *portNumber*]
[timeout *timeoutValue*] [key *keyValueString*] [primary]

no tacacs-server host *ipAddress*

Release Information Command introduced before JunosE Release 7.1.0.

Description Adds or deletes a host to or from the list of TACACS+ servers. If the host is not assigned as the primary host, the router assigns an existing host as the primary. The **no** version deletes the host from the list of TACACS+ servers.

NOTE: You can configure the TACACs+ server only on default virtual routers. If you attempt to configure TACACS+ server settings on VRs other than the default VR or in a VRF, an error message is displayed.

Options

- *ipAddress*—IP address of the TACACS+ server
- *portNumber*—TACACS+ server's TCP port number in the range 1–655535
- *timeoutValue*—Response timeout interval for the TACACS+ client to server exchange; number in the range 1–255; default value is 5
- *keyValueString*—Secret used in TACACS+ client to server exchange; string of up to 100 characters
- primary—Assigns the host as the primary host

Mode Global Configuration

tacacs-server key

Syntax tacacs-server key *keyValueString*

no tacacs-server key

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets or resets the authentication and encryption key value shared by all TACACS+ servers that do not have a server-specific key set up by the **tacacs-server host** command. The **no** version removes the key value shared by all TACACS+ servers.

NOTE: You can configure the TACACs+ server only on default virtual routers. If you attempt to configure TACACS+ server settings on VRs other than the default VR or in a VRF, an error message is displayed.

Options

- *keyValueString*—String of up to 100 characters; must match key configured on the TACACS+ daemon

Mode Global Configuration

tacacs-server retransmit-retries

Syntax [no] tacacs-server retransmit-retries *retryNum*

Release Information Command introduced in JunosE Release 13.1.0.

Description Specifies the number of retry attempts that will be made to establish a Transmission Control Protocol (TCP) connection between a TACACS+ client and the TACACS+ server. The maximum retry attempt for a request is five. By default, the retry value is two. The **no** version restores the default value.

NOTE: You can configure the TACACs+ server only on default virtual routers. If you attempt to configure TACACS+ server settings on VRs other than the default VR or in a VRF, an error message is displayed.

Options
- *retryNum*—Number of retry attempts in the range 1–5

Mode Global Configuration, Interface Configuration

Related Documentation
- *Retry Attempts for Successful TCP Connection Overview*

tacacs-server source-address

Syntax tacacs-server source-address *ipAddress*

no tacacs-server source-address

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets or resets an alternative source address to be used for TACACS+ server communications. The **no** version removes the address.

NOTE: You can configure the TACACs+ server only on default virtual routers. If you attempt to configure TACACS+ server settings on VRs other than the default VR or in a VRF, an error message is displayed.

Options

- *ipAddress*—IP address used as source by the TACACS+ server

Mode Global Configuration

tacacs-server timeout

Syntax tacacs-server timeout *timeoutValue*

no tacacs-server timeout

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets the interval in seconds that the server waits for the TACACS+ server host to reply. This value is shared by those TACACS+ servers that do not have a timeout interval set by the **tacacs-server host** command. The **no** version resets the timeout interval shared by all TACACS+ servers.

NOTE: You can configure the TACACs+ server only on default virtual routers. If you attempt to configure TACACS+ server settings on VRs other than the default VR or in a VRF, an error message is displayed.

Options

- *timeoutValue*—Response timeout interval for the TACACS+ client to server exchange; number in the range 1–255; default value is 5

Mode Global Configuration

PART 3

Administration

CHAPTER 5

Verifying TACACS+ Statistics

Setting Baseline TACACS+ Statistics

You can set a baseline for TACACS+ statistics.

To set the baseline:

- Issue the **baseline tacacs** command:

  host1#baseline tacacs

There is no **no** version.

Related Documentation

- baseline tacacs on page 38

Monitoring TACACS+ Statistics

Purpose Display TACACS+ statistics.

Action To display TACACS+ statistics:

```
host1#show statistics tacacs
          TACACSPLUS Statistics
          ---------------------
   Statistic      10.5.0.174   10.5.1.199
---------------   ----------   ----------
Search Order      1            2
TCP Port          3049         4049
Auth Requests     140          0
Auth Replies      85           0
Auth Pending      43           0
Auth Timeouts     12           0
Author Requests   6399         97
Author Replies    6301         0
Author Pending    0            0
Author Timeouts   98           97
Acct Requests     6321         37
Acct Replies      6280         0
Acct Pending      4            0
Acct Timeouts     37           37
```

Meaning Table 5 on page 34 lists the **show statistics tacacs** command output fields.

Table 5: show statistics tacacs Output Fields

Field Name	Field Description
Statistic	IP address of the host
Search Order	The order in which requests are sent to hosts until a response is received
TCP Port	TCP port of the host
Auth Requests	Number of authentication requests sent to the host
Auth Replies	Number of authentication replies received from the host
Auth Pending	Number of expected but not received authentication replies from the host
Auth Timeouts	Number of authentication timeouts for the host
Author Requests	Number of authorization requests sent to the host
Author Replies	Number of authorization replies received from the host
Author Pending	Number of expected but not received authorization replies from the host
Author Timeouts	Number of authorization timeouts for the host
Acct Requests	Number of accounting requests sent to the host
Acct Replies	Number of accounting replies received from the host
Acct Pending	Number of expected but not received accounting replies from the host
Acct Timeouts	Number of accounting timeouts for the host

Related Documentation

- show statistics tacacs on page 39

CHAPTER 6

Viewing TACACS+ Server Settings

Monitoring TACACS+ Information

Purpose Display TACACS+ information.

Action To display TACACS+ information.

```
host1#show tacacs
Key = hippo
Timeout = <NOTSET>, built-in timeout of 5 will be used
Source-address = <NOTSET>
Retry-attempts = 3

  TACACS+ Configuration, (*) denotes inherited
  ----------------------------------------
             Tcp                                        Search
IP Address   Port   Timeout   Primary      Key         Order
----------   ----   -------   -------   ---------      ------
10.5.0.174   3049   5 (*)     y         hippo (*)      1
10.5.1.199   1049   5 (*)     n         hippo (*)      2
```

To display overall statistics:

```
host1#show tacacs statistics
```

To display statistics since they were baselined; deltas are not calculated for the pending statistics:

```
host1#show tacacs delta
```

Meaning Table 6 on page 35 lists the **show tacacs** command output fields.

Table 6: show tacacs Output Fields

Field Name	Field Description
Key	Authentication and encryption key
Timeout	TACACS+ host response timeout in seconds
Source-address	Alternative source IP address configured

Table 6: show tacacs Output Fields *(continued)*

Field Name	Field Description
Retry-attempts	Number of retry attempts that will be made to establish a TCP connection between a TACACS+ client and the TACACS+ server
TACACSPLUS Configuration	Table contains statistics for each host
IP Address	IP address of the host
TCP Port	TCP port of the host for each IP address
Timeout	Timeout interval in seconds for each IP address
Primary	This IP address's primary host; options: y = yes, n = no
Key	Authentication and encryption key for this IP address
Search Order	The order in which requests are sent to hosts until a response is received

Related Documentation

- show tacacs on page 40

CHAPTER 7

Monitoring Commands

baseline tacacs

Syntax baseline tacacs

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets a baseline for TACACS+ statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

show statistics tacacs

Syntax show statistics tacacs [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays TACACS+ server or TACACS+ statistics information.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show tacacs

Syntax show tacacs [statistics | delta] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays general or detailed TACACS+ information.

Options
- statistics—Specifies TACACS+ server statistics
- delta—Displays baselined statistics
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

PART 4

Index

Index