JUNIPER NETWORKS

JunosE™ Software for E Series™ Broadband Services Routers

RADIUS Dynamic-Request Server

Release
15.1.x

Published: 2014-08-20

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 RADIUS Dynamic-Request Server
Release 15.1.x

Revision History
August 2014—FRS JunosE 15.1.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

About the Documentation ix
E Series and JunosE Documentation and Release Notes ix
Audience ix
E Series and JunosE Text and Syntax Conventions ix
Obtaining Documentation xi
Documentation Feedback xi
Requesting Technical Support xii
Self-Help Online Tools and Resources xii
Opening a Case with JTAC xii

Part 1 Overview

Chapter 1 How RADIUS Dynamic-Request Server Works 3

RADIUS Dynamic-Request Server Overview 3
RADIUS Dynamic-Request Server Platform Considerations 4
RADIUS Dynamic-Request Server References 4

Chapter 2 Processing of RADIUS Disconnect and CoA Messages 7

Understanding RADIUS-Initiated Change of Authorization 7
Change-of-Authorization Messages 7
Message Exchange 7
Supported Error-Cause Codes (RADIUS Attribute 101) 8
Qualifications for Change of Authorization 8
Security/Authentication 9
Understanding RADIUS-Initiated Disconnect 9
Disconnect Messages 9
Message Exchange 10
Supported Error-Cause Codes (RADIUS Attribute 101) 10
Qualifications for Disconnect 10
Security/Authentication 11

Chapter 3 Interoperation with Packet Mirroring 13

RADIUS-Based Mirroring Overview 13
RADIUS Attributes Used for Packet Mirroring 14

Part 2 Configuration

Chapter 4 Configuration Tasks for RADIUS Dynamic-Request Server 19

Configuring RADIUS-Initiated Change of Authorization 19
Configuring RADIUS-Initiated Disconnect 20

Chapter 5 RADIUS Dynamic-Request Server Statistics 21
Setting the Baseline for RADIUS Dynamic-Request Server Statistics 21
Chapter 6 Configuration Commands 23
authorization change 24
key 25
radius dynamic-request server 27
subscriber disconnect 28
udp-port 29
Part 3 Administration
Chapter 7 Monitoring Tasks 33
Monitoring RADIUS Dynamic-Request Server Statistics 33
Monitoring the Configuration of the RADIUS Dynamic-Request Server 34
Chapter 8 Monitoring Commands 37
baseline radius dynamic-request 38
show radius servers 39
show radius statistics 40
Part 4 Index
Index 43

List of Figures

Part 1 Overview

Chapter 1 How RADIUS Dynamic-Request Server Works 3

Figure 1: Sample Remote Access Network Using RADIUS 4

List of Tables

About the Documentation ix

Table 1: Notice Icons x
Table 2: Text and Syntax Conventions x

Part 1 Overview

Chapter 2 Processing of RADIUS Disconnect and CoA Messages 7

Table 3: Error-Cause Codes (RADIUS Attribute 101) 8
Table 4: Error-Cause Codes (RADIUS Attribute 101) 10

Chapter 3 Interoperation with Packet Mirroring 13

Table 5: RADIUS Attributes Used as Packet Mirroring Triggers (Vendor ID 4874) 14
Table 6: RADIUS Attributes Used as Packet Mirroring Triggers (Vendor ID 3561) 14
Table 7: RADIUS-Based Mirroring Attributes 15

Part 3 Administration

Chapter 7 Monitoring Tasks 33

Table 8: show radius dynamic-request statistics Output Fields 33
Table 9: show radius dynamic-request servers Output Fields 35

About the Documentation

- E Series and JunosE Documentation and Release Notes on page ix
- Audience on page ix
- E Series and JunosE Text and Syntax Conventions on page ix
- Obtaining Documentation on page xi
- Documentation Feedback on page xi
- Requesting Technical Support on page xii

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 x 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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page x 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.

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

Convention	Description	Examples
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
Italic text like this	Represents variables.	*mask*, *accessListName*
| (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 website 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 website at http://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: http://kb.juniper.net/InfoCenter/
- 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

- How RADIUS Dynamic-Request Server Works on page 3
- Processing of RADIUS Disconnect and CoA Messages on page 7
- Interoperation with Packet Mirroring on page 13

CHAPTER 1

How RADIUS Dynamic-Request Server Works

- RADIUS Dynamic-Request Server Overview on page 3
- RADIUS Dynamic-Request Server Platform Considerations on page 4
- RADIUS Dynamic-Request Server References on page 4

RADIUS Dynamic-Request Server Overview

The E Series router's RADIUS dynamic-request server feature provides an efficient way for you to use RADIUS servers to centrally manage user sessions. The RADIUS dynamic-request server enables the router to receive the following types of messages from RADIUS servers:

- Disconnect messages—Immediately terminate specific user sessions.
- Change-of-Authorization (COA) messages—Dynamically modify session authorization attributes, such as data filters.

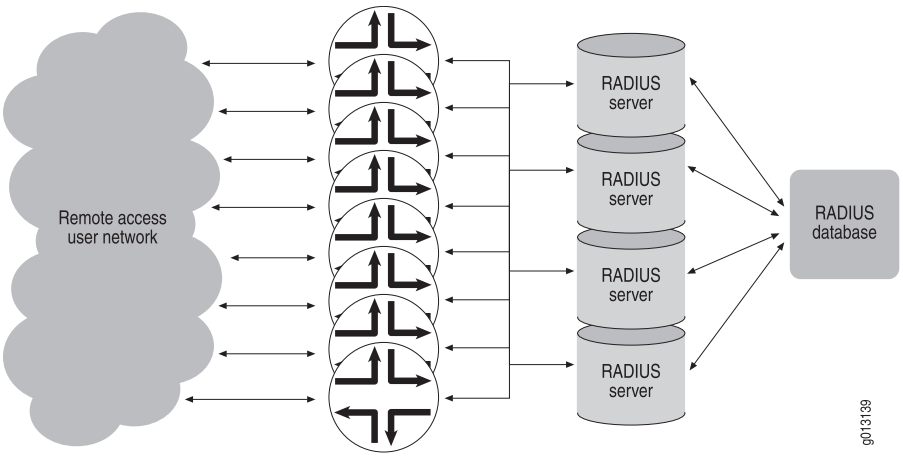
NOTE: The RADIUS dynamic-request server's support for COA messages is used by the Service Manager and by the E Series router's packet mirroring feature. For information about using the Service Manager, see the *Configuring Service Manager* chapter in this guide. For specific information about using the dynamic-request server with packet mirroring, see the *Configuring RADIUS-Based Packet Mirroring* chapter in the *JunosE Policy Management Configuration Guide*.

For example, you might use the RADIUS dynamic-request server to terminate specific user sessions. Without the RADIUS dynamic-request server, the only way to disconnect a RADIUS user is from the E Series router. This disconnect method is cumbersome when a network has many systems. The RADIUS dynamic-request server allows RADIUS servers to initiate user-related operations, such as a termination operation, by sending unsolicited request messages to an E Series router.

Figure 1 on page 4 shows a network that would benefit from the RADIUS dynamic-request server functionality. In Figure 1 on page 4, instead of disconnecting users on each E Series router, the RADIUS servers can initiate the disconnection. Although the network has

multiple RADIUS servers, the servers share a common database that contains authorization and accounting information. Having a common database allows any server to view who is currently valid and connected, and allows service providers to manage the disconnection of users.

Figure 1: Sample Remote Access Network Using RADIUS



Related Documentation

- Monitoring the Configuration of the RADIUS Dynamic-Request Server on page 34
- Setting the Baseline for RADIUS Dynamic-Request Server Statistics on page 21

RADIUS Dynamic-Request Server Platform Considerations

RADIUS dynamic-request server 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

- RADIUS Dynamic-Request Server Overview on page 3

RADIUS Dynamic-Request Server References

For more information about the RADIUS dynamic-request server feature, see the following references:

- RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)
- RFC 2866—RADIUS Accounting (June 2000)
- RFC 5176—Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS) (January 2008)

Related Documentation

- RADIUS Dynamic-Request Server Overview on page 3
- RADIUS Dynamic-Request Server Platform Considerations on page 4

CHAPTER 2

Processing of RADIUS Disconnect and CoA Messages

- Understanding RADIUS-Initiated Change of Authorization on page 7
- Understanding RADIUS-Initiated Disconnect on page 9

Understanding RADIUS-Initiated Change of Authorization

This section describes the RADIUS dynamic-request server's support for COA messages. COA messages are used by the E Series router's RADIUS-initiated packet mirroring feature, which is described in the *Configuring RADIUS-Based Packet Mirroring* chapter in the *JunosE Policy Management Configuration Guide*, and by Service Manager, which is described in the *Configuring Service Manager* chapter of this guide.

Change-of-Authorization Messages

The RADIUS dynamic-request server receives and processes the unsolicited COA messages from RADIUS servers. The RADIUS-initiated COA feature uses the following codes in its RADIUS request and response messages:

- COA-Request (43)
- COA-ACK (44)
- COA-NAK (45)

Message Exchange

The RADIUS server and the router's RADIUS dynamic-request server exchange messages using UDP. The COA-Request message sent by the RADIUS server has the same format as the Disconnect-Request packet that is sent for a disconnect operation.

The response is either a COA-ACK or a COA-NAK message:

- If AAA successfully changes the authorization, the response is a RADIUS-formatted packet with a COA-ACK message, and the data filter is applied to the session.
- If AAA is unsuccessful, the request is malformed, or attributes are missing, the response is a RADIUS-formatted packet with a COA-NAK message.

Supported Error-Cause Codes (RADIUS Attribute 101)

When AAA is unsuccessful, the RADIUS dynamic-request server includes an error-cause attribute (RADIUS attribute 101) in the COA-NAK message that it sends back to the RADIUS server. If the detected error does not map to one of the supported error-cause attributes, the router sends the COA-NAK without an error-cause attribute. Table 3 on page 8 lists the supported error-cause codes.

Table 3: Error-Cause Codes (RADIUS Attribute 101)

Code	Value	Description
401	Unsupported attribute	The request contains an attribute that is not supported (for example, a third-party attribute).
402	Missing attribute	A critical attribute (for example, the session identification attribute) is missing from a request.
404	Invalid request	Some other aspect of the request is invalid, such as if one or more attributes (for example, the packet mirroring Mirror Identifier value) are not formatted properly.
503	Session context not found	The session context identified in the request does not exist on the NAS.
504	Session context not removable	The subscriber identified by attributes in the disconnect request is owned by a component that does not support RADIUS-initiated disconnect (for example, IP LAC subscribers cannot be disconnected).
506	Resources unavailable	A request could not be honored due to lack of available NAS resources (such as memory).

Qualifications for Change of Authorization

To complete the change of authorization for a user, the COA-Request must contain one of the following RADIUS attributes or pairs of attributes. AAA services handle the actual request.

- User-Name [attribute 1] with Virtual-Router [attribute 26–1] to identify the user per virtual router context
- Framed-IP-Address [attribute 8] with Virtual-Router [attribute 26–1] to identify the address per virtual router context
- Calling-Station-ID [attribute 31]
- Acct-Session-ID [attribute 44] (mandatory for all COA requests, except when the request is for packet mirroring)
- Nas-Port-ID [attribute 5]
- DHCP-Option-82 [attribute 26–159], Vendor ID 4874

- Agent-Circuit-ID [attribute 26–1], Vendor ID 3561
- Agent-Remote-ID [attribute 26–2], Vendor ID 3561

NOTE: The Calling-Station-ID attribute is valid only for the tunneled subscribers and on the LNS. Additionally, the Calling-Station-ID and Nas-Port-ID attributes are valid only if there is no RADIUS override setting.

Security/Authentication

For change-of-authorization operations, the RADIUS server calculates the authenticator as specified for an Accounting-Request message in RFC 2866. The RADIUS dynamic-request server verifies the request using authenticator calculation as specified for an Accounting-Request in RFC 2866. A key (secret), as specified in RFC 2865, must be configured and used in the calculation of the authenticator. The response authenticator is calculated as specified for an Accounting-Response message in RFC 2866.

Related Documentation

- Configuring RADIUS-Initiated Change of Authorization on page 19
- Understanding RADIUS-Initiated Disconnect on page 9
- Configuring RADIUS-Initiated Disconnect on page 20

Understanding RADIUS-Initiated Disconnect

In a typical client-server RADIUS environment, the E Series router functions as the client and the RADIUS server functions as the server. However, when using the RADIUS dynamic-request server feature, the roles are reversed. For example, during a RADIUS-initiated disconnect operation, the E Series router's RADIUS dynamic-request server functions as the server, and the RADIUS server functions as the disconnect client.

This section describes the RADIUS dynamic-request server's RADIUS-initiated disconnect feature.

Disconnect Messages

To centrally control the disconnection of remote access users, the RADIUS dynamic-request server on the router must receive and process unsolicited messages from RADIUS servers.

The RADIUS-initiated disconnect feature uses the existing format of RADIUS disconnect request and response messages. The RADIUS-initiated disconnect feature uses the following codes in its RADIUS request and response messages:

- Disconnect-Request (40)
- Disconnect-ACK (41)
- Disconnect-NAK (42)

Message Exchange

The RADIUS server and the router's RADIUS dynamic-request server exchange messages using User Datagram Protocol (UDP). The Disconnect-Request message sent by the RADIUS server has the same format as the COA-Request packet that is sent for a change of authorization operation.

The disconnect response is either a Disconnect-ACK or a Disconnect-NAK message:

- If AAA successfully disconnects the user, the response is a RADIUS-formatted packet with a Disconnect-ACK message.
- If AAA cannot disconnect the user, the request is malformed, or attributes are missing from the request, the response is a RADIUS-formatted packet with a Disconnect-NAK message.

Supported Error-Cause Codes (RADIUS Attribute 101)

When a disconnect request fails, the RADIUS dynamic-request server includes an error-cause attribute (RADIUS attribute 101) in the Disconnect-NAK message that it sends back to the RADIUS server. If the detected error does not map to one of the supported error-cause attributes, the router sends the Disconnect-NAK without an error-cause attribute. Table 4 on page 10 lists the supported error-cause codes.

Table 4: Error-Cause Codes (RADIUS Attribute 101)

Code	Value	Description
401	Unsupported attribute	The request contains an attribute that is not supported (for example, a third-party attribute).
402	Missing attribute	A critical attribute (for example, the session identification attribute) is missing from a request.
404	Invalid request	Some other aspect of the request is invalid, such as if one or more attributes (for example, the packet mirroring Mirror Identifier value) are not formatted properly.
503	Session context not found	The session context identified in the request does not exist on the NAS.
504	Session context not removable	The subscriber identified by attributes in the disconnect request is owned by a component that does not support RADIUS-initiated disconnect (for example, IP LAC subscribers cannot be disconnected).
506	Resources unavailable	A request could not be honored due to lack of available NAS resources (such as memory).

Qualifications for Disconnect

For the server to disconnect a user, the Disconnect-Request message must contain an attribute with a session ID. The Disconnect-Request message can contain an

Acct-Session-Id (44) attribute or a Acct-Multi-Session-Id (50) attribute for the session ID or both. If both the Acct-Session-Id and Acct-Multi-Session-Id attributes are present in the request, the router uses both attributes. If the User-Name (1) attribute is also present in the request, the username and session ID are used to perform the disconnection. Authentication, authorization, and accounting (AAA) services handle the actual request.

NOTE: The inclusion of the Acct-Multi-Session-Id (50) attribute in RADIUS Disconnect-Request messages for LAC L2TP sessions causes the disconnection of L2TP LAC user sessions to occur properly. The value of this attribute is constructed from the Acct-Session-ID (44) attribute of the first PPP link established for MLPPP bundles. If the Acct-Multi-Session-Id (50) attribute is contained in the Disconnect-Request message for MLPPP links, which are on the LAC side of an L2TP tunnel, the subscriber session is disconnected.

Security/Authentication

The RADIUS server (the disconnect client) must calculate the authenticator as specified for an Accounting-Request message in RFC 2866. The router's RADIUS dynamic-request server verifies the request using authenticator calculation as specified for an Accounting-Request message in RFC 2866. A key (secret), as specified in RFC 2865, must be configured and used in the calculation of the authenticator. The response authenticator is calculated as specified for an Accounting-Response message in RFC 2866.

Related Documentation

- Configuring RADIUS-Initiated Disconnect on page 20
- Understanding RADIUS-Initiated Change of Authorization on page 7
- Configuring RADIUS-Initiated Change of Authorization on page 19

CHAPTER 3

Interoperation with Packet Mirroring

- RADIUS-Based Mirroring Overview on page 13
- RADIUS Attributes Used for Packet Mirroring on page 14

RADIUS-Based Mirroring Overview

RADIUS-based packet mirroring enables you to mirror traffic related to a specific user, without regard to how often the user logs in or out, or which E Series router or interface the user uses. RADIUS-based mirroring is particularly appropriate for large networks, because you can use a single RADIUS server to provision mirroring on multiple E Series routers in a service provider's network. RADIUS-based mirroring is useful when debugging network problems related to mobile users, who do not always log in to a particular router.

You configure RADIUS-based mirroring independent of the actual mirroring session—you can configure the mirroring parameters at any time. RADIUS-based mirroring uses RADIUS and VSAs, rather than CLI commands, to specify the user whose traffic is to be mirrored. The VSAs specify attributes that are carried in Access-Accept messages and change-of-authorization messages from the RADIUS dynamic-request server to the E Series router.

NOTE: **You cannot use RADIUS-based packet mirroring to mirror static interfaces, which might not be authenticated through RADIUS. To mirror static interfaces, you must use CLI-based mirroring.**

Related Documentation

- *Comparing CLI-Based Mirroring and RADIUS-Based Mirroring*
- *Configuring RADIUS-Based Packet Mirroring*
- *Packet Mirroring Overview*
- *RADIUS-Based Mirroring Sequence of Events*
- RADIUS Attributes Used for Packet Mirroring on page 14

RADIUS Attributes Used for Packet Mirroring

Table 5 on page 14 and Table 6 on page 14 list the packet mirroring triggers. The triggers are RADIUS attributes that identify a user whose traffic is to be mirrored. A packet mirroring session starts when the router receives a RADIUS packet that contains mirroring attributes and then applies the mirroring configuration to the appropriate interface. For example, packet mirroring starts when a logon request occurs that contains a specified User-Name attribute.

The triggers also enable RADIUS-initiated mirroring to start when the user is already logged in.

Table 5: RADIUS Attributes Used as Packet Mirroring Triggers (Vendor ID 4874)

Standard Number	Attribute Name	Order of Preference
[1]	User-Name	4
[8]	Framed-IP-Address	3
[26-1]	Virtual-Router	Used with Framed-IP-Address and User-Name
[31]	Calling-Station-ID	2
[44]	Acct-Session-ID	1
[87]	Nas-Port-ID	5
[26–159]	DHCP- Option-82	6

Table 6: RADIUS Attributes Used as Packet Mirroring Triggers (Vendor ID 3561)

Standard Number	Attribute Name	Order of Preference
[26-1]	Agent-Circuit-ID	7
[26-2]	Agent-Remote-ID	8

You add the trigger to the RADIUS record of the user whose traffic will be mirrored. In addition, you must include the RADIUS VSAs listed in Table 7 on page 15 in the mirrored user's RADIUS record.

NOTE: For IP mirroring, you must include both VSA 26-59 and VSA 26-61, or you must omit both of these VSAs. If you use only one of these VSAs, the configuration fails.

Table 7: RADIUS-Based Mirroring Attributes

Standard Number	Attribute Name	Setting
[26-58]	LI-Action	0 = disable mirroring 1 = enable mirroring 2 = no action
[26-59]	Med-Dev-Handle	String (not null-terminated)
[26-60]	Med-IP-Address	IP address of analyzer device
[26-61]	Med-Port-Number	UDP port number of monitoring application in analyzer device

An LI-Action setting of 2 specifies that the router does not perform any packet mirroring–related configuration. This setting can provide additional security by confusing unauthorized users who attempt to access packet mirroring communication between the router and the RADIUS server.

Related Documentation

- RADIUS-Based Mirroring Overview on page 13
- *RADIUS-Based Mirroring Sequence of Events*

PART 2

Configuration

- Configuration Tasks for RADIUS Dynamic-Request Server on page 19
- RADIUS Dynamic-Request Server Statistics on page 21
- Configuration Commands on page 23

CHAPTER 4

Configuration Tasks for RADIUS Dynamic-Request Server

- Configuring RADIUS-Initiated Change of Authorization on page 19
- Configuring RADIUS-Initiated Disconnect on page 20

Configuring RADIUS-Initiated Change of Authorization

To configure the RADIUS dynamic-request change of authorization (COA) feature, perform the following steps to set up the RADIUS dynamic-request server that will perform the COA operation:

1. Configure the RADIUS dynamic-request server, and enter RADIUS Configuration mode.

   host1(config)#radius dynamic-request server 10.10.5.10

2. Enable the COA capability on the RADIUS dynamic-request server.

   host1(config-radius)#authorization change

3. Define the key (secret) used in the RADIUS Authenticator field during exchanges between the RADIUS dynamic-request server and the RADIUS server.

   host1(config-radius)#key Secret21Clientkey

4. (Optional) Specify the UDP port on which the router listens for messages from the RADIUS server. The default is 1700.

   host1(config-radius)#udp-port 1770

Related Documentation

- Setting the Baseline for RADIUS Dynamic-Request Server Statistics on page 21
- Monitoring RADIUS Dynamic-Request Server Statistics on page 33
- Monitoring the Configuration of the RADIUS Dynamic-Request Server on page 34
- authorization change on page 24
- key on page 25
- udp-port on page 29

Configuring RADIUS-Initiated Disconnect

To configure RADIUS-initiated disconnect feature, perform the following steps to set up the RADIUS dynamic-request server that will perform the disconnect operation:

1. Configure the RADIUS dynamic-request server, and enter RADIUS Configuration mode.

   ```
   host1(config)#radius dynamic-request server 10.10.5.10
   host1(config-radius)#
   ```

2. Enable the RADIUS-initiated disconnect capability on the RADIUS dynamic-request server.

   ```
   host1(config-radius)#subscriber disconnect
   ```

3. Define the secret used in the RADIUS Authenticator field during exchanges between the RADIUS dynamic-request server and the RADIUS server.

   ```
   host1(config-radius)#key Secret3Clientkey
   ```

4. (Optional) Specify the UDP port on which the RADIUS dynamic-request server listens for messages from the RADIUS server. The default is 1700.

   ```
   host1(config-radius)#udp-port 1770
   ```

Related Documentation

- Setting the Baseline for RADIUS Dynamic-Request Server Statistics on page 21
- Monitoring RADIUS Dynamic-Request Server Statistics on page 33
- Monitoring the Configuration of the RADIUS Dynamic-Request Server on page 34
- key on page 25
- *radius disconnect client*
- subscriber disconnect on page 28
- udp-port on page 29

CHAPTER 5

RADIUS Dynamic-Request Server Statistics

- Setting the Baseline for RADIUS Dynamic-Request Server Statistics on page 21

Setting the Baseline for RADIUS Dynamic-Request Server Statistics

You can set a statistics baseline for packet mirroring-related RADIUS statistics. To show baseline statistics, use the **delta** keyword with the **show radius dynamic-request statistics** command.

To set a baseline for RADIUS statistics for packet mirroring:

- Issue the **baseline radius dynamic-request** command:

  host1#baseline radius dynamic-request

There is no **no** version.

Related Documentation

- Monitoring RADIUS Dynamic-Request Server Statistics on page 33
- **baseline radius dynamic-request on page 38**

CHAPTER 6

Configuration Commands

- authorization change
- key
- radius dynamic-request server
- subscriber disconnect
- udp-port

authorization change

Syntax [no] authorization change

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables the router to receive change-of-authorization messages, such as packet mirroring attributes and Service Manager attributes, from the RADIUS server. The **no** version restores the default, in which support for RADIUS-initiated change-of-authorization messages is disabled on the router.

Mode RADIUS Configuration

Related Documentation

- *Configuring RADIUS-Based Packet Mirroring*

key

Syntax To assign a RADIUS key:

key *secret*

no key

To assign a RADIUS relay key:

key *ipAddress ipMask relaySecret*

no key *ipAddress ipMask*

To assign an ISAKMP/IKE key:

key *keyString*

no key

Release Information Command introduced before JunosE Release 7.1.0.

Description From RADIUS Configuration mode, specifies the secret for the RADIUS authentication, accounting, dynamic-request server, or preauthentication server that is used to calculate the RADIUS authenticator field during exchanges with the RADIUS server. The **no** version removes the secret and causes the router to drop all requests for the RADIUS client.

From RADIUS Relay Configuration mode, specifies the IP address and mask of the network that will use the relay authentication or accounting server, and the secret used during exchanges between the RADIUS relay server and client. The **no** version removes the secret.

From IPsec Manual Key Configuration mode, configures a manual ISAKMP/IKE preshared key. There is no **no** version. To delete a key, use the **no** version of the **ipsec key manual** command.

Options

- *secret*—Authentication, accounting, dynamic-request, or preauthentication server secret text string used by RADIUS to encrypt the client and server authenticator field during exchanges between the router and a RADIUS server. The router encrypts PPP PAP passwords using this text string.
- *ipAddress*—IP address for client network
- *ipMask*—IP mask for the client network
- *relaySecret*—Text string; up to 32 characters
- *keyString*—Key value in ASCII format; up to 200 characters

Mode IPsec Manual Key Configuration, RADIUS Configuration, RADIUS Relay Configuration

Related Documentation

- *Configuring RADIUS-Based Packet Mirroring*

radius dynamic-request server

Syntax [no] radius dynamic-request server *ipAddress*

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the IP address of a RADIUS dynamic-request server and puts the E Series router into RADIUS Configuration mode. The **no** version deletes the instance of the RADIUS server.

NOTE: The **radius dynamic-request server** command replaces the functionality of the **radius disconnect client** command.

The RADIUS Disconnect Configuration mode is deprecated. Use the **radius dynamic-request server** command to enter RADIUS Configuration mode and configure options formerly available in RADIUS Disconnect Configuration mode.

Options
- *ipAddress*—IP address of the server

Mode Global Configuration

Related Documentation
- *Configuring RADIUS-Based Packet Mirroring*

subscriber disconnect

Syntax [no] subscriber disconnect

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables the E Series router to receive RADIUS-initiated disconnect messages from the RADIUS server. The **no** version restores the default, in which support for RADIUS-initiated disconnect messages is disabled on the router.

NOTE: This command and the RADIUS dynamic-request server feature replace the **radius disconnect client** command, which has been deprecated and may be removed completely in a future release. The RADIUS Disconnect Configuration mode has also been deprecated.

Mode RADIUS Configuration

udp-port

Syntax udp-port *port*

no udp-port

Release Information Command introduced before JunosE Release 7.1.0.

Description From RADIUS Configuration mode, specifies the UDP port on the router where the RADIUS authentication, accounting, or dynamic-request servers reside. The router uses this port to communicate with the RADIUS servers. The **no** version restores the default value.

From RADIUS Relay Configuration mode, specifies the UDP port on the router where the RADIUS relay authentication or accounting server resides. The router uses this port to communicate with the RADIUS relay servers. The **no** version restores the default value.

Options

- *port*—Port number in the range 1–65535
  - 1812—Default for RADIUS and RADIUS relay authentication servers
  - 1813—Default for RADIUS and RADIUS relay accounting servers
  - 1700—Default for RADIUS dynamic-request servers

Mode RADIUS Configuration, RADIUS Relay Configuration

Related Documentation

- *Configuring RADIUS-Based Packet Mirroring*

PART 3

Administration

- Monitoring Tasks on page 33
- Monitoring Commands on page 37

CHAPTER 7

Monitoring Tasks

- Monitoring RADIUS Dynamic-Request Server Statistics on page 33
- Monitoring the Configuration of the RADIUS Dynamic-Request Server on page 34

Monitoring RADIUS Dynamic-Request Server Statistics

Purpose Display RADIUS dynamic-request server statistics.

Action To display RADIUS dynamic-request statistics:

```
host1#show radius dynamic-request statistics

       RADIUS Request Statistics
       -------------------------
          Statistic              10.10.3.4
-----------------------------    -------
UDP Port                         1700
Disconnect Requests              0
Disconnect Accepts               0
Disconnect Rejects               0
Disconnect No Session ID         0
Disconnect Bad Authenticators    0
Disconnect Packets Dropped       0
COA Requests                     0
COA Accepts                      0
COA Rejects                      0
COA No Session ID                0
COA Bad Authenticators           0
COA Packets Dropped              0
No Secret                        0
Unknown Request                  0

Invalid Addresses Received  :0
```

Meaning Table 8 on page 33 lists the **show radius dynamic-request statistics** command output fields.

Table 8: show radius dynamic-request statistics Output Fields

Field Name	Field Description
Udp Port	Port on which the router listens for RADIUS server
Disconnect or COA Requests	RADIUS-initiated disconnect or COA requests received

Table 8: show radius dynamic-request statistics Output Fields *(continued)*

Field Name	Field Description
Disconnect or COA Accepts	RADIUS-initiated disconnect or COA requests accepted
Disconnect or COA Rejects	RADIUS-initiated disconnect or COA requests rejected
Disconnect or COA No Session ID	RADIUS-initiated disconnect or COA messages rejected because the request did not include a session ID attribute
Disconnect or COA Bad Authenticators	RADIUS-initiated disconnect or COA messages rejected because the calculated authenticator in the authenticator field of the request did not match
Disconnect or COA Packets Dropped	RADIUS-initiated disconnect or COA packets dropped because of queue overflow
No Secret	Messages rejected because a secret was not present in the authenticator field
Unknown Requests	Packets received with an invalid RADIUS code for RADIUS disconnect or change of authorization
Invalid Addresses Received	Number of invalid addresses received

Related Documentation

- Setting the Baseline for RADIUS Dynamic-Request Server Statistics on page 21
- show radius statistics on page 40

Monitoring the Configuration of the RADIUS Dynamic-Request Server

Purpose Display the configuration of the RADIUS dynamic-request server.

Action To display the configuration of the RADIUS dynamic-request server:

```
host1#show radius dynamic-request servers

                RADIUS Request Configuration
                ----------------------------
                                          Change
                 Udp                        Of
 IP Address      Port   Disconnect   Authorization   Secret
-------------    ----   ----------   -------------   ------
192.168.2.3      1700   disabled     disabled        <NULL>
10.10.120.104    1700   disabled     disabled        mysecret
```

Meaning Table 9 on page 35 lists the **show radius dynamic-request servers** command output fields.

Table 9: show radius dynamic-request servers Output Fields

Field Name	Field Description
IP address	IP address of the RADIUS server
Udp Port	Port on which the router listens for RADIUS server
Disconnect	Status of RADIUS-initiated disconnect feature
Change of Authorization	Status of change of authorization feature
Secret	Secret used to connect to RADIUS server

Related Documentation

- show radius servers on page 39

CHAPTER 8

Monitoring Commands

- baseline radius dynamic-request
- show radius servers
- show radius statistics

baseline radius dynamic-request

Syntax baseline radius dynamic-request

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets a statistics baseline for RADIUS dynamic-request 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

Related Documentation

- *Monitoring Packet Mirroring Overview*

show radius servers

Syntax show radius [*serverType*] servers [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
pre-authentication keyword added in JunosE Release 8.1.0.

Description Displays information about the RADIUS servers configured on the router.

Options
- *serverType*—One of the following RADIUS server types:
  - authentication—Displays authentication information only
  - accounting—Displays accounting information only
  - dynamic-request—Displays dynamic-request information only
  - pre-authentication—Displays preauthentication information only
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

Related Documentation
- *Monitoring RADIUS Dynamic-Request Server Information*

show radius statistics

Syntax show radius [*serverType*] statistics [delta] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
pre-authentication keyword added in JunosE Release 8.1.0.

Description Displays statistics for the RADIUS servers configured on the router.

Options
- *serverType*—One of the following RADIUS server types:
  - authentication—Displays authentication statistics only
  - accounting—Displays accounting statistics only
  - dynamic-request—Displays dynamic-request statistics only
  - pre-authentication—Displays preauthentication statistics only
- delta—Displays baselined statistics
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

Related Documentation
- *Monitoring RADIUS Dynamic-Request Server Information*

PART 4

Index

- Index on page 43

Index

A

AAA domain map commands
- auth-router-name....24

B

B-RAS commands
- auth-router-name....24
- authorization change....24
- baseline radius dynamic-request....38
- key....25
- radius dynamic-request server....27
- show radius servers....39
- show radius statistics....40
- subscriber disconnect....28
- udp-port....29

baseline commands
- baseline radius dynamic-request....21

C

conventions
- notice icons....ix
- text and syntax....x

customer support....xii
- contacting JTAC....xii

D

documentation set
- comments on....xi

I

IPsec commands
- key....25

M

manuals
- comments on....xi

N

notice icons....ix

P

packet mirroring....7

R

RADIUS (Remote Authentication Dial-In User Service)
- change of authority messages....3
- disconnect messages....3
- RADIUS dynamic-request server....3

RADIUS commands
- authorization change....24
- baseline radius dynamic-request....38
- key....25
- radius dynamic-request server....27
- subscriber disconnect....28
- udp-port....29

radius dynamic-request
- platform....4

RADIUS dynamic-request server
- change of authorization messages....7
- disconnect messages....9
- how it works....9
- message exchange....7, 10
- overview....3
- qualifications for disconnect....10
- security and authentication....10

RADIUS-initiated change of authorization
- qualifications for change of authorization....7

RADIUS-initiated COA
- configuring....19

RADIUS-initiated disconnect
- configuring....20
- L2TP LAC users....11
- references....4
- sample network....4
- security and authentication....7

S

show radius commands
- show radius dynamic-request servers....34
- show radius dynamic-request statistics....33
- show radius servers....34
- show radius statistics....33

support, technical *See* technical support

T

technical support
- contacting JTAC....xii

text and syntax conventions....x