



JunosE™ Software for E Series™ Broadband Services Routers

RADIUS Relay Server

Release

14.1.x



Published: 2012-12-20

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

Copyright © 2012, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

JunosE™ Software for E Series™ Broadband Services Routers RADIUS Relay Server
Release 14.1.x
Copyright © 2012, Juniper Networks, Inc.
All rights reserved.

Revision History
December 2012—FRS JunosE 14.1.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	xi
	Self-Help Online Tools and Resources	xii
	Opening a Case with JTAC	xii
Part 1	Overview	
Chapter 1	How the RADIUS Relay Server Works	3
	Understanding the RADIUS Relay Server	3
	How RADIUS Relay Server Works	4
	Authentication and Addressing	4
	Accounting	5
	Terminating the Wireless Subscriber's Connection	5
	RADIUS Relay Server Platform Considerations	6
	RADIUS Relay Server References	6
Chapter 2	Interworking with SRC Software	7
	RADIUS Relay Server and the SRC Software	7
	Using the SRC Software for Addressing	7
	Using the SRC Software for Accounting	7
Part 2	Configuration	
Chapter 3	Configuration Task for RADIUS Relay Server	11
	Configuring RADIUS Relay Server Support	11
Chapter 4	RADIUS Relay Server Statistics	13
	Setting a Baseline for RADIUS Relay Statistics	13
Chapter 5	Configuration Commands	15
	baseline radius relay	16
	key	17
	radius relay server	19
	subscriber disconnect	20
	udp-port	21

Part 3	Administration	
Chapter 6	Monitoring Tasks	25
	Monitoring the Configuration of the RADIUS Relay Server	25
	Monitoring the Status of RADIUS Relay UDP Checksums	26
	Monitoring RADIUS Relay Server Statistics	26
Chapter 7	Monitoring Commands	29
	show radius relay	30
	show radius relay udp-checksum	31
Part 4	Index	
	Index	35

List of Figures

Part 1	Overview	
Chapter 1	How the RADIUS Relay Server Works	3
	Figure 1: RADIUS Relay Server	4

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	x
	Table 2: Text and Syntax Conventions	x
Part 1	Overview	
Chapter 1	How the RADIUS Relay Server Works	3
	Table 3: Required RADIUS Access-Request Attributes	4
	Table 4: Required RADIUS Accounting Attributes	5
Part 3	Administration	
Chapter 6	Monitoring Tasks	25
	Table 5: show radius relay servers Output Fields	25
	Table 6: show radius relay udp-checksum Output Fields	26
	Table 7: show radius relay statistics Output Fields	27

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 xi

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.

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.	<ul style="list-style-type: none"> 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)
<i>Italic text like this</i>	<ul style="list-style-type: none"> Emphasizes words. Identifies variables. Identifies chapter, appendix, and book names. 	<ul style="list-style-type: none"> There are two levels of access: <i>user</i> and <i>privileged</i>. <i>clusterId</i>, <i>ipAddress</i>. <i>Appendix A, System Specifications</i>
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
<i>Italic text like this</i>	Represents variables.	<i>mask</i> , <i>accessListName</i>

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 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: <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

- [How the RADIUS Relay Server Works on page 3](#)
- [Interworking with SRC Software on page 7](#)

CHAPTER 1

How the RADIUS Relay Server Works

- [Understanding the RADIUS Relay Server on page 3](#)
- [RADIUS Relay Server Platform Considerations on page 6](#)
- [RADIUS Relay Server References on page 6](#)

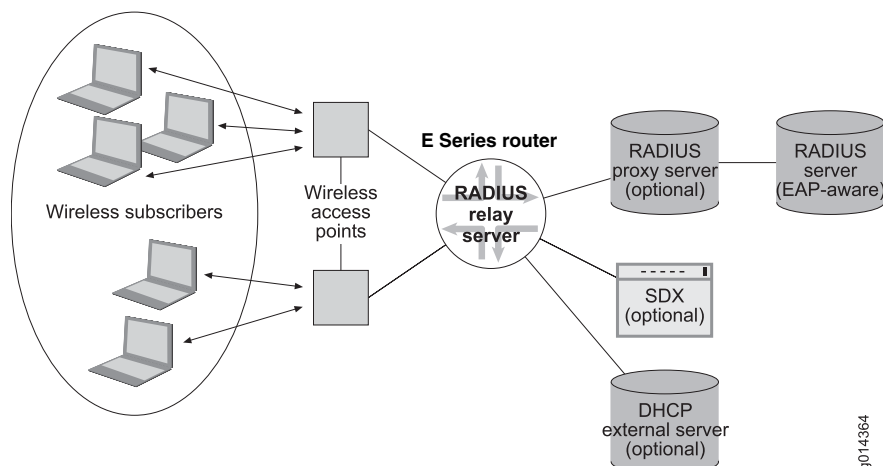
Understanding the RADIUS Relay Server

The JunosE RADIUS relay server provides authentication, authorization, accounting, and addressing services in an 802.1x-based wireless environment.

The IEEE 802.1x standard is an authentication standard for wireless LANs; it enables a wireless subscriber to be authenticated by a central authority. The standard uses the Extensible Authentication Protocol (EAP) for message exchange during the authentication process. The E Series router's RADIUS relay server enhances the 802.1x environment by including authorization, accounting, and addressing support for wireless subscribers.

[Figure 1 on page 4](#) illustrates a typical 802.1x-based wireless environment. In the figure, wireless subscribers connect to wireless access points (WAPs) for authentication. The WAPs in turn connect to the E Series router's RADIUS relay server. The RADIUS relay server passes the request on to the authentication server, which might be a RADIUS or TACACS+ server. The RADIUS server authenticates the subscriber, who is then granted access. After authentication, the RADIUS relay server obtains an IP address for the subscriber from the Dynamic Host Configuration Protocol (DHCP) local or external server. The RADIUS relay server can also use the RADIUS server or the optional Session and Resource Control (SRC) software (formerly the SDX software), to provide the accounting support.

Figure 1: RADIUS Relay Server



How RADIUS Relay Server Works

When a wireless subscriber starts a session, the WAP encapsulates EAP attributes into a RADIUS Access-Request message and sends the request to the E Series router, which the WAP views as the RADIUS server. The encapsulated message uses the RADIUS EAP-Message (79) attribute. The RADIUS relay server does not process any of the EAP attributes in the RADIUS Access-Request message; the encrypted message is simply passed through the router to the actual RADIUS server. The RADIUS server must be EAP aware.

You can also use an optional RADIUS proxy server to provide additional enhancements to the 802.1x-based environment. For example, the RADIUS proxy server enables subscribers to be multiplexed to multiple Internet service providers (ISPs) that are customers of the same carrier. The server performs one of the following actions:

- If the ISP's RADIUS server supports EAP, the RADIUS proxy server extends the EAP session to the RADIUS server.
- If the ISP's RADIUS server does not support EAP, the RADIUS proxy server translates the EAP session into a legacy RADIUS session for the RADIUS server.

Authentication and Addressing

The WAP initiates the authentication and authorization request by sending a standard RADIUS Access-Request to the RADIUS relay server. The Access-Request must include the attributes listed in [Table 3 on page 4](#). The attributes uniquely identify the wireless subscriber.

Table 3: Required RADIUS Access-Request Attributes

Attribute Name	Description
Called-Station-id [30]	Subscriber's WAP
Calling-Station-id [31]	Subscriber's media access control (MAC) address

When the RADIUS server authenticates the subscriber, the router's RADIUS relay server creates a RADIUS Access-Accept message and sends the message back to the subscriber. The router's DHCP server (either the router's DHCP local server or an external DHCP server) assigns an IP address to the subscriber and creates the subscriber interface.

For information about using the optional SRC software with the RADIUS relay server to assign IP addresses, see the *Using the SRC Software for Addressing* section in ["RADIUS Relay Server and the SRC Software"](#) on page 7.

The WAP might periodically reauthenticate a subscriber. For example, reauthentication is necessary to renegotiate a new Wired Equivalent Privacy (WEP) key. The RADIUS relay server ignores any new RADIUS attributes that are sent during a renegotiation operation.

Accounting

The RADIUS relay server's clients (the WAPs) send standard accounting request messages to the RADIUS relay server. The accounting server processes the request and sends the results back to the RADIUS relay server, which then creates a RADIUS accounting response message and forwards the information to the client WAP.

For tracking purposes, the forwarding RADIUS relay server adds the Radius-Client-Address vendor-specific attribute (VSA 26-52) to the forwarded accounting request messages. The VSA indicates the RADIUS relay server's IP address.

For information about using the SRC software with the RADIUS relay server to provide accounting, see the *Using the SRC Software for Addressing* section in ["RADIUS Relay Server and the SRC Software"](#) on page 7.

[Table 4 on page 5](#) shows the RADIUS attributes that must be included in accounting requests. The attributes uniquely identify subscribers.

Table 4: Required RADIUS Accounting Attributes

For RADIUS Acct-Start and Acct-Stop Messages	Description
Called-Station-id [30]	Subscriber's WAP
Calling-Station-id [31]	Subscriber's MAC address
For RADIUS Acct-On and Acct-Off Messages	
Called-Station-id [30]	Subscriber's WAP

Terminating the Wireless Subscriber's Connection

The RADIUS relay server terminates the wireless subscriber's session when one of the following events occurs. When a subscriber session is terminated, the subscriber's IP address is released back into the available address pool.

- The RADIUS relay server receives a RADIUS accounting stop request.
- No RADIUS accounting messages are received for this subscriber for more than 24 hours.

- Related Documentation**
- [RADIUS Relay Server and the SRC Software on page 7](#)
 - [Configuring RADIUS Relay Server Support on page 11](#)

RADIUS Relay Server Platform Considerations

RADIUS relay 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 the RADIUS Relay Server on page 3](#)
 - [RADIUS Relay Server References on page 6](#)

RADIUS Relay Server References

For more information about RADIUS relay server, see the following resources:

- IEEE 802.1x-2001—Port-Based Network Access Control
- RFC 2869—RADIUS Extensions (June 2000)
- RFC 2284—PPP Extensible Authentication Protocol (EAP) (March 1998)
- RFC 3539—Authentication, Authorization and Accounting (AAA) Transport Profile (June 2003)

- Related Documentation**
- [Understanding the RADIUS Relay Server on page 3](#)
 - [RADIUS Relay Server Platform Considerations on page 6](#)

CHAPTER 2

Interworking with SRC Software

- [RADIUS Relay Server and the SRC Software on page 7](#)

RADIUS Relay Server and the SRC Software

The SRC software is an advanced subscriber configuration and management service. The RADIUS relay server can optionally use the SRC software to perform addressing and accounting services for the subscriber and WAP.

The RADIUS relay server uses the E Series router's DHCP local server or DHCP external server and SRC client process to communicate with the SRC software.

Using the SRC Software for Addressing

If you integrate the SAE software into the RADIUS relay server configuration, the application can contribute to the address pool selection used to lease an address to the subscriber. The SRC software only contributes to address pool selection when the DHCP local server is used; it is not supported when a DHCP external server is used.

Using the SRC Software for Accounting

If you use the SRC software with the RADIUS relay server feature, two accounting domains might actually be created. The first domain is established by the WAP, when the subscriber is authenticated. The second domain is created for the connection between the E Series router and the SRC software.

If you want to continue to use the SRC software's user session and problem-tracking features, you should *not* configure the SRC software to generate RADIUS accounting records. Also, the following attributes must be configured on the RADIUS server used by the WAP:

- Service-Bundle [26-31]
- Class [25]
- User-Name [1]

Related Documentation

- [Understanding the RADIUS Relay Server on page 3](#)

PART 2

Configuration

- [Configuration Task for RADIUS Relay Server on page 11](#)
- [RADIUS Relay Server Statistics on page 13](#)
- [Configuration Commands on page 15](#)

Configuration Task for RADIUS Relay Server

- [Configuring RADIUS Relay Server Support on page 11](#)

Configuring RADIUS Relay Server Support

To configure the RADIUS relay server feature, you enable support for the feature on the E Series router and identify the key (secret) used for the connection between the WAP and the RADIUS relay server. The following example configures a RADIUS relay authentication server. Use similar steps to configure a RADIUS relay accounting server.



NOTE: The E Series router supports one instance of the RADIUS relay server per virtual router. The instance can provide authentication, authorization, and accounting support.

1. Enable RADIUS relay server support on the E Series router, and enter RADIUS Relay Configuration mode.

```
host1(config)#radius relay authentication server
host1(config-radius-relay)#
```

2. Specify the IP address and mask of the network that will use the relay authentication server, and the secret used during exchanges between the relay authentication server and clients (the WAPs).

```
host1(config-radius-relay)#key 192.168.25.9 255.255.255.255 mysecret
```

3. Specify the router's User Datagram Protocol (UDP) port on which the RADIUS relay server listens.

```
host1(config-radius-relay)#udp-port 1812
```

4. (Optional) Verify the configuration.

```
host1(config-radius-relay)#exit
host1(config)#exit
host1#show radius relay servers
```

RADIUS Relay Authentication Server Configuration

IP Address	IP Mask	Secret
192.168.25.9	255.255.255.255	mysecret

```
-----
10.10.15.0      255.255.255.0      secret
10.10.8.15     255.255.255.255    newsecret
192.168.25.9   255.255.255.255    mysecret
192.168.102.5  255.255.255.255    999Y2K
Udp Port: 1812
```

RADIUS Relay Accounting Server Configuration

```
-----
IP Address      IP Mask      Secret
-----
10.10.1.0       255.255.255.0  N08pxq
192.168.102.5   255.255.255.255 12BE$56
Udp Port: 1813
```

**Related
Documentation**

- [Setting a Baseline for RADIUS Relay Statistics on page 13](#)
- [Monitoring RADIUS Relay Server Statistics on page 26](#)
- [Monitoring the Configuration of the RADIUS Relay Server on page 25](#)
- [Monitoring the Status of RADIUS Relay UDP Checksums on page 26](#)

CHAPTER 4

RADIUS Relay Server Statistics

- [Setting a Baseline for RADIUS Relay Statistics on page 13](#)

Setting a Baseline for RADIUS Relay Statistics

You can set a baseline for RADIUS relay statistics. To show baseline statistics, use the **delta** keyword with the **show radius relay** command.

To set a baseline for RADIUS relay statistics:

- Issue the **baseline radius relay** command:

```
host1#baseline radius relay
```

There is no **no** version.

Related Documentation

- [Monitoring RADIUS Relay Server Statistics on page 26](#)
- [baseline radius relay on page 16](#)

CHAPTER 5

Configuration Commands

baseline radius relay

Syntax baseline radius relay

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets a baseline for RADIUS relay 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

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 relay server

Syntax radius relay { authentication | accounting } server
 no radius relay [{ authentication | accounting } server]

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures a RADIUS relay authentication or accounting server, and enters RADIUS Relay Configuration mode. The **no** version deletes all RADIUS relay servers or the specific authentication or accounting server.

Options • authentication—Configure the RADIUS relay authentication server
 • accounting—Configure the RADIUS relay accounting server

Mode Global Configuration

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 25](#)
- [Monitoring Commands on page 29](#)

CHAPTER 6

Monitoring Tasks

- [Monitoring the Configuration of the RADIUS Relay Server on page 25](#)
- [Monitoring the Status of RADIUS Relay UDP Checksums on page 26](#)
- [Monitoring RADIUS Relay Server Statistics on page 26](#)

Monitoring the Configuration of the RADIUS Relay Server

Purpose Display information about the RADIUS relay server configuration.

Action To display the RADIUS relay server configuration:

```
host1#show radius relay servers
```

RADIUS Relay Authentication Server Configuration

IP Address	IP Mask	Secret
10.10.8.15	255.255.255.255	newsecret
192.168.102.5	255.255.255.255	999Y2K

Udp Port: 1812

RADIUS Relay Accounting Server Configuration

IP Address	IP Mask	Secret
10.10.1.0	255.255.255.0	N08pxq
192.168.102.5	255.255.255.255	12BE\$56

Udp Port: 1813

Meaning [Table 5 on page 25](#) lists the **show radius relay servers** command output fields.

Table 5: show radius relay servers Output Fields

Field Name	Field Description
IP Address	Address of the RADIUS relay server
IP Mask	Mask of the RADIUS relay server
Secret	Secret used for exchanges between the RADIUS relay server and client
Udp Port	Router's port on which the RADIUS relay server listens

Related Documentation • [show radius relay on page 30](#) servers

Monitoring the Status of RADIUS Relay UDP Checksums

Purpose Display status of RADIUS relay UDP checksums.

Action To display the status of UDP checksums:

```
host1(config)#show radius relay udp-checksum
udp-checksums enabled
```

Meaning [Table 6 on page 26](#) lists the **show radius relay udp-checksum** command output fields.

Table 6: show radius relay udp-checksum Output Fields

Field Name	Field Description
udp-checksums	Status of UDP checksums: enabled or disabled

Related Documentation • [show radius relay on page 30](#) udp-checksum

Monitoring RADIUS Relay Server Statistics

Purpose Display RADIUS relay server statistics.

Action To show RADIUS relay server statistics that were baselined:

```
host1#show radius relay statistics delta

RADIUS Relay Authentication Server Statistics
-----
Statistic      Total
-----
Access Requests 1000
Access Accepts  1000
Access Challenges 0
Access Rejects  0
Pending Requests 0
Duplicate Requests 0
Malformed Requests 0
Bad Authenticators 0
Unknown Requests 0
Dropped Packets  0
Invalid Requests 0
Statistics baseline set FRI APR 02 2004 19:01:52 UTC

RADIUS Relay Accounting Server Statistics
-----
Statistic      Total
-----
Accounting Requests 1000
  Start              1000
  Stop               0
  Interim             0
Accounting Responses 1000
```

```

      Start          1000
      Stop           0
      Interim        0
Pending Requests    0
Duplicate Requests  0
Malformed Requests  0
Bad Authenticators  0
Unknown Requests    0
Dropped Packets     0
Invalid Requests    0
Statistics baseline set FRI APR 02 2004 19:01:52 UTC

```

Meaning [Table 7 on page 27](#) lists the **show radius relay statistics** command output fields.

Table 7: show radius relay statistics Output Fields

Field Name	Field Description
Access Requests	Number of access requests received
Access Accepts	Number of access accepts received
Access Challenges	Number of access challenges received
Access Rejects	Number of access rejects received
Pending Requests	Number of access requests waiting for a response
Duplicate Requests	Number of duplicate requests received while the previous request is pending
Malformed Requests	Requests with attributes having an invalid length or unexpected attributes
Bad Authenticators	Authenticator in the response is incorrect for the matching request; can occur if the secret for the RADIUS relay server and the WAP does not match
Unknown Requests	Packets received from nonconfigured clients
Dropped Packets	Packets dropped because of queue overflow
Invalid Requests	Number of invalid requests received
Accounting Requests	Number of accounting requests received, broken down by type of request
Accounting Responses	Number of accounting responses, broken down by type of request

- Related Documentation**
- [Setting a Baseline for RADIUS Relay Statistics on page 13](#)
 - [show radius relay on page 30](#) statistics

CHAPTER 7

Monitoring Commands

show radius relay

Syntax show radius relay [authentication | accounting]
{ servers | statistics [*ipAddress*] [delta] } [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about RADIUS relay authentication and accounting servers.

- Options**
- authentication—Displays authentication information only
 - accounting—Displays accounting information only
 - servers—Displays a list of authentication and/or accounting servers
 - statistics—Displays authentication and/or accounting statistics
 - *ipAddress*—Address of a RADIUS relay client for which statistics are displayed
 - delta—Displays baselined statistics
 - *filter*—See Filtering show Commands

Mode Privileged Exec

show radius relay udp-checksum

Syntax show radius relay udp-checksum [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about RADIUS relay UDP checksums.

Options • *filter*—See Filtering show Commands

Mode Privileged Exec

PART 4

Index

- [Index on page 35](#)

Index

B

B-RAS commands

baseline radius relay.....	16
key.....	17
radius relay server.....	19
show radius relay.....	30
show radius relay udp-checksum.....	30
subscriber disconnect.....	20
udp-port.....	21

baseline commands

baseline radius relay.....	13
----------------------------	----

C

conventions

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

customer support.....xi

contacting JTAC.....	xi
----------------------	----

D

documentation set

comments on.....	xi
------------------	----

I

IPsec commands

key.....	17
----------	----

M

manuals

comments on.....	xi
------------------	----

N

notice icons.....	ix
-------------------	----

R

radius commands

radius relay server.....	11
radius relay udp-checksum.....	11

RADIUS commands

baseline radius relay.....	16
key.....	17

radius relay server.....	19
show radius relay.....	30
show radius relay udp-checksum.....	30
subscriber disconnect.....	20
udp-port.....	21

radius relay

platform.....	6
---------------	---

RADIUS Relay Server.....3

SRC Software.....	7
-------------------	---

RADIUS relay server

configuring.....	11
------------------	----

S

show radius relay commands

show radius relay servers.....	25
show radius relay statistics.....	26
show radius relay udp-checksum.....	26

support, technical See technical support

T

technical support

contacting JTAC.....	xi
----------------------	----

text and syntax conventions.....x

