RADIUS for Multiple UDP Ports

RADIUS security servers are identified on the basis of their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific authentication, authorization, and accounting (AAA) service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as a failover backup to the first one. If the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RADIUS for Multiple UDP Ports

To configure RADIUS on your Cisco device or access server, you must perform these tasks:

- Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use RADIUS.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.
- Use **line** and **interface** commands to enable the defined method lists to be used.

Information About RADIUS for Multiple UDP Ports

Device-to-RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (CiscoSecure ACS), Livingston, Merit, Microsoft, or another software provider. Configuring device to RADIUS server communication can have several components:

- Hostname or IP address
- Authentication destination port
- Accounting destination port
- Timeout period
- Retransmission value
- Key string

RADIUS security servers are identified on the basis of their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as a failover backup to the first one. If the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order they are configured.)

A RADIUS server and a Cisco device use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the device.

The timeout, retransmission, and encryption key values are configurable globally for all RADIUS servers, on a per-server basis or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the device, use the three unique global commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** command.

Note You can configure both global and per-server timeout, retransmission, and key value commands simultaneously on the same Cisco network access server. If both global and per-server functions are configured on a device, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands.

How to Configure RADIUS for Multiple UDP Ports

Configuring Device-to-RADIUS Server Communication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]
4. **radius-server key** {**0** *string* | **7** *string* | *string*}
5. **radius-server retransmit** *retries*
6. **radius-server timeout** *seconds*
7. **radius-server deadtime** *minutes*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout**	Specifies the IP address or hostname of the remote RADIUS server host and assigns authentication and accounting destination port numbers. **Note** In this step, the timeout, retransmission, and encryption key values are configured on a per-server basis.

	Command or Action	Purpose
	seconds] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] **Example:** `Device(config)# radius-server host 10.45.1.2`	• **auth-port** *port-number***—**configures a specific UDP port on this RADIUS server to be used solely for authentication. • **acct-port** *port-number***—**configures a specific UDP port on this RADIUS server to be used solely for accounting. • **alias—**configures up to eight multiple IP addresses for use when referring to RADIUS servers. • To configure the network access server to recognize more than one host entry associated with a single IP address, repeat this command as many times as necessary, making sure that each UDP port number is different. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host. • If no timeout is set, the global value is used; otherwise, enter a value from 1 to 1000. If no retransmit value is set, the global value is used; otherwise, enter a value from 1 to 1000. If no key string is specified, the global value is used. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Step 4	**radius-server key** {**0** *string* | **7** *string* | *string*}
	Example:
	`Device(config)# radius-server key myRaDIUSpassword`
		Specifies the shared secret text string used between the device and a RADIUS server.
		Note In this step, the encryption key value is configured globally for all RADIUS servers.
		• Use the **0** *string* option to configure an unencrypted shared secret. Use the **7** *string* option to configure an encrypted shared secret.

Step 5	**radius-server retransmit** *retries* **Example:** `Device(config)# radius-server retransmit 25`	Specifies how many times the device transmits each RADIUS request to the server before giving up (the default is 3). **Note** In this step, the retransmission value is configured globally for all RADIUS servers.
Step 6	**radius-server timeout** *seconds* **Example:** `Device(config)# radius-server timeout 6`	Specifies for how many seconds a device waits for a reply to a RADIUS request before retransmitting the request. **Note** In this step, the timeout value is configured globally for all RADIUS servers.

	Command or Action	Purpose
Step 7	**radius-server deadtime** *minutes* **Example:** `Device(config)# radius-server deadtime 5`	Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.
Step 8	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Configuration Examples for RADIUS for Multiple UDP Ports

Example: Device-to-RADIUS Server Communication

The following example shows how to configure two RADIUS servers with specific timeout, retransmit, and key values. In this example, the **aaa new-model** command enables AAA services on the device, and specific AAA commands define the AAA services. The **radius-server retransmit** command changes the global retransmission value to 4 for all RADIUS servers. The **radius-server host** command configures specific timeout, retransmission, and key values for the RADIUS server hosts with IP addresses 172.16.1.1 and 172.29.39.46.

```
! Enable AAA services on the device and define those services.
aaa new-model
aaa authentication login default group radius
aaa authentication login console-login none
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
enable password tryit1
!
! Change the global retransmission value for all RADIUS servers.
radius-server retransmit 4
!
! Configure per-server specific timeout, retransmission, and key values.
! Change the default auth-port and acct-port values.
radius-server host 172.16.1.1 auth-port 1612 acct-port 1616 timeout 3 retransmit 3 key
radkey
!
! Configure per-server specific timeout and key values. This server uses the global
! retransmission value.
radius-server host 172.29.39.46 timeout 6 key rad123
```

Example: RADIUS Server with Server-Specific Values

The following example shows how to configure server-specific timeout, retransmit, and key values for the RADIUS server with IP address 172.31.39.46:

```
radius-server host 172.31.39.46 timeout 6 retransmit 5 key rad123
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
AAA and RADIUS commands	*Cisco IOS Security Command Reference*
AAA	*Authentication, Authorization, and Accounting Configuration Guide* (part of the Securing User Services Configuration Library)

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RADIUS for Multiple UDP Ports

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for RADIUS for Multiple UDP Ports

Feature Name	Releases	Feature Information
RADIUS for Multiple UDP Ports	Cisco IOS XE Release 3.2SE	RADIUS security servers are identified on the basis of their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. The following command was introduced or modified: **radius-server host**.