RADIUS Packet of Disconnect

Last Updated: January 17, 2012

The RADIUS Packet of Disconnect feature is used to terminate a connected voice call.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 Packet of Disconnect

Configure AAA as described in the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2.

Restrictions for RADIUS Packet of Disconnect

Proper matching identification information must be communicated by the following:

- Billing server and gateway configuration

- Gateway's original accounting start request
- Server's POD request

Information About RADIUS Packet of Disconnect

The Packet of Disconnect (POD) is a RADIUS access_request packet and is intended to be used in situations where the authenticating agent server wants to disconnect the user after the session has been accepted by the RADIUS access_accept packet.

When the POD is Needed

The POD may be needed in at least two situations:

- Detection of fraudulent use, which cannot be performed before accepting the call. A price structure so complex that the maximum session duration cannot be estimated before accepting the call. This may be the case when certain types of discounts are applied or when multiple users use the same subscription simultaneously.
- To prevent unauthorized servers from disconnecting users, the authorizing agent that issues the POD packet must include three parameters in its packet of disconnect request. For a call to be disconnected, all parameters must match their expected values at the gateway. If the parameters do not match, the gateway discards the packet of disconnect packet and sends a NACK (negative acknowledgement message) to the agent.

POD Parameters

The POD has the following parameters:

- An h323-conf-id vendor-specific attribute (VSA) with the same content as received from the gateway for this call.
- An h323-call-origin VSA with the same content as received from the gateway for the leg of interest.
- A 16-byte MD5 hash value that is carried in the *authentication* field of the POD request.
- Cisco IOS XE software allocates POD code 50 as the code value for the Voice POD Request based on RFC 3576 *Dynamic Authorization Extensions to RADIUS*, which extends RADIUS standards to officially support both a Disconnect Message (DM) and Change-of-Authorization (CoA) that are supported through the POD.

RFC 3576 specifies the following POD codes:

-
  - 40 - Disconnect-Request
  - 41 - Disconnect-ACK
  - 42 - Disconnect-NAK
  - 43 - CoA-Request
  - 44 - CoA-ACK
  - 45 - CoA-NAK

How to Configure the RADIUS Packet of Disconnect

Configuring the RADIUS POD

Use the following tasks to configure the RADIUS POD:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router (config)# **aaa pod server** [**port** *port-number*] [**auth-type** {**any**| **all**| **session-key**}] **server-key** [*encryption-type*] *string*
4. Router# **end**
5. Router# **show running-configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	Router (config)# **aaa pod server** [**port** *port-number*] [**auth-type** {**any**| **all**| **session-key**}] **server-key** [*encryption-type*] *string* **Example:** `Router(config)#` **aaa pod server server-key xyz123**	Enables inbound user sessions to be disconnected when specific session attributes are presented, where: • **port** *port-number* --(Optional) The network access server User Datagram Protocol (UDP) port to use for POD requests. Default value is 1700. • **auth-type** --(Optional) The type of authorization required for disconnecting sessions. ◦ **any**--Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key). ◦ **all**--Only a session that matches all four key attributes is disconnected. **All**is the default. ◦ **session-key**--Session with a matching session-key attribute is disconnected. All other attributes are ignored. • **server-key--** Configures the shared-secret text string. • *encryption-type* --(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using an encryption algorithm defined by Cisco. • *string*-- The shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.
Step 4	Router# **end**	Exits global configuration mode and returns to privileged EXEC mode.

Command or Action	Purpose

Step 5 Router# **show running-configuration**
 	
Example:
`Router# show running-configuration`
 	
Example:
`!`
 	
Example:
`aaa authentication login h323 group radius`
 	
Example:
`aaa authorization exec h323 group radius`
 	
Example:
`aaa accounting update newinfo`
 	
Example:
`aaa accounting connection h323 start-stop group radius`
 	
Example:
`aaa pod server server-key cisco`
 	
Example:
`aaa session-id common`
 	
Example:
`!`
	Verifies that the gateway is configured correctly in privileged EXEC mode.

- Troubleshooting Tips, page 5

Troubleshooting Tips

Use the following tips to troubleshoot POD issues:

- Ensure that the POD port is configured correctly in both the gateway (using **aaa pod server**command) and the radius server. Both should be the same.
- Ensure that the shared-secret key configured in the gateway (using **aaa pod server**command) and in the AAA server are the same.
- Turn on **debug aaa pod** command to see what's going on. This will let you know if the gateway receives the POD packet from the server and if so, it will display any errors encountered.

The following example shows output from a successful POD request, when using the **show debug** command.

```
Router# debug aaa podAAA POD packet processing debugging is on
Router# show debugGeneral OS:
  AAA POD packet processing debugging is on
Router#
Apr 25 17:15:59.318:POD:172.19.139.206 request queued
Apr 25 17:15:59.318:voice_pod_request:
Apr 25 17:15:59.318:voip_populate_pod_attr_list:
Apr 25 17:15:59.318:voip_pod_get_guid:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=50
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr=h323-conf-id
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=50 value_len=35
Apr 25 17:15:59.318:voip_pod_get_guid:conf-id=FFA7785F F7F607BB
00000000 993FB1F4 n_bytes=35
Apr 25 17:15:59.318:voip_pod_get_guid:GUID = FFA7785F F7F607BB 00000000
993FB1F4
Apr 25 17:15:59.318:voip_populate_pod_attr_list:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=23
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr=h323-originate
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=23 value_len=6
Apr 25 17:15:59.318:voip_get_call_direction:
Apr 25 17:15:59.318:voip_get_call_direction:returning answer
Apr 25 17:15:59.318:voip_eval_pod_attr:
Apr 25 17:15:59.318:cc_api_trigger_disconnect:
Apr 25 17:15:59.322:POD:Sending ACK to 172.19.139.206/1700
Apr 25 17:15:59.322:voip_pod_clean:
```

Verifying the RADIUS POD Configuration

To verify the RADIUS POD configuration, use the **show running configuration** privileged EXEC command as shown in the following example:

```
Router# show running-configuration
!
aaa authentication login h323 group radius
aaa authorization exec h323 group radius
aaa accounting update newinfo
aaa accounting connection h323 start-stop group radius
aaa pod server server-key cisco
aaa session-id common
.
.
.
```

Additional References

The following sections provide references related to the RADIUS Packet of Disconnect feature.

Related Documents

Related Topic	Document Title
AAA	Authentication, Authorization, and Accounting (AAA) section of the *Cisco IOS XE Security Configuration Guide, Securing User Services*, Release 2.
Security commands	*Cisco IOS Security Command Reference*
CLI Configuration	*Cisco IOS XE Configuration Fundamentals Configuration Guide*, Release 2

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	*Remote Authentication Dial-in User Service*
RFC 3576	*Dynamic Authorization Extensions to RADIUS*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for RADIUS Packet of Disconnect

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 Packet of Disconnect

Feature Name	Releases	Feature Information
RADIUS Packet of Disconnect	Cisco IOS XE Release 2.1	The RADIUS Packet of Disconnect feature is used to terminate a connected voice call. In Cisco IOS XE Release 2.1, this feature was introduced on the on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **aaa pod server, debug aaa pod**

Glossary

AAA --authentication, authorization, and accounting.

NACK --negative acknowledgement message.

POD --packet of disconnect. An access_reject packet sent from a RADIUS server to the gateway in order to disconnect a call which has been connected already. After validation of the packet, the gateway disconnects the user. The packet contains the information to disconnect the call.

POD server--a Cisco gateway configured to accept and process POD requests from a RADIUS authentication/authorization agent.

RADIUS --Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet service providers.

UDP --User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

VoIP-- voice over IP. The ability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP is a blanket term that generally refers to the Cisco standards-based (for example, H.323) approach to IP voice traffic.

VSA --vendor-specific attribute.