



# RADIUS Packet of Disconnect

---

## Feature History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(2)XB	Support for the voice applications as well as support for the Cisco AS5350, Cisco AS5400, and Cisco 3600 series routers was added.
12.2(2)XB1	Support for the Cisco AS5800 was added.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T and support for the Cisco AS5850 was added.

This document describes the RADIUS Packet of Disconnect feature in Cisco IOS Release 12.2(11)T. It includes the following sections.

[Feature Overview, page 1](#)

[Supported Platforms, page 3](#)

[Supported Standards, MIBs, and RFCs, page 5](#)

[Prerequisites, page 5](#)

[Configuration Tasks, page 5](#)

[Configuration Examples, page 8](#)

[Command Reference, page 8](#)

[Glossary, page 13](#)

## Feature Overview

This feature consists of a method for terminating a call that has already been connected. This “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. This 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.

The parameters are the following:

- 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.

## Benefits

- Ability to terminate an in-progress voice call

## Restrictions

Proper matching identification information must be communicated by the:

- billing server and gateway configuration
- the gateway's original accounting start request
- the server's POD request

## Related Features and Technologies

- AAA, documented in the *Cisco IOS Security Configuration Guide*, Release 12.2

## Related Documents

- *Cisco IOS Security Configuration Guide*, Release 12.2
- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2
- *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2
- *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2

# Supported Platforms

- Cisco 3600 series
- Cisco AS5300
- Cisco AS5350
- Cisco AS5400
- Cisco AS5800
- Cisco AS5850

**Table 1** Release and Platform Support for this Feature

Platform	First Limited Cisco IOS Lifetime Release	First Cisco IOS T Release
<b>Cisco 3600 Series</b>	12.2(2)XB	12.2(11)T
<b>Cisco 5300</b>	12.1(2)XH	12.1(3)T
<b>Cisco 5350</b>	12.2(2)XB	12.2(11)T
<b>Cisco 5400</b>	12.2(2)XB	12.2(11)T
<b>Cisco 5800</b>	12.1(2)XH	12.1(3)T
<b>Cisco 5850</b>	X	12.2(11)T

## Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

**Availability of Cisco IOS Software Images**

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

# Supported Standards, MIBs, and RFCs

## Standards

None

## MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB web site on Cisco.com at

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

## RFCs

- RFC 2865, *Remote Authentication Dial-in User Service*

## Prerequisites

- Configure AAA as described in *Cisco IOS Security Configuration Guide*, Cisco IOS Release 12.2.
- Use Cisco IOS Release 12.2(11)T or later.

## Configuration Tasks

See the following sections for configuration tasks for this Packet of Disconnect feature. Each task in the list is identified as either required or optional.

- [Configuring AAA POD Server](#) (required)
- [Verifying AAA POD Server](#) (optional)

## Configuring AAA POD Server

To configure POD, perform the following tasks in global configuration mode:

Command	Purpose
<b>Step 1</b> Router(config)# <b>aaa pod server</b> [ <b>port</b> <i>port-number</i> ] [ <b>auth-type</b> { <b>any</b>   <b>all</b>   <b>session-key</b> }] <b>server-key</b> [ <i>encryption-type</i> ] <i>string</i>	<p>Enables inbound user sessions to be disconnected when specific session attributes are presented.</p> <p><b>port</b> <i>port-number</i>—(Optional) The network access server User Datagram Protocol (UDP) port to use for POD requests. Default value is 1700.</p> <p><b>auth-type</b>—(Optional) The type of authorization required for disconnecting sessions.</p> <p><b>any</b>—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).</p> <p><b>all</b>—Only a session that matches all four key attributes is disconnected. <b>All</b> is the default.</p> <p><b>session-key</b>—Session with a matching session-key attribute is disconnected. All other attributes are ignored.</p> <p><b>server-key</b>—Configures the shared-secret text string.</p> <p><i>encryption-type</i>—(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.</p> <p><i>string</i>—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.</p>

## Verifying AAA POD Server

To verify that the gateway is configured correctly to perform as an AAA POD server, enter the **show running-configuration** command in privileged EXEC mode to display the command settings for the router.

```
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
!
```

## Troubleshooting Tips

- 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 pod
AAA POD packet processing debugging is on
Router# show debug
General 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:
```

# Configuration Examples

This section provides a configuration example for a gateway performing as an AAA POD server:

- [AAA POD Server Example](#)

## AAA POD Server Example

```
Router(config)# aaa pod server server-key xyz123
```

## Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [aaa pod server](#)
- [debug aaa pod](#)

## aaa pod server

To enable inbound user sessions to be disconnected when specific session attributes are presented, use the **aaa pod server** global configuration command. To disable this feature, use the **no** form of this command.

```
aaa pod server [port port number] [auth-type {any | all | session-key}] server-key
[encryption-type] string
```

```
no aaa pod server
```

Syntax	Description
<b>port</b> <i>port number</i>	(Optional) The network access server UDP port to use for POD requests. Default value is 1700.
<b>auth-type</b>	(Optional) The type of authorization required for disconnecting sessions.
<b>any</b>	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).
<b>all</b>	Only a session that matches all four key attributes is disconnected. <b>All</b> is the default.
<b>session-key</b>	Session with a matching session-key attribute is disconnected. All other attributes are ignored.
<b>server-key</b>	Configures the shared-secret text string.
<i>encryption-type</i>	(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Currently 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.
<i>string</i>	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.

**Defaults** The POD server function is disabled.

**Command Modes** Global configuration

**Command History**

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(2)XB	The <i>encryption-type</i> argument was added, as well as support for the voice applications and the Cisco AS5350, Cisco AS5400 and Cisco 3600 series routers.
12.2(2)XB1	Support for the Cisco AS5800 was added.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support for the Cisco AS5850 was added.

**Usage Guidelines**

To disconnect a session, the values in one or more of the key fields in the POD request must match the values for a session on one of the network access server ports. Which values must match depends on the **auth-type** attribute defined in the command. If no auth-type is specified, all three values must match. If no match is found, all connections remain intact and an error response is returned. The key fields are as follows:

- 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.

**Examples**

The following example enables POD and sets the secret key to “xyz123.”

```
Router(config)# aaa pod server server-key xyz123
```

**Related Commands**

Command	Description
<b>debug aaa pod</b>	Displays debug messages for POD packets.
<b>aaa authentication</b>	Enables authentication.
<b>aaa accounting</b>	Enables accounting records.
<b>aaa accounting delay-start</b>	Delays generation of the start accounting record until the user IP address is established.
<b>radius-server host</b>	Identifies a RADIUS host.

# debug aaa pod

To display debug messages related to POD packets, use the **debug aaa pod** privileged EXEC command. To disable debugging output, use the **no** form of this command.

**debug aaa pod**

**no debug aaa pod**

## Syntax Description

This command has no keywords or arguments.

## Defaults

Debugging for POD packets is not enabled.

## Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB	Support for the voice applications aas well as support for the Cisco AS5350, Cisco AS5400 and the Cisco 3600 series was added.
12.2(2)XB1	Support for the Cisco AS5800 was added.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support for the Cisco AS5850 was added.

## Examples

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

```
Router# debug aaa pod
AAA POD packet processing debugging is on
Router# show debug
General 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:
```

■ debug aaa pod

```
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:
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>aaa pod server</b>	Enables the POD feature.

---

# 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.

