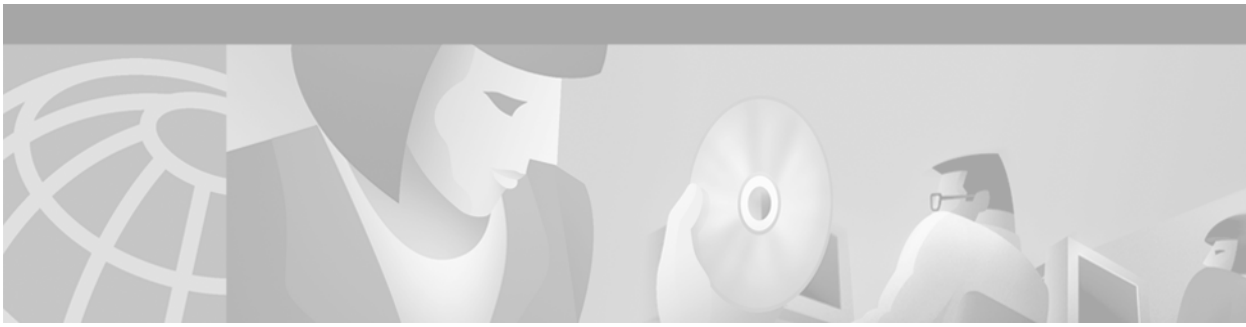


RADIUS Preauthentication for H.323 and SIP Voice Calls

Feature History

Release	Modification
12.2(11)T	This feature was introduced on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

This document describes the RADIUS Preauthentication for H.323 and SIP Voice Calls feature in Cisco IOS Release 12.2(11)T. It includes the following sections:

Feature Overview

The RADIUS Preauthentication for H.323 and SIP Voice Calls feature provides the means to evaluate and accept or reject call setup requests for both voice and dial calls received at universal gateways. This process is known as preauthentication. The feature also optionally allows voice calls to bypass this presetup evaluation.

With universal gateways, voice customers and dial customers contend for the same gateway resources. This competition can present problems for IP service wholesalers who lease their IP services to various customers such as Internet service providers (ISPs), Internet telephony service providers (ITSPs), and telephony application service providers (T-ASPs). Wholesalers need a way to implement and enforce with these customers service-level agreements (SLAs) that describe the levels of connectivity, performance, and availability that they guarantee to provide. The RADIUS Preauthentication for H.323 and SIP Voice Calls feature allows a wholesaler to determine whether a call is within SLA limits before gateway resources are dedicated to terminating the call.

With RADIUS preauthentication enabled, end customers from over-subscribed service providers are prevented from consuming ports that exceed the number allotted to their service provider in its SLA. If the call is accepted in the preauthentication step, it proceeds to full dial authentication and authorization or to voice dial-peer matching and voice session application authentication and authorization.

RADIUS preauthentication uses a RADIUS-based port-policy management (PPM) server, such as the Cisco Resource Policy Management System (RPMS), to interpret and enforce universal PPM and preauthentication SLAs. RADIUS provides the communication link between the PPM server and universal gateways.

Customer profiles are defined in the PPM server with information from the SLA. Then, when a call is received at the universal gateway, the server determines which specific customer SLA policy to apply to the call on the basis of information associated with the call. For example, calls can be identified as either dial or voice on the basis of the called number (also called the dialed number identification service number or DNIS). Then the PPM server might be set up to allow only a certain number of dial calls. When a new dial call is received, it is rejected if adding it to the count makes the count exceed the number of dial calls stipulated in the SLA.

Calls that are accepted by the PPM server continue with their normal call setup sequences after preauthentication. The response from the PPM server is returned to the calling entity—such as an ISDN or Session Initiation Protocol (SIP) call signaling interface—which then proceeds with the regular call flow. Calls that are rejected by the PPM server follow the given call model and apply the error codes or rejection reasons that are specified by the signaling entity.

Five scenarios are described below to illustrate the RADIUS Preauthentication for H.323 and SIP Voice Calls feature:

- Scenario 1: SIP-Based Voice Termination
- Scenario 2: H.323-Based Voice Termination
- Scenario 3: H.323-Based Voice Origination and Termination
- Scenario 4: H.323-Based Voice Origination and Termination with Prepaid Billing
- Scenario 5: Dial-Up (Modem) Call Origination

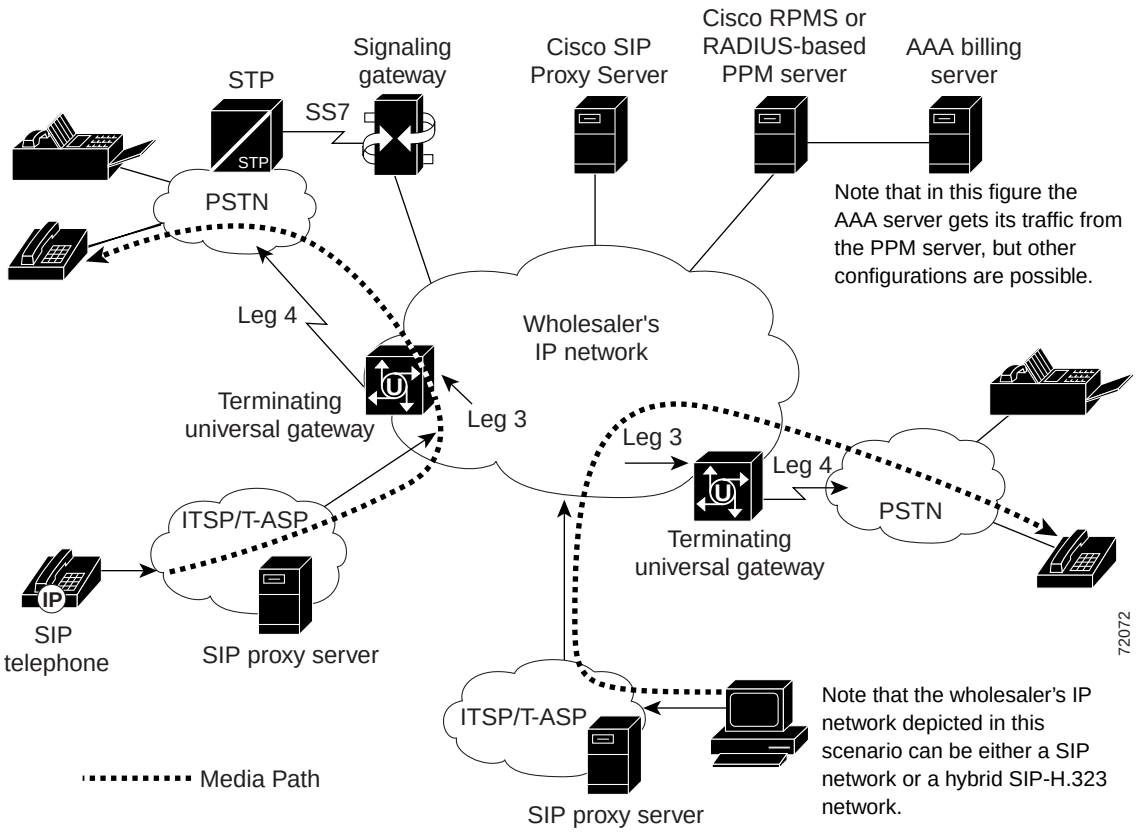
Note In all scenarios, gateway accounting must be enabled, and all call accounting information must be forwarded to the server that is performing preauthentication. Accounting stop packets must be sent to this server so that call billing is ended when calls are disconnected from the gateway. In addition, authentication and accounting start packets are needed to enable other features, such as virtual private dial-up network (VPDN).

Scenario 1: SIP-Based Voice Termination

In Scenario 1, a voice call from a SIP telephone or SIP terminal is sent from an ITSP to a wholesaler (Figure 1). In this scenario, the Cisco SIP Proxy Server (CSPS) chooses the appropriate universal gateway to which the SIP INVITE is forwarded, on the basis of its own routing mechanism. In this scenario, Step 3 is the preauthentication query that CSPS makes to the RPMS-based PPM server. CSPS locks out calls that are rejected by the RPMS-based PPM server. In Step 5 the universal gateway makes a preauthentication reservation request to the RPMS-based PPM server, which locks in the resources to handle the call.

Note This scenario requires CSPS 2.0.

Figure 1 SIP-based Voice Termination



Scenario 1 has the following call flow:

1. A SIP INVITE is sent from an end user's PC to an ITSP SIP proxy server.
2. The ITSP's SIP proxy server forwards the SIP INVITE to a CSPS at a wholesaler or ISP.
3. Preauthentication—The CSPS sends a preauthentication query to the RADIUS-based PPM server, which locates the appropriate SLA and makes sure that the call is within the SLA limits. If the call is outside the limits, the call is rejected and CSPS responds to the sender with an "Error code 480 - Temporarily not available" message. CSPS interaction with the RADIUS-based PPM server is optional and requires CSPS version 2.0 or a later release. If you are not using CSPS 2.0, the gateway makes the preauthentication query to the RADIUS-based PPM server if it has been configured to do so.
4. Gateway selection—If the preauthentication request is accepted, the CSPS uses its routing logic to determine the appropriate terminating universal gateway to which it should forward the INVITE.
5. Call admission control—If the preauthentication request is accepted, the terminating universal gateway checks its configured call admission control limits. If the call is outside the limits, the call is rejected.
6. Authentication and authorization—The universal gateway reserves a port and sends an authentication, authorization, and accounting (AAA) accounting start packet to the RADIUS-based PPM server.
7. The connection between the caller and the universal gateway is completed (call leg 3).
8. The caller is connected to the Public Switched Telephone Network (PSTN) (call leg 4).

9. Accounting stop—After the caller hangs up or is otherwise disconnected, the terminating universal gateway issues an accounting stop packet to the RADIUS-based PPM server. The PPM server uses the accounting stop packet to clear out the count for that call against the SLA.

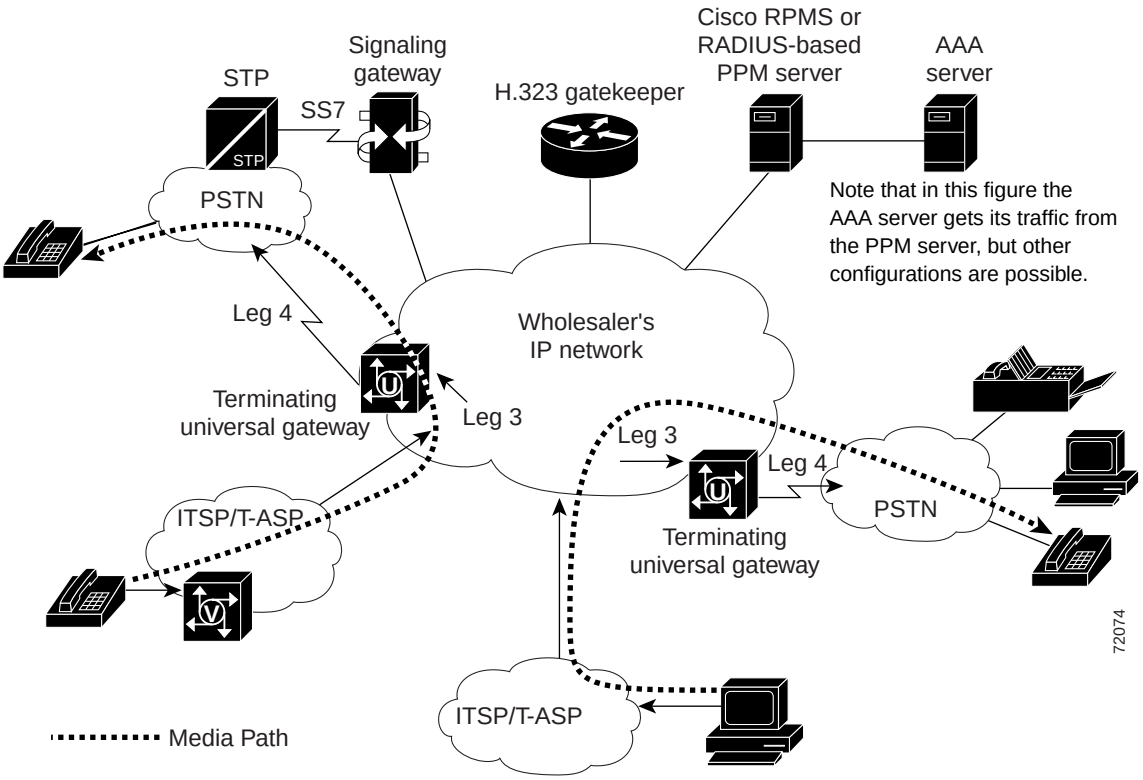
Scenario 2: H.323-Based Voice Termination

In Scenario 2, a Voice over IP (VoIP) call is received from an ITSP or T-ASP for transit over a wholesaler's IP network and then out to the PSTN (Figure 2). Note that for these calls, the call information that is passed can contain the Interzone ClearToken (IZCT), which includes:

- For intradomain calls, the origination gatekeeper zone name
- For interdomain calls, the origination domain border gatekeeper zone name

Whenever the IZCT information is available, it is used to preauthenticate H.323 VoIP calls. For more information on IZCT configuration, refer to *Inter-Domain Gatekeeper Security Enhancement*, Cisco IOS Release 12.2(4)T.

Figure 2 H.323-Based Voice Termination



In Scenario 2, a voice call originates from an Internet telephony service provider (ITSP) gateway or from a telephony application service provider (T-ASP) application. The call has the following flow:

1. If there is a Cisco gatekeeper as the terminating gatekeeper and Cisco RPMS as the RADIUS-based PPM server, SLA policy limits can be checked even before a call setup request is generated. The originating gatekeeper contacts the terminating gatekeeper to determine which gateway to use. The terminating gatekeeper communicates to the RPMS using Gatekeeper Transaction Message Protocol (GKTMP) to determine if accepting this call could violate current policy limits on the originator's access into the terminator's network. (Note that this capability is not available in Cisco IOS

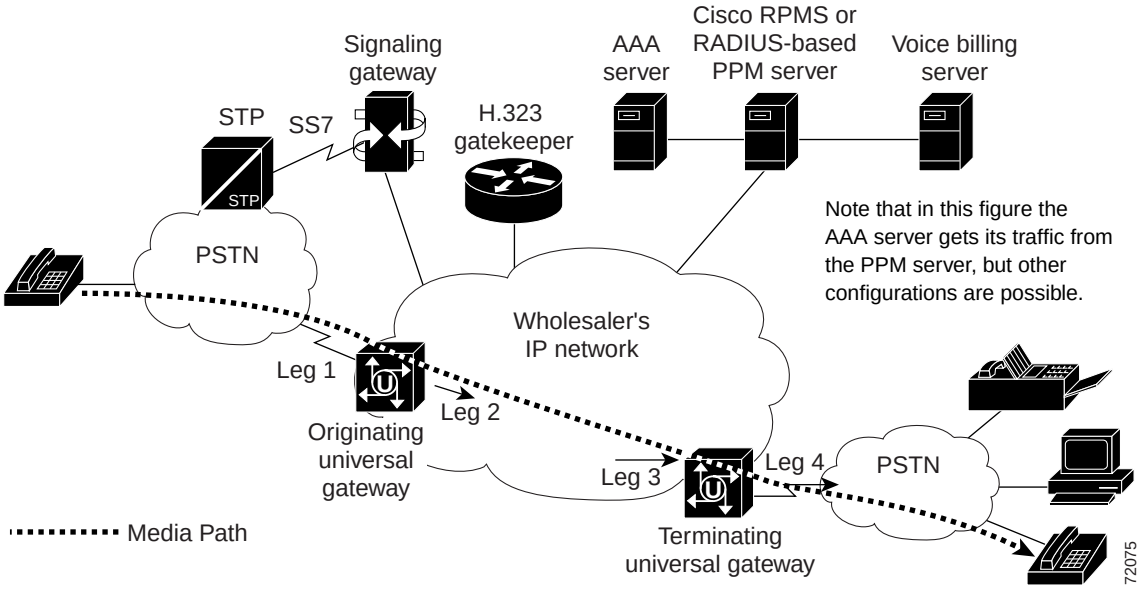
Release 12.2(11)T.) If accepting the call violates the policy, the terminating gatekeeper notifies the originating gatekeeper, which then searches for a new gateway to manage the call. If the call can be accepted, the originating gateway is free to generate a call setup request.

2. A call setup request from the IP network is received by a terminating universal gateway.
3. Preauthentication—Information about the call is sent in a preauthentication request from the universal gateway to a RADIUS-based PPM server. The server locates the appropriate SLA and makes sure that the call is within the SLA limits. If the call is outside the limits, the call is rejected and an error code is returned to the universal gateway.
4. Call admission control—If the preauthentication request is accepted, the terminating universal gateway checks the configured call admission control limits. If the call is outside the limits, the call is rejected.
5. Connection to terminating universal gateway—If adequate resources exist for the call, the call is accepted. Resources in the universal gateway are assigned to terminate the call, and the connection between the caller and the terminating universal gateway is completed (call leg 3).
6. Accounting start—An accounting start record is sent from the universal gateway to the RADIUS-based PPM server and the ISP's AAA server, which includes the resource selected. The AAA server is the billing server.
7. The caller is connected to the PSTN (call leg 4). An accounting start record is sent for each call leg.
8. Accounting stop—After the caller hangs up or is otherwise disconnected, the terminating universal gateway issues an accounting stop packet to the RADIUS-based PPM server. The PPM server uses the accounting stop packet to clear out the count for that call against the SLA. An accounting stop record is sent out for each call leg.

Scenario 3: H.323-Based Voice Origination and Termination

In Scenario 3, a voice caller from the PSTN dials into a long-distance provider and requires both call origination and termination services on the IP network (Figure 3). This scenario describes a complete VoIP call end-to-end. The terminating call flow is identical to the flow presented in Scenario 2.

Figure 3 H.323-Based Voice Origination and Termination



Scenario 3 has the following call flow:

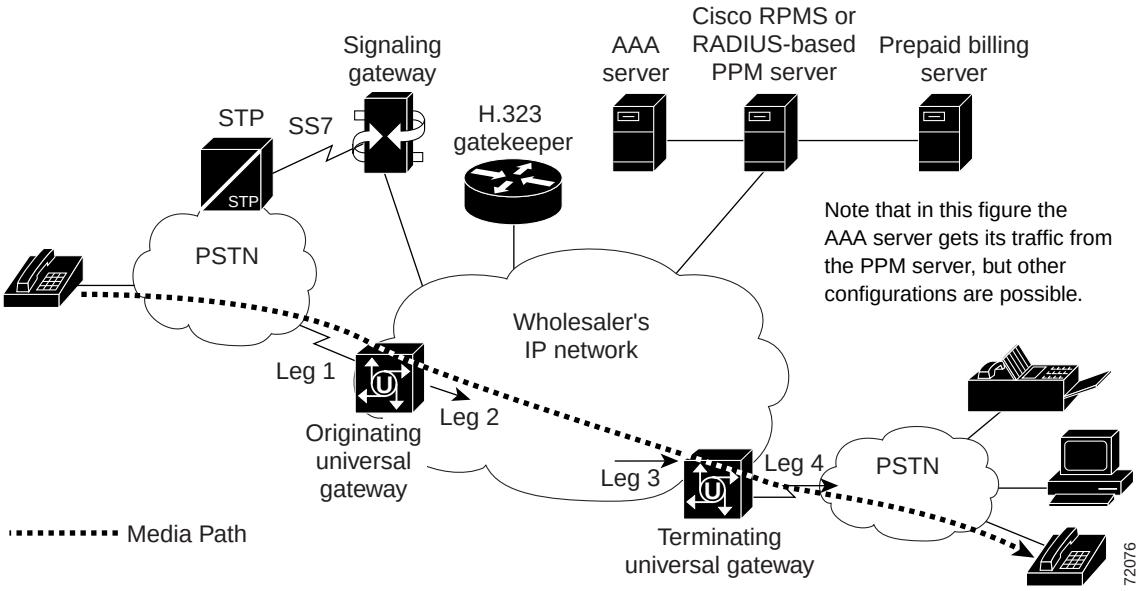
1. A call setup request from the PSTN is received by an originating universal gateway.
2. Call admission control on originating gateway—The universal gateway checks the configured call admission control limits. If the call is outside the limits, the call is rejected.
3. Preauthentication—If the call is accepted, information about the call is sent in a preauthentication request from the universal gateway to a RADIUS-based PPM server. The server locates the appropriate SLA that limits calls per customer or service, and makes sure that the current call is within the limits. If the call is outside the limits, the call is rejected and an error code is returned to the universal gateway.
4. Connection to originating gateway—If adequate resources exist for the call and the call falls within SLA limits, the call is accepted. The long-distance number is matched in the dial plan, gateway resources are assigned to terminate the call, and the connection between the caller and the originating universal gateway is completed (call leg 1).
5. Authentication and authorization—Information about the call is sent from the universal gateway to the RADIUS-based PPM server, where it is forwarded to the service provider's voice billing server. Connection is made to the Internet or to a remote intranet (call leg 2).
6. Call setup request to terminating gateway—The universal gateway processes information from the dial plan, assigns a resource (if not already assigned), and initiates a call setup request with a terminating gateway.
7. Call admission control on terminating gateway—When the call setup request is received, the universal gateway checks the configured call admission control limits. If the call is outside the limits, the call is rejected.

8. Connection to terminating gateway—If adequate resources exist for the call, the call is accepted. Resources are assigned to terminate the call, and the connection between the caller and the terminating universal gateway is completed (call leg 3).
9. The caller is connected to the PSTN (call leg 4).
10. Accounting stop—After the caller hangs up or is otherwise disconnected, the originating universal gateway issues an accounting stop packet to the RADIUS-based PPM server. The PPM server uses the accounting stop packet to clear out the count for that call against the SLA. The PPM server can be configured to forward the packet to the voice billing server.

Scenario 4: H.323-Based Voice Origination and Termination with Prepaid Billing

In Scenario 4, the end customer dials into a prepaid voice service from the PSTN and requires both call origination and termination services on the IP network (Figure 4). This scenario describes a complete VoIP call end-to-end. The terminating call flow is identical to the flow presented in Scenario 2.

Figure 4 H.323-Based Voice Origination and Termination with Prepaid Billing



Scenario 4 has the following call flow:

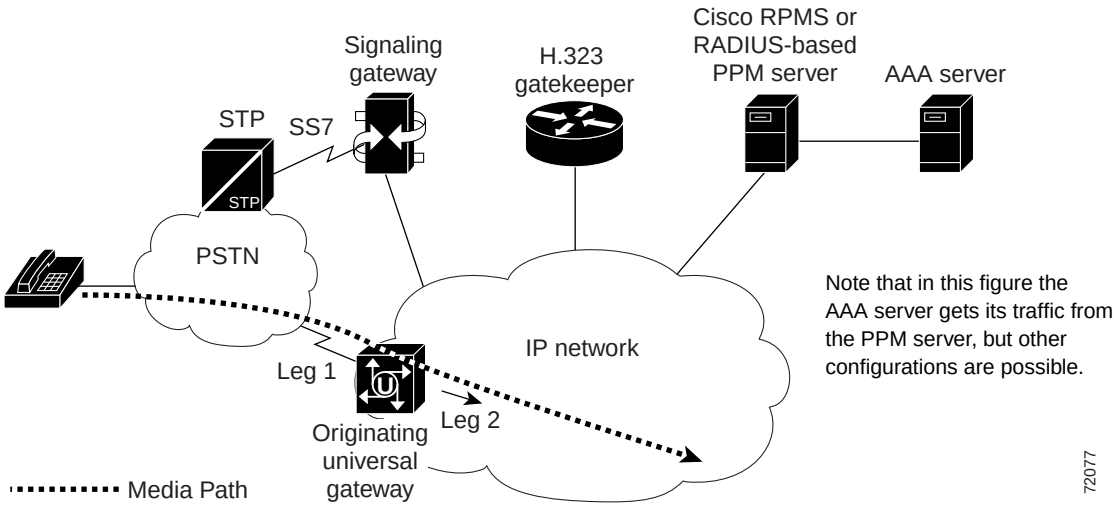
1. A call setup request from the PSTN is received by the originating universal gateway.
2. Call admission control on originating gateway—The universal gateway checks the configured call admission control limits. If the call is outside the limits, the call is rejected.
3. Preauthentication—If the call is accepted, information about the call is sent in a preauthentication request from the universal gateway to a RADIUS-based PPM server. The server locates the appropriate SLA that limits calls per customer or service, and makes sure that the current call is within the limits. If the call is outside the limits, the call is rejected and an error code is returned to the universal gateway.

4. Connection to originating gateway—If adequate resources exist for the call and the call falls within SLA limits, the call is accepted. Resources in the universal gateway are assigned to terminate the call, and the connection between the caller and the originating universal gateway is completed (call leg 1).
5. Authentication and authorization—User authentication takes place, and information about the call is sent from the universal gateway to the RADIUS-based PPM server and the service provider's AAA server, including the resource selected to handle the call and billing information.
6. Billing identification—The caller is queried for billing identification (PIN), which is sent to the prepaid billing server by the RADIUS-based PPM server. Call duration authorization is then relayed back over the same path.
7. Call admission control on terminating gateway—A call setup request from the IP network is received by the terminating universal gateway. The universal gateway checks the configured call admission control limits. If the call is outside the limits, the call is rejected.
8. Connection to terminating universal gateway—If adequate resources exist for the call, the call is accepted. Resources in the universal gateway are assigned to terminate the call, and the connection between the caller and the terminating universal gateway is completed (call leg 3).
9. The caller is connected to the PSTN (call leg 4).
10. Accounting stop—After the caller hangs up or is otherwise disconnected, the originating universal gateway issues an accounting stop packet to the RADIUS-based PPM server. The PPM server uses the accounting stop packet to clear out the count for that call against the SLA. The PPM server can be configured to forward the packet to the prepaid billing server.

Scenario 5: Dial-Up (Modem) Call Origination

In Scenario 5, the end customer dials into an ISP from the PSTN (Figure 5). The universal gateway preauthenticates the call and connects it to the IP network.

Figure 5 Dial-Up (Modem) Call Origination



Scenario 5 has the following call flow:

1. A call setup request from the PSTN is received by the originating universal gateway.
2. Call admission control—The universal gateway checks the configured call admission control limits. If the call is outside the limits, the call is rejected.
3. Preauthentication—If the call is accepted, information about the call is sent in a preauthentication request from the universal gateway to the RADIUS-based PPM server. On the basis of dialed number (DNIS) or trunk group, the server locates the appropriate SLA and makes sure that the call is within the SLA limits. If the call is outside the limits, the call is rejected and an error code is returned to the universal gateway.
4. Connection to originating universal gateway—If adequate resources exist for the call, the call is accepted. Resources in the universal gateway are assigned to terminate the call, and the connection between the caller and the originating universal gateway is completed (call leg 1).
5. Authentication and authorization—Information about the call is sent from the universal gateway to the RADIUS-based PPM server and the service provider's AAA server, including the resource selected to handle the call and billing information.
6. The call is connected to the Internet or to a remote intranet (call leg 2).
7. Accounting stop—Upon termination of the session, an accounting stop packet is forwarded to the RADIUS-based PPM server. The PPM server uses the accounting stop packet to clear out the count for that call against the SLA and sends the packet on to the ISP's AAA server.

Benefits

- RADIUS preauthentication allows wholesalers to accept or reject calls to enforce SLAs before calls are connected, thereby conserving gateway resources.
- Call admission control prevents call connections when resources are unavailable.
- Extended dial plan features enable the call service type to be determined from preauthentication request data, simplifying dial plan entries.
- Universal gateways provide other specific benefits:
  - Flexibility in deploying new services and adapting to changes in the business environment
  - Cost savings through reduction of total number of ports required to provide different services
  - Optimized utilization of access infrastructure by supporting more services during off-peak hours
  - Flexibility in access network engineering by leveraging dial infrastructure to handle both dial and voice

Restrictions

- If Cisco Resource Policy Management System (RPMS) is used as the RADIUS-based PPM server, it must be Version 2.0 or a later release.
- In SIP environments, if you want the Cisco SIP Proxy Server to generate the preauthentication queries, you must be running CSPS 2.0 or a later version.
- Media Gateway Control Protocol (MGCP) calls are not supported in Cisco IOS Release 12.2(11)T.

Related Features and Technologies

- *Cisco Any Service, Any Port (ASAP) Solution*
- *Cisco Resource Policy Management System (RPMS) 2.0*
- AAA network security services and RADIUS security system
- Call Admission Control (CAC)
- H.323 gateways and gatekeepers
- Session Initiation Protocol
- Voice over IP (VoIP)

Related Documents

- *Cisco IOS Security Configuration Guide*, Release 12.2
- *Cisco IOS Security Command Reference*, 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
- *RADIUS Vendor-Specific Attributes Voice Implementation Guide*, Cisco IOS Release 12.2(11)T
- *Inter-Domain Gatekeeper Security Enhancement*, Cisco IOS Release 12.2(4)T
- *VoIP Call Admission Control*
- *Call Admission Control based on CPU Utilization*, Cisco IOS Release 12.1(5)XM
- *Call Admission Control for H.323 VoIP Gateways*, Cisco IOS Release 12.2(2)XA
- *SIP Gateway Support of RSVP and TEL URL*, Cisco IOS Release 12.2(2)XB
- *Fine-Grain Address Segmentation in Dial Peers*, Cisco IOS Release 12.2(2)XB
- *Cisco Resource Policy Management System 2.0*
- *Cisco SIP Proxy Server Administration Guide*
- Cisco AS5300 product documentation
- Cisco AS5350 product documentation
- Cisco AS5400 product documentation
- Cisco AS5800 product documentation
- Cisco AS5850 product documentation

Supported Platforms

- Cisco AS5300
- Cisco AS5350
- Cisco AS5400
- Cisco AS5800
- Cisco AS5850

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on 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 quickly 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. 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 found at this URL:

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

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access Cisco MIB Locator, 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. 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 found at this URL:

http://www.cisco.com/register

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

- Cisco IOS Release 12.2(11)T or a later release.
- An application that supports preauthentication. Preauthentication profiles must be set up and running on a RADIUS-based PPM server in your network.
  - For information on setting up the preauthentication profiles, refer to the "Configuring AAA Preauthentication" section in the "Configuring RADIUS" chapter of the *Cisco IOS Security Configuration Guide*, Release 12.2.
  - For information on Cisco RPMS, refer to *Cisco Resource Policy Management System 2.0.*
  - For standards supporting RADIUS-based PPM servers, refer to RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*.

Configuration Tasks

See the following section for configuration tasks for the RADIUS Preauthentication for H.323 and SIP Voice Calls feature. Each task in the list is identified as either required or optional.

- Configuring AAA RADIUS for RADIUS Preauthentication (required)

Configuring AAA RADIUS for RADIUS Preauthentication

This section explains how to configure the AAA RADIUS communication link between a universal gateway and a RADIUS-based PPM server for RADIUS preauthentication.

Information about an incoming call is relayed through the gateway to the RADIUS-based PPM server in the network before the call is connected. The RADIUS-based PPM server provides port policy management and preauthentication by evaluating the call information against contracted parameter levels in SLAs. If the call falls within SLA limits, the server preauthenticates the call and the universal gateway accepts it. If the server does not authorize the call, the universal gateway sends a disconnect message to the public network switch to reject the call. The available call information includes one or more of the following:

- DNIS number, also referred to as the called number.
- CLID number (calling line identification number), also referred to as the calling number.
- Call type, also referred to as the bearer capability.
- IP address of the originating domain.

- Interzone ClearToken (IZCT) information, which contains the origination gatekeeper zone name for intradomain calls or the origination domain border gatekeeper zone name for interdomain calls. Whenever IZCT information is available, it is used to preauthenticate leg-3 H.323 VoIP calls.

Note To enable IZCT, the **security izct password** command must be configured on the gatekeeper. For multiple gatekeeper zones, the **lrq forward-queries** command must also be configured. For more information on IZCT configuration, refer to *Inter-Domain Gatekeeper Security Enhancement*, Cisco IOS Release 12.2(4)T.

A timer monitors the preauthentication query in case the RADIUS-based PPM server application is unavailable or slow to respond. If the timer expires before an acceptance or rejection is provided, the universal gateway rejects the call.

The RADIUS Preauthentication for H.323 and SIP Voice Calls feature supports the use of RADIUS attributes that are configured in RADIUS preauthentication profiles to specify preauthentication behavior. These attributes can also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used.

The commands in this section are used for both leg 1 calls (calls from a PSTN that enter an incoming, or originating, gateway) and leg 3 calls (calls that exit the IP network to an outgoing, or terminating, gateway). The use of optional commands depends on individual network factors.

Note Before configuring AAA preauthentication, you must make sure that the supporting preauthentication application is running on a RADIUS-based PPM server in your network, such as a Cisco RPMS. You must also set up preauthentication profiles on the RADIUS-based PPM server.

The following are general guidelines for configuring AAA RADIUS. Specific commands that can be used with this feature are shown in the configuration task table that follows. All references are to chapters in the *Cisco IOS Security Configuration Guide*, Release 12.2.

- Use the **aaa new-model** global configuration command to enable AAA. For more information about using the **aaa new-model** command, refer to the “AAA Overview” chapter.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication. For more information about using the **aaa authentication** command, refer to the “Configuring Authentication” chapter.
- Use **line** and **interface** commands to enable the defined method lists to be used. For more information, refer to the “Configuring Authentication” chapter.

The following configuration tasks are optional:

- You may use the **aaa server group** command to group selected RADIUS hosts for specific services. For more information about using the **aaa server group** command, refer to the “Configuring AAA Server Groups” section in the “Configuring RADIUS” chapter.
- You may use the **aaa dnis map** command to select RADIUS server groups on the basis of DNIS number. To use this command, you must define RADIUS server groups using the **aaa server group** command. For more information about using the **aaa dnis map** command, refer to the “Configuring AAA Server Group Selection Based on DNIS” section in the “Configuring RADIUS” chapter.
- You may use the **aaa authorization** global configuration command to authorize specific user functions. For more information about using the **aaa authorization** command, refer to the “Configuring Authorization” chapter.

- The **aaa accounting** command enables accounting for RADIUS connections, and it is required for preauthentication to work with a RADIUS-based PPM server. For more information about using the **aaa accounting** command, refer to the "Configuring Accounting" chapter.
- You may use the **dialer aaa** interface configuration command to create remote site profiles that contain outgoing call attributes on the AAA server. For more information about using the **dialer aaa** command, refer to the "Configuring Suffix and Password in RADIUS Access Requests" section in the "Configuring RADIUS" chapter.

Note For the RADIUS Preauthentication for H.323 and SIP Voice Calls feature, gateway accounting must be enabled and all call accounting information must be forwarded to the server that is performing preauthentication. Accounting stop packets must be sent to this server so that call billing is ended when calls are disconnected from the gateway. In addition, authentication and accounting start packets are needed to enable other features, such as virtual private dial-up network (VPDN).

To configure the RADIUS Preauthentication for H.323 and SIP Voice Calls feature, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa new-model`	(Required) Enables the AAA access control model.
Step 2	`Router(config)# aaa group server radius group-name`	(Optional) Specifies a subset of RADIUS servers to use as the login authorization method and initiates server-group configuration mode to configure the IP address of the RADIUS server to use for the group.
Step 3	`Router(config-sg-radius)# server ip-address auth-port port acct-port port`	(Required if the **aaa group server** command is used) Configures the IP address of the RADIUS server and ports to use for the group named in the **aaa group server** command.
Step 4	`Router(config-sg-radius)# exit`	(Required if the **aaa group server** command is used) Exits server-group configuration mode.
Step 5	`Router(config)# aaa authentication login h323 group group-name`	(Required) Defines a method list called h323 in which RADIUS is defined as the only method of login authentication for all voice calls. The **group** *group-name* keyword and argument pair specifies the subset of RADIUS servers for authentication that was defined by the **aaa group server radius** command in Steps 2 and 3.
Step 6	`Router(config)# aaa authentication ppp default group group-name`	(Required for PPP dial-in methods that are to be used with preauthentication) Creates a local authentication list to enable AAA authentication for serial lines that use PPP authentication methods. Note that the **ppp authentication** command must also be configured on the interfaces that will use PPP authentication methods.
Step 7	`Router(config)# aaa authorization exec list-name group group-name`	(Optional) Creates an authorization method list to restrict access to EXEC terminal sessions on a network.

	Command	Purpose
Step 8	`Router(config)# aaa authorization network default group {radius | rpms} if-authenticated`	(Optional) Configures the network access server to contact the RADIUS-based PPM server to determine if users are permitted to start an EXEC shell when they log in. If an error occurs when the network access server contacts the RADIUS or RPMS server, the fallback method is to permit the command-line interface (CLI) to start, provided the user has been properly authenticated.
Step 9	`Router(config)# aaa authorization reverse-access default local`	(Optional) Configures the network access server to request authorization information before allowing a user to establish a reverse Telnet session.
Step 10	`Router(config)# aaa accounting suppress null-username`	(Optional) Prevents the Cisco IOS software from sending accounting records for users whose username string is NULL.
Step 11	`Router(config)# aaa accounting send stop-record authentication failure`	(Required if using Cisco RPMS) Generates accounting stop records for users who fail to authenticate at login or during session negotiation.
Step 12	`Router(config)# aaa accounting delay-start`	(Optional) Delays generation of accounting start records until the user IP address is established.
Step 13	`Router(config)# aaa accounting update periodic` *number*	(Optional) Causes an interim accounting record to be sent to the accounting server periodically, as defined by the argument *number*, which indicates the number of minutes in each interval.
Step 14	`Router(config)# aaa accounting exec default start-stop group` *group-name*	(Optional) Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. Use a separate command for each service specified.
Step 15	`Router(config)# aaa accounting exec` *list-name* `start-stop group` *group-name*	(Optional) Runs accounting for EXEC shell sessions.
Step 16	`Router(config)# aaa accounting network default start-stop group` *group-name*	(Required for PPP dial-in methods that are to be used with preauthentication) Runs accounting for all network-related (PPP, SLIP, ARAP) service requests.
Step 17	`Router(config)# aaa accounting connection h323 start-stop group` *group-name*	(Required for voice call accounting) Runs accounting for all VoIP connections made from the universal gateway.
Step 18	`Router(config)# aaa accounting system default start-stop group` *group-name*	(Optional) Performs accounting for all system-level events not associated with users, such as reloads.
Step 19	`Router(config)# aaa accounting resource default start-stop-failure group` *group-name*	(Optional) Enables full resource accounting, which generates both an accounting start record at call setup and an accounting stop record at call termination.
Step 20	`Router(config)# gw-accounting aaa`	(Required) Enables VoIP gateway accounting through the AAA system and enters gateway accounting mode.
Step 21	`Router(gw-accounting aaa)# exit`	(Required) Exits gateway accounting mode.
Step 22	`Router(config)# aaa preauth`	(Required) Enters AAA preauthentication configuration mode.
Step 23	`Router(config-preauth)# group {radius |` *group-name*`}`	(Required) Selects the security server group to use for AAA preauthentication requests. The default is **radius**.
Step 24	`Router(config-preauth)# clid [if-avail | required] [accept-stop] [password` *string*`]`	(Optional) Preauthenticates calls on the basis of the CLID number.
Step 25	`Router(config-preauth)# ctype [if-avail | required] [accept-stop] [password` *string*`]`	(Optional) Preauthenticates calls on the basis of the call type.

	Command	Purpose
Step 26	`Router(config-preauth)# dnis [if-avail | required] [accept-stop] [password string]`	(Optional) Preauthenticates calls on the basis of DNIS and optionally specifies a password to use in Access-Request packets.
Step 27	`Router(config-preauth)# dnis bypass {dnis-group-name}`	(Optional) Specifies a group of DNIS numbers that will be bypassed for preauthentication.
Step 28	`Router(config-preauth)# filter voice`	(Optional) Specifies that voice calls should not go through preauthentication.
Step 29	`Router(config-preauth)# timeout leg3 time`	(Optional) Specifies a timeout value for leg 3 preauthentication in milliseconds. The range is from 100 to 1000. The default is 100.
Step 30	`Router(config-preauth)# service-type call-check`	(Optional) Identifies preauthentication requests to the AAA server. This command is required for incoming leg 3 calls from ITSPs or T-ASPs that need preauthentication before proceeding to a terminating universal gateway.
Step 31	`Router(config-preauth)# exit`	(Required) Exits AAA preauthentication configuration mode.
Step 32	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string] [alias {hostname | ip-address}]`	(Required) Defines the IP address and ports for the RADIUS-based PPM server.
Step 33	`Router(config)# radius-server retransmit retries`	(Optional) Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
Step 34	`Router(config)# radius-server attribute 6 support-multiple`	(Optional) Supports multiple service-type values in each RADIUS profile.
Step 35	`Router(config)# radius-server attribute 44 include-in-access-req`	(Required) Sends RADIUS Attribute 44 (Accounting Session ID) to the RADIUS-based PPM server in a preauthentication request. For more information on RADIUS attributes, refer to the "RADIUS Attributes" appendix of the *Cisco IOS Security Configuration Guide*, Release 12.2.
Step 36	`Router(config)# radius-server attribute nas-port format c`	(Required if using Cisco RPMS) Selects the NAS-Port format used for RADIUS accounting features. Format c is required if you are using Cisco RPMS.
Step 37	`Router(config)# radius-server key {0 string | 7 string | string}`	(Optional) Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
Step 38	`Router(config)# radius-server vsa send accounting`	(Optional) Configures the universal gateway to recognize and use vendor-specific accounting attributes.
Step 39	`Router(config)# radius-server vsa send authentication`	(Optional) Configures the universal gateway to recognize and use vendor-specific authentication attributes.

Verifying RADIUS Preauthentication for H.323 and SIP Voice Calls

To verify the configuration, use the **show running-config** command. An example of the output from this command is provided in the "H.323 Voice Termination Example" section on page 18.

Troubleshooting Tips

The following commands provide diagnostic information for the RADIUS Preauthentication for H.323 and SIP Voice Calls feature:

- **show rpms-proc counters**—Displays the number of leg 3 preauthentication requests, successes, and rejects.
- **clear rpms-proc counters**—Resets the counters that record the statistics that the **show rpms-proc counters** command displays.
- **debug rpms-proc preauth**—Enables debug tracing on the RPMS process for H.323 calls, SIP calls, or both H.323 and SIP calls.
- **debug ccsip preauth**—Enables debug tracing on the SIP service provider interface (SPI) for preauthentication.
- **debug cch323 preauth**—Enables debug tracing on the H.323 SPI for preauthentication.
- **debug aaa authentication**—Displays high-level diagnostics related to AAA logins.
- **show radius statistics**—Displays RADIUS statistics for accounting and authentication packets.
- **debug radius**—Enables debug tracing of RADIUS attributes, as shown in the following example:

```
Router# debug radius

Radius protocol debugging is on
Radius protocol brief debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius packet retransmission debugging is off
Radius server fail-over debugging is off

Jan 23 14:30:25.421:RADIUS/ENCODE(00071EBF):acct_session_id:742769
Jan 23 14:30:25.421:RADIUS(00071EBF):sending
Jan 23 14:30:25.421:RADIUS:Send to unknown id 25 192.168.41.57:1812, Access-Request,
len 179
Jan 23 14:30:25.421:RADIUS: authenticator 88 94 AC 32 89 84 73 6D - 71 00 50 6C D0 F8
FD 11
Jan 23 14:30:25.421:RADIUS: User-Name           [1]   9   "2210001"
Jan 23 14:30:25.421:RADIUS: User-Password       [2]   18  *
Jan 23 14:30:25.421:RADIUS: Vendor, Cisco       [26]  32
Jan 23 14:30:25.421:RADIUS: Cisco AVpair        [1]   26  "resource-service=reserve"
Jan 23 14:30:25.421:RADIUS: Service-Type        [6]   6   Call Check    [10]
Jan 23 14:30:25.421:RADIUS: Vendor, Cisco       [26]  19
Jan 23 14:30:25.421:RADIUS:  cisco-nas-port     [2]   13  "Serial6/0:0"
Jan 23 14:30:25.425:RADIUS: NAS-Port            [5]   6   6144
Jan 23 14:30:25.425:RADIUS: Vendor, Cisco       [26]  29
Jan 23 14:30:25.425:RADIUS:  Cisco AVpair       [1]   23  "interface=Serial6/0:0"
Jan 23 14:30:25.425:RADIUS: Called-Station-Id   [30]  9   "2210001"
Jan 23 14:30:25.425:RADIUS: Calling-Station-Id  [31]  9   "1110001"
Jan 23 14:30:25.425:RADIUS: NAS-Port-Type       [61]  6   Async
[0]
Jan 23 14:30:25.425:RADIUS: NAS-IP-Address      [4]   6   192.168.81.101
Jan 23 14:30:25.425:RADIUS: Acct-Session-Id     [44]  10  "000B5571"
```

```
Jan 23 14:30:25.429:RADIUS:Received from id 25 192.168.41.57:1812, Access-Accept, len
20
Jan 23 14:30:25.429:RADIUS: authenticator 2C 16 63 18 36 56 18 B2 - 76 EB A5 EF 11 45
BE F4
Jan 23 14:30:25.429:RADIUS:Received from id 71EBF
Jan 23 14:30:25.429:RADIUS/DECODE:parse response short packet; IGNORE
Jan 23 14:30:25.433:RADIUS/ENCODE(00071EBF):Unsupported AAA attribute start_time
Jan 23 14:30:25.433:RADIUS/ENCODE(00071EBF):Unsupported AAA attribute timezone
Jan 23 14:30:25.433:RADIUS/ENCODE:format unknown; PASS
Jan 23 14:30:25.433:RADIUS(00071EBF):sending
Jan 23 14:30:25.433:RADIUS:Send to unknown id 26 192.168.41.57:1813,
Accounting-Request, len 443
Jan 23 14:30:25.433:RADIUS: authenticator DA 1B 03 83 20 90 11 39 - F3 4F 70 F0 F5 8C
CC 75
Jan 23 14:30:25.433:RADIUS: Acct-Session-Id     [44]  10  "000B5571"
Jan 23 14:30:25.433:RADIUS: Vendor, Cisco       [26]  56
Jan 23 14:30:25.433:RADIUS:  h323-setup-time    [25]  50
"h323-setup-time=14:30:25.429 GMT Wed Jan 23 2002"
Jan 23 14:30:25.433:RADIUS: Vendor, Cisco       [26]  26
Jan 23 14:30:25.433:RADIUS:  h323-gw-id         [33]  20  "h323-gw-id=OrigGW."
Jan 23 14:30:25.433:RADIUS: Vendor, Cisco       [26]  56
Jan 23 14:30:25.433:RADIUS:  Conf-Id            [24]  50  "h323-conf-id=931C146B
0F4411D6 AB5591F0 CBF3D765"
Jan 23 14:30:25.433:RADIUS: Vendor, Cisco       [26]  31
Jan 23 14:30:25.437:RADIUS:  h323-call-origin   [26]  25  "h323-call-origin=answer"
Jan 23 14:30:25.437:RADIUS: Vendor, Cisco       [26]  32
Jan 23 14:30:25.437:RADIUS:  h323-call-type     [27]  26  "h323-call-type=Telephony"
Jan 23 14:30:25.437:RADIUS: Vendor, Cisco       [26]  65
Jan 23 14:30:25.437:RADIUS:  Cisco AVpair       [1]   59
"h323-incoming-conf-id=931C146B 0F4411D6 AB5591F0 CBF3D765"
Jan 23 14:30:25.437:RADIUS: Vendor, Cisco       [26]  30
Jan 23 14:30:25.437:RADIUS:  Cisco AVpair       [1]   24  "subscriber=RegularLine"
Jan 23 14:30:25.437:RADIUS: User-Name           [1]   9   "1110001"
Jan 23 14:30:25.437:RADIUS: Acct-Status-Type    [40]  6   Start             [1]
Jan 23 14:30:25.437:RADIUS: Vendor, Cisco       [26]  19
Jan 23 14:30:25.437:RADIUS:  cisco-nas-port     [2]   13  "Serial6/0:0"
Jan 23 14:30:25.437:RADIUS: NAS-Port            [5]   6   0
Jan 23 14:30:25.437:RADIUS: Vendor, Cisco       [26]  29
Jan 23 14:30:25.437:RADIUS:  Cisco AVpair       [1]   23  "interface=Serial6/0:0"
Jan 23 14:30:25.437:RADIUS: Called-Station-Id   [30]  9   "2210001"
Jan 23 14:30:25.437:RADIUS: Calling-Station-Id  [31]  9   "1110001"
Jan 23 14:30:25.437:RADIUS: NAS-Port-Type       [61]  6   Async
[0]
Jan 23 14:30:25.437:RADIUS: Service-Type        [6]   6   Login
[1]
Jan 23 14:30:25.437:RADIUS: NAS-IP-Address      [4]   6   192.168.81.101
Jan 23 14:30:25.437:RADIUS: Event-Timestamp     [55]  6   1011796225
Jan 23 14:30:25.437:RADIUS: Delay-Time          [41]  6   0
Jan 23 14:30:25.441:RADIUS/ENCODE(00071EC0):Unsupported AAA attribute start_time
Jan 23 14:30:25.441:RADIUS/ENCODE(00071EC0):Unsupported AAA attribute timezone
Jan 23 14:30:25.441:RADIUS(00071EC0):sending
Jan 23 14:30:25.441:RADIUS:Send to unknown id 27 192.168.41.57:1813, Accounting-Request, len 411
Jan 23 14:30:25.441:RADIUS: authenticator 15 83 23 D8 0B B2 3A C2 - 1D 8C EF B4 18 0F
1C 65
Jan 23 14:30:25.441:RADIUS: Acct-Session-Id     [44]  10  "000B5572"
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  56
Jan 23 14:30:25.441:RADIUS:  h323-setup-time    [25]  50
"h323-setup-time=14:30:25.441 GMT Wed Jan 23 2002"
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  26
Jan 23 14:30:25.441:RADIUS:  h323-gw-id         [33]  20  "h323-gw-id=OrigGW."
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  56
Jan 23 14:30:25.441:RADIUS:  Conf-Id            [24]  50  "h323-conf-id=931C146B
0F4411D6 AB5591F0 CBF3D765"
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  34
```

```
Jan 23 14:30:25.441:RADIUS:  h323-call-origin   [26]  28  "h323-call-origin=originate"
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  27
Jan 23 14:30:25.441:RADIUS:  h323-call-type     [27]  21  "h323-call-type=VoIP"
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  65
```

Configuration Examples

This section provides the following configuration examples:

- H.323 Voice Termination Example

Note IP addresses and host names in examples are fictitious.

H.323 Voice Termination Example

The following example shows a configuration example for Scenario 2: H.323-Based Voice Termination.

```
Router# show running-config
!
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
service internal
!
hostname OrigGW
!
boot system flash c5400-mj-sz
no boot startup-test
no logging buffered
no logging rate-limit
logging console
aaa new-model
!
aaa group server radius RPMS
 server 192.168.41.57 auth-port 1812 acct-port 1813
!
aaa authentication login h323 group RPMS
aaa authentication ppp default group RPMS
aaa authorization exec h323 group RPMS
aaa authorization network default group RPMS if-authenticated
aaa authorization reverse-access default local
aaa accounting suppress null-username
aaa accounting send stop-record authentication failure
aaa accounting delay-start
aaa accounting update periodic 2
aaa accounting exec default start-stop group RPMS
aaa accounting exec h323 start-stop group RPMS
aaa accounting network default start-stop group RPMS
aaa accounting connection h323 start-stop group RPMS
aaa accounting system default start-stop group RPMS
aaa accounting resource default start-stop-failure group RPMS
aaa preauth
 group RPMS
 timeout leg3 1000
 service-type call-check
 dnis required
```

```
!
aaa session-id common
!
username async_hgw password 0 grape
username parana_vpdn_bundle1 password 0 guava
username async_caller1 password 0 mango
username OrigGW password 0 pear
!
resource-pool disable
clock timezone GMT 0
dial-tdm-clock  priority 1 6/0
dial-tdm-clock  priority 2 6/1
dial-tdm-clock  priority 3 6/2
dial-tdm-clock  priority 4 6/3
dial-tdm-clock  priority 5 6/4
dial-tdm-clock  priority 6 6/5
dial-tdm-clock  priority 7 6/6
dial-tdm-clock  priority 8 6/7
calltracker enable
spe country e1-default
!
spe default-firmware spe-firmware-1
!
!
!
!
ip subnet-zero
no ip domain-lookup
ip host mind 192.168.80.50
ip host digiquant 192.168.80.51
ip host jurai 192.168.254.254
ip host brios 192.168.254.253
ip host sip-proxy 192.168.80.70
ip host aaa-pc 192.168.80.20
!
ip cef
multilink virtual-template 1
isdn switch-type primary-net5
chat-script dial ABORT ERROR ABORT BUSY ABORT "NO CARRIER" TIMEOUT 120 "" at OK "\datd\T"
CONNECT
!
!
voice service voip
 fax protocol t38 ls-redundancy 0 hs-redundancy 0
 h323
!
voice class codec 1
 codec preference 1 g711alaw
 codec preference 2 g723r63
 codec preference 3 g729r8
!
voice class h323 101
  call start fast
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
memory check-interval 3200
memory validate-checksum 3200
!
```

```
controller E1 6/0
 pri-group timeslots 1-31
 description calls from abacus
!
controller E1 6/1
 pri-group timeslots 1-31
 description calls from abacus
!
controller E1 6/2
 pri-group timeslots 1-31
 description calls from abacus
!
controller E1 6/3
 pri-group timeslots 1-31
 description calls from abacus
!
controller E1 6/4
 pri-group timeslots 1-31
 description calls from abacus
!
controller E1 6/5
 pri-group timeslots 1-31
 description calls from abacus
!
controller E1 6/6
 pri-group timeslots 1-31
 description calls from abacus
!
controller E1 6/7
 pri-group timeslots 1-31
 description calls from abacus
!
controller E1 7/0
 pri-group timeslots 1-31
 description fax from hammer span0
!
controller E1 7/1
 pri-group timeslots 1-31
 description fax from hammer span1
!
controller E1 7/2
 pri-group timeslots 1-31
 description "E1 7/0 - 7/3, digital calls "
!
controller E1 7/3
 pri-group timeslots 1-31
 description "E1 7/0 - 7/3, digital calls "
!
controller E1 7/4
 pri-group timeslots 1-31
 description "E1 7/4 - 7/7, async modem calls"
!
controller E1 7/5
 pri-group timeslots 1-31
 description "E1 7/4 - 7/7, async modem calls"
!
controller E1 7/6
 pri-group timeslots 1-31
 description "E1 7/4 - 7/7, async modem calls"
!
controller E1 7/7
 pri-group timeslots 1-31
 description "E1 7/4 - 7/7, async modem calls"
!
```

```
gw-accounting aaa
!
!
!
!
interface Loopback0
 ip address 10.102.103.104 255.255.0.0
!
interface FastEthernet0/0
 description 10.4.41.106 255.255.0.0 172.22.43.97 255.255.255.0
 ip address 10.4.41.106 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet0/1
 ip address 192.168.81.101 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
 h323-gateway voip interface
 h323-gateway voip id sxn.gk1.com ipaddr 192.168.81.115 1719
 h323-gateway voip h323-id OrigGW@sxn1.com
 h323-gateway voip tech-prefix 1#
 hold-queue 1024 in
 hold-queue 1024 out
!
!
!
interface Serial0/0
 no ip address
 shutdown
 clockrate 2000000
 no cdp enable
!
interface Serial6/0
 no ip address
 shutdown
!
interface Serial7/0
 no ip address
 shutdown
!
interface Serial0/1
 no ip address
 shutdown
 clockrate 2000000
 no cdp enable
!
interface Serial6/0:15
 no ip address
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
interface Serial6/1:15
 no ip address
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
```

```
interface Serial6/2:15
 no ip address
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
interface Serial6/3:15
 no ip address
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
interface Serial6/4:15
 no ip address
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
interface Serial6/5:15
 no ip address
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
interface Serial6/6:15
 no ip address
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
interface Serial6/7:15
 no ip address
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
interface Serial7/0:15
 description fax from hammer span0
 no ip address
 no keepalive
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
interface Serial7/1:15
 description fax from hammer span1
 no ip address
 no keepalive
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
interface Serial7/2:15
 description digital calls from vpdn-async serial4:15
 ip address 192.168.253.253 255.255.255.252
 encapsulation ppp
 no keepalive
 dialer map ip 192.168.253.254 broadcast 15105551212
 dialer load-threshold 1 either
 dialer-group 1
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
```

```
interface Serial7/3:15
 description digital calls from vpdn-async serial5:15
 ip address 192.168.254.253 255.255.255.252
 encapsulation ppp
 no keepalive
 dialer map ip 192.168.254.254 broadcast 15105551212
 dialer load-threshold 1 either
 dialer-group 1
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no cdp enable
!
interface Serial7/4:15
 description -----D-CHANNELS 7/4 to 7/5 are for async VPDN
 ip unnumbered FastEthernet0/0
 encapsulation ppp
 no keepalive
 dialer-group 1
 no snmp trap link-status
 isdn switch-type primary-net5
 isdn incoming-voice modem
 peer default ip address pool default
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname parana_vpdn_bundle1
 hold-queue 10 in
!
interface Serial7/5:15
 description -----D-CHANNELS 7/4 to 7/5 are for async VPDN
 ip unnumbered FastEthernet0/0
 encapsulation ppp
 no keepalive
 dialer-group 1
 no snmp trap link-status
 isdn switch-type primary-net5
 isdn incoming-voice modem
 peer default ip address pool default
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname parana_vpdn_bundle1
 hold-queue 10 in
!
interface Serial7/6:15
 description -----D-CHANNELS 7/4 to 7/5 are for async VPDN
 ip unnumbered FastEthernet0/0
 encapsulation ppp
 no keepalive
 dialer-group 1
 no snmp trap link-status
 isdn switch-type primary-net5
 isdn incoming-voice modem
 peer default ip address pool default
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname parana_vpdn_bundle1
 hold-queue 10 in
!
interface Serial7/7:15
 description -----D-CHANNELS 7/4 to 7/5 are for async VPDN
 ip unnumbered FastEthernet0/0
 encapsulation ppp
 no keepalive
 dialer-group 1
 no snmp trap link-status
```

```
 isdn switch-type primary-net5
 isdn incoming-voice modem
 peer default ip address pool default
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname parana_vpdn_bundle1
 hold-queue 10 in
!
interface Group-Async0
 ip unnumbered Loopback0
 encapsulation ppp
 async default routing
 async mode dedicated
 peer default ip address pool default
 ppp quality 50
 ppp authentication chap callin
 ppp chap hostname parana_vpdn_bundle1
 group-range 1/00 5/107
!
ip local pool default 172.16.1.1 172.16.1.120
ip classless
ip route 172.26.0.0 255.0.0.0 192.168.0.0
ip route 10.1.1.1 255.255.255.255 172.30.1.1
ip route 10.1.1.2 255.255.255.255 172.30.1.2
.
.
.
ip route 10.1.1.120 255.255.255.255 172.30.1.120
ip route 172.22.51.0 255.255.255.0 172.22.42.1
ip route 192.168.254.0 255.255.255.0 10.4.0.1
no ip http server
ip pim bidir-enable
!
ip radius source-interface FastEthernet0/1
!
logging source-interface FastEthernet0/1
dialer-list 1 protocol ip permit
no cdp run
!
!
snmp-server community public RO
snmp-server packetsize 2048
!
radius-server host 192.168.41.57 auth-port 1812 acct-port 1813 key cisco
radius-server retransmit 3
radius-server attribute 6 support-multiple
radius-server attribute 44 include-in-access-req
radius-server attribute 25 accounting prefer-preauth
radius-server attribute nas-port format c
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
call treatment on
call threshold poll-interval cpu-avg 10
call threshold global cpu-5sec low 80 high 90 treatment
call threshold global cpu-avg low 80 high 90 treatment
call threshold global total-mem low 70 high 80
call threshold global io-mem low 75 high 80
call threshold global proc-mem low 85 high 90
call threshold global total-calls low 450 high 484
call rsvp-sync
!
```

```
call application voice debitcard tftp://brios/sxnguyen/skynyrd/app_debitcard.2.0.0.tcl
call application voice debitcard uid-len 6
call application voice debitcard pin-len 8
call application voice debitcard language 1 en
call application voice debitcard language 2 ch
call application voice debitcard set-location en 0 tftp://brios/sxnguyen/skynyrd/au/en/
call application voice debitcard set-location ch 0 tftp://brios/sxnguyen/skynyrd/au/ch/
!
voice-port 6/0:D
!
voice-port 6/1:D
!
voice-port 6/2:D
!
voice-port 6/3:D
!
voice-port 6/4:D
!
voice-port 6/5:D
!
voice-port 6/6:D
!
voice-port 6/7:D
!
voice-port 7/0:D
!
voice-port 7/1:D
!
voice-port 7/2:D
!
voice-port 7/3:D
!
voice-port 7/4:D
!
voice-port 7/5:D
!
voice-port 7/6:D
!
voice-port 7/7:D
!
mgcp ip qos dscp cs5 media
mgcp ip qos dscp cs3 signaling
!
mgcp profile default
!
!
dial-peer cor custom
!
!
dial-peer voice 1 pots
 description incoming H.323 Leg1 calls from PSTN
 incoming called-number 221....
 destination-pattern 111....
 direct-inward-dial
 port 6/0:D
 prefix 111
!
dial-peer voice 1001 voip
 description outgoing H.323 VoIP calls to 54-TGW
 incoming called-number 111....
 destination-pattern 221....
 session target ras
 tech-prefix 2#
 codec g711alaw
```

```
!
dial-peer voice 2 pots
 description incoming H.323 Leg1 calls from PSTN
 destination-pattern 112....
 direct-inward-dial
 port 6/1:D
 prefix 112
!
dial-peer voice 1002 voip
 description outgoing H.323 VoIP calls to 54-TGW
 incoming called-number 112....
 destination-pattern 222....
 session target ras
 tech-prefix 2#
 codec g711alaw
!
dial-peer voice 3 pots
 description outgoing H.323 Leg3 calls to PSTN
 incoming called-number 223....
 destination-pattern 1#113....
 direct-inward-dial
 port 6/2:D
 prefix 113
!
dial-peer voice 1003 voip
 description incoming H.323 Leg3 calls from 54-TGW
 incoming called-number 1#113....
 destination-pattern 223....
 session target ras
 tech-prefix 2#
 codec g711alaw
!
dial-peer voice 4 pots
 description terminating H.323 Leg3 calls to PSTN
 incoming called-number 224....
 destination-pattern 1#114....
 direct-inward-dial
 port 6/3:D
 prefix 114
!
dial-peer voice 1004 voip
 description incoming H.323 Leg3 calls from 54-TGW
 incoming called-number 1#114....
 destination-pattern 224....
 session target ras
 tech-prefix 2#
 codec g711alaw
!
dial-peer voice 5 pots
 description incoming SIP calls from  PSTN
 incoming called-number 225....
 destination-pattern 115....
 direct-inward-dial
 port 6/4:D
 prefix 115
!
dial-peer voice 1005 voip
 description outgoing SIP VoIP to 54-TGW
 incoming called-number 115....
 destination-pattern 225....
 session protocol sipv2
 session target sip-server
 codec g711alaw
!
```

```
dial-peer voice 6 pots
 description incoming SIP calls from  PSTN
 incoming called-number 226....
 destination-pattern 116....
 direct-inward-dial
 port 6/5:D
 prefix 116
!
dial-peer voice 1006 voip
 description outgoing SIP VoIP to 54-TGW
 incoming called-number 116....
 destination-pattern 226....
 session protocol sipv2
 session target sip-server
 codec g711alaw
!
dial-peer voice 7 pots
 description terminating SIP Leg3 calls to PSTN
 incoming called-number 227....
 destination-pattern 117....
 direct-inward-dial
 port 6/6:D
 prefix 117
!
dial-peer voice 1007 voip
 description incoming SIP  Leg3 calls from 54-TGW
 incoming called-number 117....
 destination-pattern 227....
 session protocol sipv2
 session target sip-server
 codec g711alaw
!
dial-peer voice 8 pots
 description terminating SIP Leg3 calls to PSTN
 incoming called-number 228....
 destination-pattern 118....
 direct-inward-dial
 port 6/7:D
 prefix 118
!
dial-peer voice 1008 voip
 description incoming SIP  Leg3 calls from 54-TGW
 incoming called-number 118....
 destination-pattern 228....
 session protocol sipv2
 session target sip-server
 codec g711alaw
!
dial-peer voice 9 pots
 incoming called-number 1234567
 direct-inward-dial
 port 7/0:D
 prefix 1234567
!
dial-peer voice 1009 voip
 destination-pattern 1234567
 session target ipv4:192.168.81.102
 codec g711alaw
 fax protocol t38 ls-redundancy 0 hs-redundancy 0
!
dial-peer voice 10 pots
 incoming called-number 7654321
 direct-inward-dial
 port 7/1:D
```

```
 prefix 7654321
!
dial-peer voice 1010 voip
 destination-pattern 7654321
 session target ipv4:192.168.81.102
 codec g711alaw
 fax protocol t38 ls-redundancy 0 hs-redundancy 0
!
dial-peer voice 100 pots
 description outgoing leg3 IP callgen calls to 72-Callgen
 destination-pattern +922....
 port 6/0:D
!
dial-peer voice 55100 voip
 description incoming leg3 IP callgen calls from 72-Callgen Router
 incoming called-number +911....
 dtmf-relay h245-signal h245-alphanumeric
 codec g711alaw
!
dial-peer voice 200 pots
 description digital calls from vpdn-async serial4:15
 application data_dialpeer
 incoming called-number 15105551212
 port 7/2:D
!
dial-peer voice 201 pots
 description digital calls from vpdn-async serial5:15
 incoming called-number 4151234
 port 7/3:D
!
gateway
!
sip-ua
 max-forwards 1
 retry invite 10
 retry response 10
 retry cancel 1
 timers trying 1000
 timers expires 300000
 timers connect 1000
 timers disconnect 1000
 no oli
 sip-server ipv4:192.168.80.70
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 exec-timeout 0 0
 logging synchronous
line 1/00 2/59
 session-timeout 300
 no flush-at-activation
 script dialer dial
 logging synchronous
 modem InOut
 transport input all
 autoselect during-login
 autoselect ppp
```

```
line 2/60 2/107
 no flush-at-activation
 modem InOut
line 3/00 4/107
 session-timeout 300
 no flush-at-activation
 script dialer dial
 logging synchronous
 modem InOut
 transport input all
 autoselect during-login
 autoselect ppp
line 5/00 5/107
 no flush-at-activation
 modem InOut
!
scheduler allocate 10000 400
ntp clock-period 17180007
ntp master 1
end
```

Command Reference

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

New Commands

- **clear rpms-proc counters**
- **debug cch323 preauth**
- **debug ccsip preauth**
- **debug rpms-proc preauth**
- **filter voice**
- **radius-server attribute 6**
- **service-type call-check**
- **show rpms-proc counters**
- **timeout leg3**

clear rpms-proc counters

To clear statistics counters for the number of leg 3 authentication, authorization, and accounting (AAA) preauthentication requests, successes, and rejects, use the **clear rpms-proc counters** command in privileged EXEC mode.

clear rpms-proc counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples

The following example clears statistics counters for leg 3 AAA preauthentication requests, successes, and rejects:

```
Router# clear rpms-proc counters
```

Related Commands

Command	Description
show rpms-proc counters	Displays statistics for the number of leg 3 AAA preauthentication requests, successes, and rejects.

debug cch323 preauth

To enable diagnostic reporting of authentication, authorization, and accounting (AAA) call preauthentication for H.323 calls, use the **debug cch323 preauth** command in privileged EXEC mode. To disable diagnostic reporting, use the **no** form of this command.

debug cch323 preauth

no debug cch323 preauth

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples

The following example shows debug output for a single H.323 call:

```
Router# debug cch323 preauth

CCH323 preauth tracing is enabled
cch323_is_preauth_reqd is TRUE
Jan 23 18:39:56.393: In cch323_send_preauth_req for preauth_id = -1
Jan 23 18:39:56.393: Entering rpms_proc_print_preauth_req

Jan 23 18:39:56.393: Request = 0
Jan 23 18:39:56.393: Preauth id = 86514
Jan 23 18:39:56.393: EndPt Type  = 1
Jan 23 18:39:56.393: EndPt = 192.168.81.102
Jan 23 18:39:56.393: Resource Service = 1
Jan 23 18:39:56.393: Call_origin = answer
Jan 23 18:39:56.393: Call_type = voip
Jan 23 18:39:56.393: Calling_num = 2230001
Jan 23 18:39:56.393: Called_num = 1#1130001
Jan 23 18:39:56.393: Protocol  = 0
Jan 23 18:39:56.393: cch323_insert_preauth_tree:Created node with preauth_id = 86514 ,ccb
6852D5BC , node 651F87FC
Jan 23 18:39:56.393:rpms_proc_create_node:Created node with preauth_id = 86514
Jan 23 18:39:56.393:rpms_proc_send_aaa_req:uid got is 466725
Jan 23 18:39:56.397:rpms_proc_preauth_response:Context is for preauth_id 86514, aaa_uid
466725
Jan 23 18:39:56.397: Entering Function cch323_rpms_proc_callback_func

Jan 23 18:39:56.397:cch323_rpms_proc_callback_func:PREAUTH_SUCCESS for preauth id 86514
aaa_uid 466725 auth_serv 1688218168

Jan 23 18:39:56.397:rpms_proc_preauth_response:Deleting Tree node for preauth id 86514 uid
466725
Jan 23 18:39:56.397:cch323_get_ccb_and_delete_from_preauth_tree:Preauth_id=86514
cch323_get_ccb_and_delete_from_preauth_tree:651F87FC node and 6852D5BC ccb
```

Table 1 describes the significant fields shown in the display.

Table 1 debug cch323 preauth Field Descriptions

Field	Description
Request	Request Type—0 for preauthentication, 1 for disconnect.
Preauth id	Identifier for the preauthentication request.
EndPt Type	Call Origin End Point Type—1 for IP address, 2 for IZCT value.
EndPt	Call Origin End Point Value—An IP address or IZCT value.
Resource Service	Resource Service Type—1 for Reservation, 2 for Query.
Call_origin	Answer.
Call_type	VoIP.
Calling_num	Calling Party Number (CLID).
Called_num	Called Party Number (DNIS).
Protocol	0 for H.323, 1 for SIP.
function reports	Various identifiers and status reports for executed functions.

debug ccsip preauth

To enable diagnostic reporting of authentication, authorization, and accounting (AAA) preauthentication for Session Initiation Protocol (SIP) calls, use the **debug ccsip preauth** command in privileged EXEC mode. To disable diagnostic reporting, use the **no** form of this command.

debug ccsip preauth

no debug ccsip preauth

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples

The following example shows debug output for a single SIP call:

```
Router# debug ccsip preauth

SIP Call preauth tracing is enabled
Jan 23 18:43:17.898::Preauth Required
Jan 23 18:43:17.898: In sipSPISendPreauthReq for preauth_id = 86515, ccb = 67AF4E10
Jan 23 18:43:17.898: Entering rpms_proc_print_preauth_req

Jan 23 18:43:17.898: Request = 0
Jan 23 18:43:17.898: Preauth id = 86515
Jan 23 18:43:17.898: EndPt Type  = 1
Jan 23 18:43:17.898: EndPt = 192.168.80.70
Jan 23 18:43:17.898: Resource Service = 1
Jan 23 18:43:17.898: Call_origin = answer
Jan 23 18:43:17.898: Call_type = voip
Jan 23 18:43:17.898: Calling_num = 2270001
Jan 23 18:43:17.898: Called_num = 1170001
Jan 23 18:43:17.898: Protocol  = 1
Jan 23 18:43:17.898:sipSPISendPreauthReq:Created node with preauth_id = 86515, ccb
67AF4E10 , node 6709C280
Jan 23 18:43:17.898:rpms_proc_create_node:Created node with preauth_id = 86515
Jan 23 18:43:17.898:rpms_proc_send_aaa_req:uid got is 466728
Jan 23 18:43:17.902:rpms_proc_preauth_response:Context is for preauth_id 86515, aaa_uid
466728
Jan 23 18:43:17.902:rpms_proc_preauth_response:Deleting Tree node for preauth id 86515 uid
466728
Jan 23 18:43:17.902:sipSPIGetNodeForPreauth:Preauth_id=86515

Jan 23 18:43:17.902: ccsip_spi_process_preauth_event:67AF4E10 ccb & 6709C280 node
Jan 23 18:43:17.902: In act_preauth_response:67AF4E10 ccb
Jan 23 18:43:17.902: act_preauth_response:Deleting node 6709C280 from tree
```

Table 2 describes the significant fields shown in the display.

Table 2 debug ccsip preauth Field Descriptions

Field	Description
Request	Request Type—0 for preauthentication, 1 for disconnect.
Preauth id	Identifier for the preauthentication request.
EndPt Type	Call Origin End Point Type—1 for IP address, 2 for Interzone ClearToken (IZCT) value.
EndPt	Call Origin End Point Value—An IP address or IZCT value.
Resource Service	Resource Service Type—1 for Reservation, 2 for Query.
Call_origin	Answer.
Call_type	VoIP.
Calling_num	Calling Party Number (CLID).
Called_num	Called Party Number (DNIS).
Protocol	0 for H.323, 1 for SIP.
function reports	Various identifiers and status reports for executed functions.

debug rpms-proc preauth

To enable diagnostic reporting of preauthentication information, use the **debug rpms-proc preauth** command in privileged EXEC mode. To disable diagnostic reporting, use the **no** form of this command.

debug rpms-proc preauth {**all** | **h323** | **sip**}

no debug rpms-proc preauth {**all** | **h323** | **sip**}

Syntax Description

all	Provides information for all calls.
h323	Provides information for H.323 calls.
sip	Provides information for Session Initiation Protocol (SIP) calls.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples

The following example shows debug output for two calls. The first is a leg 3 SIP call, and the second is a leg 3 H.323 call:

```
Router# debug rpms-proc preauth all

All RPMS Process preauth tracing is enabled
Feb 10 14:00:07.236: Entering rpms_proc_print_preauth_req

Feb 10 14:00:07.236: Request = 0
Feb 10 14:00:07.236: Preauth id = 8
Feb 10 14:00:07.236: EndPt Type  = 1
Feb 10 14:00:07.236: EndPt = 192.168.80.70
Feb 10 14:00:07.236: Resource Service = 1
Feb 10 14:00:07.236: Call_origin = answer
Feb 10 14:00:07.236: Call_type = voip
Feb 10 14:00:07.236: Calling_num = 2220001
Feb 10 14:00:07.236: Called_num = 1120001
Feb 10 14:00:07.236: Protocol  = 1
Feb 10 14:00:07.236:rpms_proc_create_node:Created node with preauth_id = 8
Feb 10 14:00:07.236:rpms_proc_send_aaa_req:uid got is 19
Feb 10 14:00:07.240:rpms_proc_preauth_response:Context is for preauth_id 8, aaa_uid 19
Feb 10 14:00:07.240:rpms_proc_preauth_response:Deleting Tree node for preauth id 8 uid 19
Feb 10 14:00:07.284: Entering rpms_proc_print_preauth_req

Feb 10 14:00:07.284: Request = 0
Feb 10 14:00:07.284: Preauth id = 9
Feb 10 14:00:07.284: EndPt Type  = 1
Feb 10 14:00:07.284: EndPt = 192.168.81.102
Feb 10 14:00:07.284: Resource Service = 1
Feb 10 14:00:07.284: Call_origin = answer
Feb 10 14:00:07.284: Call_type = voip
Feb 10 14:00:07.284: Calling_num = 2210001
Feb 10 14:00:07.284: Called_num = 1#1110001
```

```
Feb 10 14:00:07.284: Protocol  = 0
Feb 10 14:00:07.288:rpms_proc_create_node:Created node with preauth_id = 9
Feb 10 14:00:07.288:rpms_proc_send_aaa_req:uid got is 21
Feb 10 14:00:07.300:rpms_proc_preauth_response:Context is for preauth_id 9, aaa_uid 21
Feb 10 14:00:07.300:rpms_proc_preauth_response:Deleting Tree node for preauth id 9 uid 21
```

The following example shows the output for a single leg 3 H.323 call:

```
Router# debug rpms-proc preauth h323

RPMS Process H323 preauth tracing is enabled
Feb 10 14:04:57.867: Entering rpms_proc_print_preauth_req

Feb 10 14:04:57.867: Request = 0
Feb 10 14:04:57.867: Preauth id = 10
Feb 10 14:04:57.867: EndPt Type  = 1
Feb 10 14:04:57.867: EndPt = 192.168.81.102
Feb 10 14:04:57.867: Resource Service = 1
Feb 10 14:04:57.867: Call_origin = answer
Feb 10 14:04:57.867: Call_type = voip
Feb 10 14:04:57.867: Calling_num = 2210001
Feb 10 14:04:57.867: Called_num = 1#1110001
Feb 10 14:04:57.867: Protocol  = 0
Feb 10 14:04:57.867:rpms_proc_create_node:Created node with preauth_id = 10
Feb 10 14:04:57.867:rpms_proc_send_aaa_req:uid got is 25
Feb 10 14:04:57.875:rpms_proc_preauth_response:Context is for preauth_id 10, aaa_uid 25
Feb 10 14:04:57.875:rpms_proc_preauth_response:Deleting Tree node for preauth id 10 uid 25
```

The following example shows output for a single leg 3 SIP call:

```
Router# debug rpms-proc preauth sip

RPMS Process SIP preauth tracing is enabled
Feb 10 14:08:02.880: Entering rpms_proc_print_preauth_req

Feb 10 14:08:02.880: Request = 0
Feb 10 14:08:02.880: Preauth id = 11
Feb 10 14:08:02.880: EndPt Type  = 1
Feb 10 14:08:02.880: EndPt = 192.168.80.70
Feb 10 14:08:02.880: Resource Service = 1
Feb 10 14:08:02.880: Call_origin = answer
Feb 10 14:08:02.880: Call_type = voip
Feb 10 14:08:02.880: Calling_num = 2220001
Feb 10 14:08:02.880: Called_num = 1120001
Feb 10 14:08:02.880: Protocol  = 1
Feb 10 14:08:02.880:rpms_proc_create_node:Created node with preauth_id = 11
Feb 10 14:08:02.880:rpms_proc_send_aaa_req:uid got is 28
Feb 10 14:08:02.888:rpms_proc_preauth_response:Context is for preauth_id 11, aaa_uid 28
Feb 10 14:08:02.888:rpms_proc_preauth_response:Deleting Tree node for preauth id 11 uid 28
```

Table 3 describes the significant fields shown in the display.

Table 3 debug rpms-proc preauth Field Descriptions

Field	Description
Request	Request Type—0 for preauthentication, 1 for disconnect.
Preauth id	Identifier for the preauthentication request.
EndPt Type	Call Origin End Point Type—1 for IP address, 2 for Interzone ClearToken (IZCT) value.
EndPt	Call Origin End Point Value—An IP address or IZCT value.

Table 3 debug rpms-proc preauth Field Descriptions (continued)

Field	Description
Resource Service	Resource Service Type—1 for Reservation, 2 for Query.
Call_origin	Answer.
Call_type	VoIP.
Calling_num	Calling party number (calling line identification, or CLID).
Called_num	Called party number (dialed number identification service, or DNIS).
Protocol	0 for H.323, 1 for SIP.
function reports	Various identifiers and status reports for executed functions.

filter voice

To specify that voice calls bypass authentication, authorization, and accounting (AAA) preauthentication, use the **filter voice** command in AAA preauthentication configuration mode. To disable this functionality, use the **no** form of this command.

filter voice

no filter voice

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples

The following example specifies that voice calls bypass AAA preauthentication:

```
Router(config)# aaa preauth
Router(config-preauth)# filter voice
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

radius-server attribute 6

To set an option for RADIUS Attribute 6 (Service-Type) values in a RADIUS profile, use the **radius-server attribute 6** command in global configuration mode. To return to the default, use the **no** form of this command.

radius-server attribute 6 {**on-for-login-auth** | **support-multiple** | **voice 1**}

no radius-server attribute 6

Syntax Description

on-for-login-auth	Sends Attribute 6 (Service-Type) in the authentication packet.
support-multiple	Supports multiple service-type values in each RADIUS profile.
voice 1	Selects the service-type value for voice calls. The **voice 1** keyword pair sets the service-type value to login or login-user.

Defaults

None of the Attribute 6 options is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The **support-multiple** keyword allows for multiple instances of the Service-Type attribute to be present in an Access-Accept packet. The default behavior is to disallow multiple instances, which results in treating an Access-Accept that contains them as though an Access-Reject was received.

Examples

The following example sets support for multiple service-type values in each RADIUS profile:

```
Router(config)# radius-server attribute 6 support-multiple
```

service-type call-check

To identify preauthentication requests to the authentication, authorization, and accounting (AAA) server, use the **service-type call-check** command in AAA preauthentication configuration mode. To return this setting to the default, use the **no** form of this command.

service-type call-check

no service-type call-check

Syntax Description

This command has no arguments or keywords.

Defaults

The service type is not set to call-check.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Setting the service-type attribute to call-check causes preauthentication Access-Requests to include this value, which allows AAA servers to distinguish preauthentication requests from other types of Access-Requests. This command has no effect on packets that are not of the preauthentication type.

Examples

The following example sets the RADIUS service type attribute to call-check:

```
Router(config)# aaa preauth
Router(config-preauth)# service-type call-check
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

show rpms-proc counters

To display statistics for the number of leg 3 authentication, authorization, and accounting (AAA) preauthentication requests, successes, and rejects, use the **show rpms-proc counters** command in privileged EXEC mode.

show rpms-proc counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Leg 3 refers to a call segment from the IP network to a terminating (outgoing) gateway that takes traffic from an IP network to a PSTN network.

Examples

The following example displays leg 3 statistics for AAA preauthentication requests, successes, and rejects:

```
Router# show rpms-proc counters

H323 Calls

Preauth Requests Sent      : 43433
Preauth Requests Accepted  : 43433
Preauth Requests Rejected  : 0
Preauth Requests TimedOut  : 0
Disconnects during Preauth : 0

SIP Calls

Preauth Requests Sent      : 43080
Preauth Requests Accepted  : 43080
Preauth Requests Rejected  : 0
Preauth Requests TimedOut  : 0
Disconnects during Preauth : 0
```

Table 4 describes the significant fields shown in the display.

Table 4 show rpms-proc counters Field Descriptions

Field	Description
Preauth Requests Sent	Number of preauthentication requests sent.
Preauth Requests Accepted	Number of preauthentication requests accepted.

Table 4 show rpms-proc counters Field Descriptions (continued)

Field	Description
Preauth Requests Rejected	Number of preauthentication requests rejected.
Preauth Requests Timed Out	Number of preauthentication requests rejected because they timed out.
Disconnects during Preauth	Number of calls that were disconnected during the preauthentication process.

Related Commands

Command	Description
clear rpms-proc counters	Clears statistics counters for AAA preauthentication requests, successes, and rejects.

timeout leg3

To set the timeout value for a leg 3 authentication, authorization, and accounting (AAA) preauthentication request, use the **timeout leg3** command in AAA preauthentication configuration mode. To return the timeout value to its default, use the **no** form of this command.

timeout leg3 *milliseconds*

no timeout leg3 *milliseconds*

Syntax Description

milliseconds	Timeout value for leg 3 preauthentication, in milliseconds. The range is from 100 to 1000.

Defaults

The default is 100 milliseconds.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

If the timeout timer expires before AAA has responded to a preauthentication request, the call is rejected.

Leg 3 refers to a call segment from the IP network to a terminating (outgoing) gateway that takes traffic from an IP network to a PSTN network.

Examples

The following example sets the timeout for a leg 3 AAA preauthentication request to 250 milliseconds:

```
Router(config)# aaa preauth
Router(config-preauth)# timeout leg3 250
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

Glossary

AAA—authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on a Cisco router or access server.

authentication—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol that you select, encryption.

call leg—Discrete segment of a call connection that lies between two points in a connection. A call leg is a logical connection between the gateway router and either a telephony endpoint over a bearer channel or another endpoint using a session protocol. Each call processed through a gateway router consists of an incoming and an outgoing call leg.

CLID—Calling line identification number, also referred to as the calling number.

CSPS—Cisco SIP Proxy Server.

DNIS—Dialed number identification service number, also referred to as the called number.

H.323—An International Telecommunication Union (ITU-T) standard that describes packet-based video, audio, and data conferencing. H.323 is an umbrella standard that describes the architecture of the conferencing system and refers to a set of other standards (H.245, H.225.0, and Q.931) to describe its actual protocol.

ITSP—Internet telephony service provider. Company that provides telephone services over IP to end users.

IZCT—Interzone ClearToken. Packet of information about a call that is circulated between gatekeepers and between gatekeepers and gateways to manage the routing of the call.

leg 1—Call segment between the PSTN and the originating gateway (see also *call leg*).

leg 2—Call segment between the originating gateway and the IP network (see also *call leg*).

leg 3—Call segment between the IP network and the terminating gateway (see also *call leg*).

leg 4—Call segment between the terminating gateway and the PSTN (see also *call leg*).

PPM—port policy management. The handling of gateway port resources based on configured parameters that enforce specified policies.

PPMS—port policy management server.

preauthentication—Feature that allows a universal gateway to accept or reject a call before it is connected on the basis of information associated with the call, such as DNIS, CLID, or call type (also referred to as the *bearer capability*).

PSTN—Public Switched Telephone Network.

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a distributed client-server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

RADIUS-based PPM server—Software that manages port policy in conjunction with RADIUS and AAA. Can be Cisco RPMS or a third-party product.

RPMS—Cisco Resource Policy Management System. Management software with a web-browser-based configuration utility that enables telephone companies and Internet service providers (ISPs) to count, control, manage, and provide accounting data for shared resources for wholesale virtual private dial-up network (VPDN) and non-VPDN dial network services across one or more network access server (NAS) stacks. RPMS is an example of a RADIUS-based PPM server.

SIP—Session Initiation Protocol. Protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.

SLA—service-level agreements. Contract between a wholesaler and a service provider that specifies the connectivity, performance, and availability levels that the wholesaler guarantees.

T-ASP—telephony application service provider. Company that provides voice applications such as prepaid calling.