RADIUS-Based Lawful Intercept

First Published: February 21, 2006
Last Updated: March 9, 2006

The RADIUS-Based Lawful Intercept feature introduces a new method of conducting lawful interception of traffic data. Intercept requests are sent from the RADIUS server to the network access server (NAS) or to the Layer 2 Tunnel Protocol access concentrator (LAC) by using Access-Accept packets or Change of Authorization (CoA) Request packets. All data traffic going to or from a PPP or L2TP session is passed to a mediation device.

Previously, to intercept traffic data you had to wait for an IP address to be assigned to the session.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for RADIUS-Based Lawful Intercept" section on page 31.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- Prerequisites for RADIUS-Based Lawful Intercept, page 2
- Restrictions for RADIUS-Based Lawful Intercept, page 2
- Information About RADIUS-Based Lawful Intercept, page 2
- How to Configure RADIUS-Based Lawful Intercept, page 5
- Configuration Examples for RADIUS-Based Lawful Intercept, page 8
- Additional References, page 9
- Command Reference, page 10
- Feature Information for RADIUS-Based Lawful Intercept, page 31

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for RADIUS-Based Lawful Intercept

Before enabling a RADIUS-based lawful intercept solution, ensure that your network supports the following features:

- Intercept requests in Access-Accept packets, which allow data interception to start at the beginning of a session.
- Intercept requests in CoA packets, which allow data interception to start or stop during an existing session.
- PPP packet interception.

Restrictions for RADIUS-Based Lawful Intercept

- The RADIUS-Based Lawful Intercept feature cannot honor both CoA requests and lawful intercept requests simultaneously. When a CoA-Request packet is identified as a lawful intercept request, the packet is consumed by the lawful intercept functionality, and it is not passed to other CoA packets.
- If there are attributes other than the required four LI attributes and the Acct-Session-ID attribute 44, the CoA-Request packet is rejected. However, Access-Accept packets can contain attributes that are not related to lawful intercept.
- When using the IP address, the tap must be set by using the Simple Network Management Protocol (SNMP); the tap cannot be set by using RADIUS.

Information About RADIUS-Based Lawful Intercept

To configure the RADIUS-Based Lawful Intercept feature, you need to understand the following concepts:

- RADIUS-Based Lawful Intercept Solutions, page 2
- RADIUS Attributes Used to Specify an Intercept Request, page 3
- Intercept Operation, page 4

RADIUS-Based Lawful Intercept Solutions

A RADIUS-based lawful intercept solution enables intercept requests to be sent (via Access-Accept packets or CoA-Request packets) to the NAS or to the LAC from the RADIUS server. All traffic data going to or from a PPP or L2TP session is passed to a mediation device. Another advantage of RADIUS-based lawful intercept is the synchronicity of the solution—the tap is set with Access-Accept packets so that all target traffic is intercepted.

Without a RADIUS-based solution, Cisco's lawful intercept implementation must use the CISCO-TAP-MIB. Intercept requests are initiated by the mediation device via SNMPv3 messages, and all traffic data going to or from a given IP address is passed to a mediation device. Interception based on IP addresses prevents a session from being tapped until an IP address has been assigned to the session.

RADIUS Attributes Used to Specify an Intercept Request

Table 1 describes the four attributes that are required to specify an intercept request in Access-Accept packets or in CoA-Request packets. CoA-Request packets must have attribute 44, Acct-Session-ID, to identify the user session to which the Lawful Intercept feature should be applied. If a packet contains more than four attributes, the RADIUS packet is ignored. If an attribute name is misspelled, the security for that RADIUS profile will be affected when the **debug radius** command is entered.

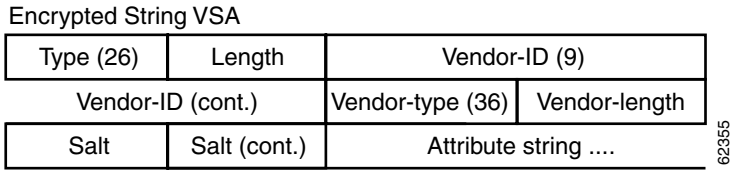
Note The RADIUS server must support encoding and decoding of salt-encrypted attributes.

Each attribute (except for CoA-Request attribute 44) is salt-encrypted. The *salt* field ensures that the uniqueness of the encryption key is used to encrypt each instance of the vendor-specific attribute (VSA). The first and most significant bit of the *salt* field must be set to 1. Cisco VSA type 36 specifies the intercept attributes. See Figure 1.

Table 1 Intercept Request RADIUS Attribute Field Descriptions

Attribute Name	Length	Vendor-Length	Attribute String	Description
Intercept-Identifier	42	36	intercept-id=*value* *value* is eight digits.	Identifies the intercepted target session. Send a unique Intercept-Identifier attribute for all tapped sessions; otherwise, the session is not tapped. (The mediation device is responsible for ensuring that this attribute is unique for all tapped sessions.)
LI-Action	26	20	li-action=0, 1, or 2.	Specifies one of the following intercept actions: • 0—Stop interception of a session. • 1—Start interception of a session. • 2—No action; a dummy interception is ignored. Check to see if a subscriber is logged on. When LI-Action is in Access-Accept packets, only 1 starts the tap. When LI-Action is in CoA-Request packets, you can enter any action.
MD-IP-Address	42 or more	36 or more	md-ip-addr=*address* *address* is a Version 4 IP address in dotted format.	Specifies the IP address of the mediation device that receives the duplicated data. **Note** The IP address cannot be 255.255.255.255 or 0.0.0.0.
MD-Port-Number	26	20	md-port=*port* *port* is 1 through 5.	Specifies the User Data Protocol (UDP) port number of the mediation device that receives the duplicated data.

Figure 1 Encrypted String VSA Format



Intercept Operation

This section describes the following:

- How Intercept Requests Work Within Access-Accept Packets, page 4
- How Intercept Requests Work Within CoA-Request Packets, page 4

How Intercept Requests Work Within Access-Accept Packets

When an intercept target begins to establish a connection, an Access-Request packet is sent to the RADIUS server. The RADIUS server responds with an Access-Accept packet containing the four RADIUS attributes that are listed in Table 1.

The NAS or the LAC receives the LI-Action attribute with the value 1, allowing the NAS or LAC to duplicate the traffic data at the start of the new session and forward the duplicated data to the mediation device that was specified via the attributes MD-IP-Address and MD-Port-Number.

Note If the NAS or LAC cannot start intercepting traffic data for a new session, the session will not be established.

If accounting is enabled (via the **aaa accounting network** command and the **aaa accounting send stop-record authentication failure** command), an Accounting-Stop packet will not be sent with the Acct-Termination-Cause attribute (attribute 49) set to 15 (which means that service is not available).

How Intercept Requests Work Within CoA-Request Packets

After a session has been established for the intercept target, CoA-Request packets can be used for the following tasks:

- Starting the interception of an existing session. The LI-Action attribute is set to 1.
- Stopping the interception of an existing session. The LI-Action attribute is set to 0.
- Issuing a “dummy” intercept request. The LI-Action attribute is set to 2. The NAS or LAC should not perform any session interception; instead, it searches the session on the basis of the Acct-Session-ID attribute value that was specified in the CoA-Request packets. If a session is found, the NAS or LAC sends a CoA acknowledgment (ACK) response to the RADIUS server. If a session is not found, the NAS or LAC issues a “session not found” error message.

Errors are in the CoA-ACK packet attribute 101. Following are possible CoA-ACK settings that the Lawful Intercept feature can set:

- 401: Unsupported Attribute (There is a non-LI attribute, except for 44 which is allowed.)
- 402: Missing Attribute (One of the four LI attributes is missing.)
- 404: Invalid Request (An LI attribute is malformed or duplicated.)
- 501: Administratively Prohibited (AAA Intercept is not configured.)
- 503: Session Context Not Found (Session does not exist.)
- 506: Resources Unavailable (Memory is low.)
- 200: Success (There are no errors; the CoA-Request was accepted and acted on.)

In each case, the RADIUS server must send CoA-Request packets (code 43) with the attributes identified in Table 1 plus the Acct-Session-ID attribute (attribute 44). Each of these attributes must be in the packet.

The Acct-Session-ID attribute identifies the session that will be intercepted. The Acct-Session-ID attribute can be obtained from either the Access-Request packet or the Accounting-Stop packet by entering the **radius-server attribute 44 include-in-access-req** command.

When a session is being tapped and the session terminates, the tap stops. The session does not start when the subscriber logs back in unless the Access-Accept indicates a start tap or a CoA-Request is sent to start the session.

Note The frequency of CoA-Request packets should not exceed a rate of one request every 10 minutes.

How to Configure RADIUS-Based Lawful Intercept

This section contains the following procedure:

- Enabling Lawful Intercept, page 5 (required)

Enabling Lawful Intercept

To enable a RADIUS-Based Lawful Intercept solution on your router, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa intercept**
4. **aaa authentication ppp** {**default** | *list-name*} **group radius**
5. **aaa accounting send stop-record authentication failure**
6. **aaa accounting network** {**default** | *list-name*} **start-stop group** {**radius** | *group-name*}
7. **radius-server attribute 44 include-in-access-req**
8. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]

9. **aaa server radius dynamic-author**
10. **client** *ip-address*
11. **server-key** [**0** | **7**] *word*
12. **port** *port-number*
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa intercept** **Example:** `Router(config)# aaa intercept`	Enables lawful intercept on a router. **Note** You should associate this command with high administrative security so that unauthorized personnel cannot stop intercepts if this command is removed.
Step 4	**aaa authentication ppp** {**default** | *list-name*} **group radius** `Rouuter(config)# aaa authentication ppp default group radius`	Specifies one or more authentication, authorization, and accounting methods for use on serial interfaces that are running PPP. **Note** This command is required because tap information resides only on the RADIUS server. You can authenticate with locally configured information, but you cannot specify a tap with locally configured information.
Step 5	**aaa accounting send stop-record authentication failure** **Example:** `Router(config)# aaa accounting send stop-record authentication failure`	(Optional) Generates accounting stop records for users who fail to authenticate either while logging in or during session negotiation. If an LI-action of 1 does *not* start the tap, the stop record contains Acct-Termination-Cause, attribute 49, set to 15 (Service Unavailable).
Step 6	**aaa accounting network** {**default** | *list-name*} **start-stop group** {**radius** | *group-name*} **Example:** `Router(config)# aaa accounting network default start-stop group radius`	(Optional) Enables accounting for all network-related service requests. This command is required only for determining the reason why a desired tap did not start.

	Command or Action	Purpose
Step 7	**radius-server attribute 44 include-in-access-req** **Example:** `Router(config)# radius-server attribute 44 include-in-access-req`	(Optional) Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication. **Note** We recommend that you enter this command to obtain attribute 44 from the Access-Request packet; otherwise, you will have to wait for the accounting packets to be received before you can determine the value of attribute 44.
Step 8	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*][**acct-port** *port-number*] [**timeout** *seconds*][**retransmit** *retries*][**key** *string*][**alias** {*hostname* | *ip-address*}] **Example:** `Router(config)# radius-server host host1`	(Optional) Specifies a RADIUS server host.
Step 9	**aaa server radius dynamic-author** **Example:** `Router(config)# aaa server radius dynamic-author`	Configures a device (such as an Intelligent Service Gateway [ISG]) as an AAA server to facilitate interaction with an external policy server and enters dynamic authorization local server configuration mode. **Note** This command is optional if taps are always started when a session starts. The command is required for starting and stopping taps on existing sessions by using CoA-Requests.
Step 10	**client** *ip-address* **Example:** `Router(config-locsvr-da-radius)# client 10.0.0.2`	(Optional) Specifies a RADIUS client from which a device will accept CoA-Request packets.
Step 11	**server-key** [**0** | **7**] *word* **Example:** `Router(config-locsvr-da-radius)# server-key cisco`	(Optional) Configures the RADIUS key to be shared between a device and RADIUS clients.
Step 12	**port** *port-number* **Example:** `Router(config-locsvr-da-radius)# port 1600`	(Optional) Specifies a RADIUS client from which a device will accept CoA-Request packets.
Step 13	**exit** **Example:** `Router(config-locsvr-da-radius)# exit`	Exits dynamic authorization local server configuration mode and returns to global configuration mode.

Troubleshooting Tips

You can use the following commands to troubleshoot your lawful intercept configuration:

- **debug aaa accounting**
- **debug aaa authentication**
- **debug aaa coa**
- **debug ppp authentication**
- **debug radius**

Configuration Examples for RADIUS-Based Lawful Intercept

This section provides the following configuration example:

- Enabling RADIUS-Based Lawful Intercept on a Router: Example, page 8

Enabling RADIUS-Based Lawful Intercept on a Router: Example

The following example shows the configuration of a RADIUS-Based Lawful Intercept solution on a router acting as NAS device employing an Ethernet PPP connection over ATM (PPPoEoA) link:

```
aaa new-model
!
aaa intercept
!
aaa group server radius SG
server 10.0.56.17 auth-port 1645 acct-port 1646
!
aaa authentication login LOGIN group SG
aaa authentication ppp default group SG
aaa authorization network default group SG
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group SG
!
aaa server radius dynamic-author
client 10.0.56.17 server-key cisco
!
vpdn enable
!
bba-group pppoe PPPoEoA-TERMINATE
virtual-template 1
!
interface Loopback0
ip address 10.1.1.2 255.255.255.0
!
interface FastEthernet4/1/0
description To RADIUS server
ip address 10.0.56.20 255.255.255.0
duplex auto
!
interface FastEthernet4/1/2
description To network
ip address 10.1.1.1 255.255.255.0
duplex auto
!
interface ATM5/0/0
```

```
description To subscriber
no ip address
!
interface ATM5/0/0.1 point-to-point
pvc 10/808
protocol pppoe group PPPoEoA-TERMINATE
!
interface Virtual-Template1
ip unnumbered Loopback0
ppp authentication chap
!
radius-server attribute 44 include-in-access-req
radius-server attribute nas-port format d
radius-server host 10.0.56.17 auth-port 1645 acct-port 1646
radius-server key cisco
```

Additional References

The following sections provide references related to the RADIUS-Based Lawful Intercept feature.

Related Documents

Related Topic	Document Title
RADIUS attributes and VSA overview information	The section "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide,* Release 12.4
Lawful Intercept Architecture	*Lawful Intercept Architecture*

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
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://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*
RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*
RFC 3576	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

- **aaa intercept**
- **aaa server radius dynamic-author**
- **client**
- **debug ssm**
- **port**
- **server-key**
- **show ssm**
- **show subscriber session**

aaa intercept

To enable lawful intercept on a router, use the **aaa intercept** command in global configuration mode. To disable lawful intercept, use the **no** form of this command.

aaa intercept

no aaa intercept

Syntax Description

This command has no arguments or keywords.

Command Default

Lawful intercept is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use the **aaa intercept** command to enable a RADIUS-Based Lawful Intercept solution on your router. Intercept requests are sent (via Access-Accept packets or CoA-Request packets) to the network access server (NAS) or the Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC) from the RADIUS server. All data traffic going to or from a PPP or L2TP session is passed to a mediation device.

Configure this command with high administrative security so that unauthoried people cannot remove the command.

Examples

The following example shows the configuration of a RADIUS-Based Lawful Intercept solution on a router acting as NAS device employing an Ethernet PPP connection over ATM (PPPoEoA) link:

```
aaa new-model
!
aaa intercept
!
aaa group server radius SG
server 10.0.56.17 auth-port 1645 acct-port 1646
!
aaa authentication login LOGIN group SG
aaa authentication ppp default group SG
aaa authorization network default group SG
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group SG
!
aaa server radius dynamic-author
client 10.0.56.17 server-key cisco
!
vpdn enable
!
bba-group pppoe PPPoEoA-TERMINATE
```

```
virtual-template 1
!
interface Loopback0
ip address 10.1.1.2 255.255.255.0
!
interface FastEthernet4/1/0
description To RADIUS server
ip address 10.0.56.20 255.255.255.0
duplex auto
!
interface FastEthernet4/1/2
description To network
ip address 10.1.1.1 255.255.255.0
duplex auto
!
interface ATM5/0/0
description To subscriber
no ip address
!
interface ATM5/0/0.1 point-to-point
pvc 10/808
protocol pppoe group PPPoEoA-TERMINATE
!
interface Virtual-Template1
ip unnumbered Loopback0
ppp authentication chap
!
radius-server attribute 44 include-in-access-req
radius-server attribute nas-port format d
radius-server host 10.0.56.17 auth-port 1645 acct-port 1646
radius-server key cisco
```

aaa server radius dynamic-author

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the **aaa server radius dynamic-author** command in global configuration mode. To remove this configuration, use the **no** form of this command.

aaa server radius dynamic-author

no aaa server radius dynamic-author

Syntax Description

This command has no arguments or keywords.

Command Default

The device will not function as a server when interacting with external policy servers.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Dynamic authorization allows an external policy server to dynamically send updates to a device.

Dynamic Authorization for the Intelligent Service Gateway (ISG)

ISG works with external devices, referred to as policy servers, that store per-subscriber and per-service information. ISG supports two models of interaction between the ISG device and external policy servers: initial authorization and dynamic authorization.

The dynamic authorization model allows an external policy server to dynamically send policies to the Intelligent Service Gateway (ISG). These operations can be initiated in-band by subscribers (through service selection) or through the actions of an administrator, or applications can change policies on the basis of an algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server.

Examples

The following example configures the ISG to act as a AAA server when interacting with the client at IP address 10.12.12.12:

```
aaa server radius dynamic-author
 client 10.12.12.12 key cisco
 message-authenticator ignore
```

Related Commands

Command	Description
client	Specifies a RADIUS client from which a device will accept CoA and disconnect requests.

client

To specify a RADIUS client from which a device will accept Change of Authorization (CoA) and disconnect requests, use the **client** command in dynamic authorization local server configuration mode. To remove this specification, use the **no** form of this command.

client {*name* | *ip-address*} [**key** [**0** | **7**] *word*] [**vrf** *vrf-id*]

no client {*name* | *ip-address*} [**key** [**0** | **7**] *word*] [**vrf** *vrf-id*]

Syntax Description

name	Hostname of the RADIUS client.
ip-address	IP address of the RADIUS client.
key	(Optional) Configures the RADIUS key to be shared between a device and a RADIUS client.
0	(Optional) Specifies that an unencrypted key will follow.
7	(Optional) Specifies that a hidden key will follow.
word	(Optional) Unencrypted server key.
vrf *vrf-id*	(Optional) Virtual Routing and Forwarding (VRF) ID of the client.

Command Default

CoA and disconnect requests are dropped.

Command Modes

Dynamic authorization local server configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **client** command to specify the RADIUS clients for which the router will act as server.

Examples

The following example configures the router to accept requests from the RADIUS client at IP address 10.0.0.1:

```
aaa server radius dynamic-author
 client 10.0.0.1 key cisco
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures an ISG as a AAA server to facilitate interaction with an external policy server.

debug ssm

To display diagnostic information about the Segment Switching Manager (SSM) for switched Layer 2 segments, use the **debug ssm** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ssm {**cm errors** | **cm events** | **fhm errors** | **fhm events** | **sm errors** | **sm events** | **sm counters** | **xdr**}

no debug ssm {**cm errors** | **cm events** | **fhm errors** | **fhm events** | **sm errors** | **sm events** | **sm counters** | **xdr**}

Syntax Description

cm errors	Displays Connection Manager errors.
cm events	Displays Connection Manager events.
fhm errors	Displays Feature Handler Manager errors.
fhm events	Displays Feature Handler Manager events.
sm errors	Displays Segment Handler Manager errors.
sm events	Displays Segment Handler Manager events.
sm counters	Displays Segment Handler Manager counters.
xdr	Displays external data representation (XDR) messages, which have to do with traffic being sent across the backplane between route processors and linecards.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated to Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The SSM manages the data-plane component of the L2VPN configuration. The CM tracks the connection-level errors and events that occur on an xconnect. The SM tracks the per-segment events and errors on the xconnect.

Use the **debug ssm** command to troubleshoot problems in bringing up the data plane.

This command is generally used only by Cisco engineers for internal debugging of SSM processes.

Examples

The following example shows sample output for the **debug ssm xdr** command.

```
Router# debug ssm xdr

SSM xdr debugging is on

2w5d: SSM XDR: [4096] deallocate segment, len 16
```

```
2w5d: SSM XDR: [8193] deallocate segment, len 16
2w5d: %LINK-3-UPDOWN: Interface FastEthernet2/1, changed state to down
2w5d: %LINK-3-UPDOWN: Interface FastEthernet2/1, changed state to up
2w5d: SSM XDR: [4102] provision segment, switch 4101, len 106
2w5d: SSM XDR: [4102] update segment status, len 17
2w5d: SSM XDR: [8199] provision segment, switch 4101, len 206
2w5d: SSM XDR: [4102] update segment status, len 17
2w5d: %SYS-5-CONFIG_I: Configured from console by console
2w5d: %LINK-3-UPDOWN: Interface FastEthernet2/1, changed state to down
2w5d: SSM XDR: [4102] update segment status, len 17
2w5d: %LINK-3-UPDOWN: Interface FastEthernet2/1, changed state to up
2w5d: SSM XDR: [4102] deallocate segment, len 16
2w5d: SSM XDR: [8199] deallocate segment, len 16
2w5d: SSM XDR: [4104] provision segment, switch 4102, len 106
2w5d: SSM XDR: [4104] update segment status, len 17
2w5d: SSM XDR: [8201] provision segment, switch 4102, len 206
2w5d: SSM XDR: [4104] update segment status, len 17
2w5d: SSM XDR: [4104] update segment status, len 17
2w5d: %SYS-5-CONFIG_I: Configured from console by console
```

The following example shows the events that occur on the segment manager when an Any Transport over MPLS (AToM) virtual circuit (VC) configured for Ethernet over MPLS is shut down and then enabled:

```
Router# debug ssm sm events

SSM Connection Manager events debugging is on

Router(config)# interface fastethernet 0/1/0.1
Router(config-subif)# shutdown

09:13:38.159: SSM SM: [SSS:AToM:36928] event Unprovison segment
09:13:38.159: SSM SM: [SSS:Ethernet Vlan:4146] event Unbind segment
09:13:38.159: SSM SM: [SSS:AToM:36928] free segment class
09:13:38.159: SSM SM: [SSS:AToM:36928] free segment
09:13:38.159: SSM SM: [SSS:AToM:36928] event Free segment
09:13:38.159: SSM SM: last segment class freed
09:13:38.159: SSM SM: [SSS:Ethernet Vlan:4146] segment ready
09:13:38.159: SSM SM: [SSS:Ethernet Vlan:4146] event Found segment data

Router(config-subif)# no shutdown

09:13:45.815: SSM SM: [SSS:AToM:36929] event Provison segment
09:13:45.815: label_oce_get_label_bundle: flags 14 label 16
09:13:45.815: SSM SM: [SSS:AToM:36929] segment ready
09:13:45.815: SSM SM: [SSS:AToM:36929] event Found segment data
09:13:45.815: SSM SM: [SSS:AToM:36929] event Bind segment
09:13:45.815: SSM SM: [SSS:Ethernet Vlan:4146] event Bind segment
```

The following example shows the events that occur on the connection manager when an AToM VC configured for Ethernet over MPLS is shut down and then enabled:

```
Router(config)# interface fastethernet 0/1/0.1
Router(config-subif)# shutdown

09:17:20.179: SSM CM: [AToM] unprovision segment, id 36929
09:17:20.179: SSM CM: CM FSM: state Open - event Free segment
09:17:20.179: SSM CM: [SSS:AToM:36929] unprovision segment 1
09:17:20.179: SSM CM: [SSS:AToM] shQ request send unprovision complete event
09:17:20.179: SSM CM: [SSS:Ethernet Vlan:4146] unbind segment 2
09:17:20.179: SSM CM: [SSS:Ethernet Vlan] shQ request send ready event
09:17:20.179: SSM CM: SM msg event send unprovision complete event
09:17:20.179: SSM CM: SM msg event send ready event

Router(config-subif)# no shutdown
```

```
09:17:35.879: SSM CM: Query AToM to Ethernet Vlan switching, enabled
09:17:35.879: SSM CM: [AToM] provision second segment, id 36930
09:17:35.879: SSM CM: CM FSM: state Down - event Provision segment
09:17:35.879: SSM CM: [SSS:AToM:36930] provision segment 2
09:17:35.879: SSM CM: [AToM] send client event 6, id 36930
09:17:35.879: SSM CM: [SSS:AToM] shQ request send ready event
09:17:35.883: SSM CM: SM msg event send ready event
09:17:35.883: SSM CM: [AToM] send client event 3, id 36930
```

The following example shows the events that occur on the connection manager and segment manager when an AToM VC is provisioned and then unprovisioned:

```
Router# debug ssm cm-ev

SSM Connection Manager events debugging is on
Router# debug ssm sm-ev

SSM Segment Manager events debugging is on

Router# configure terminal
Router(config)# interface ethernet1/0
Router(config-if)# xconnect 55.55.55.2 101 pw-class mpls

16:57:34: SSM CM: provision switch event, switch id 86040
16:57:34: SSM CM: [Ethernet] provision first segment, id 12313
16:57:34: SSM CM: CM FSM: state Idle - event Provision segment
16:57:34: SSM CM: [SSS:Ethernet:12313] provision segment 1
16:57:34: SSM SM: [SSS:Ethernet:12313] event Provison segment
16:57:34: SSM CM: [SSS:Ethernet] shQ request send ready event
16:57:34: SSM CM: SM msg event send ready event
16:57:34: SSM SM: [SSS:Ethernet:12313] segment ready
16:57:34: SSM SM: [SSS:Ethernet:12313] event Found segment data
16:57:34: SSM CM: Query AToM to Ethernet switching, enabled
16:57:34: SSM CM: [AToM] provision second segment, id 16410
16:57:34: SSM CM: CM FSM: state Down - event Provision segment
16:57:34: SSM CM: [SSS:AToM:16410] provision segment 2
16:57:34: SSM SM: [SSS:AToM:16410] event Provison segment
16:57:34: SSM CM: [AToM] send client event 6, id 16410
16:57:34: label_oce_get_label_bundle: flags 14 label 19
16:57:34: SSM CM: [SSS:AToM] shQ request send ready event
16:57:34: SSM CM: SM msg event send ready event
16:57:34: SSM SM: [SSS:AToM:16410] segment ready
16:57:34: SSM SM: [SSS:AToM:16410] event Found segment data
16:57:34: SSM SM: [SSS:AToM:16410] event Bind segment
16:57:34: SSM SM: [SSS:Ethernet:12313] event Bind segment
16:57:34: SSM CM: [AToM] send client event 3, id 16410

Router# configure terminal
Router(config)# interface e1/0
Router(config-if)# no xconnect

16:57:26: SSM CM: [Ethernet] unprovision segment, id 16387
16:57:26: SSM CM: CM FSM: state Open - event Free segment
16:57:26: SSM CM: [SSS:Ethernet:16387] unprovision segment 1
16:57:26: SSM SM: [SSS:Ethernet:16387] event Unprovison segment
16:57:26: SSM CM: [SSS:Ethernet] shQ request send unprovision complete event
16:57:26: SSM CM: [SSS:AToM:86036] unbind segment 2
16:57:26: SSM SM: [SSS:AToM:86036] event Unbind segment
16:57:26: SSM CM: SM msg event send unprovision complete event
16:57:26: SSM SM: [SSS:Ethernet:16387] free segment class
16:57:26: SSM SM: [SSS:Ethernet:16387] free segment
16:57:26: SSM SM: [SSS:Ethernet:16387] event Free segment
16:57:26: SSM SM: last segment class freed
```

```
16:57:26: SSM CM: unprovision switch event, switch id 12290
16:57:26: SSM CM: [SSS:AToM] shQ request send unready event
16:57:26: SSM CM: SM msg event send unready event
16:57:26: SSM SM: [SSS:AToM:86036] event Unbind segment
16:57:26: SSM CM: [AToM] unprovision segment, id 86036
16:57:26: SSM CM: CM FSM: state Down - event Free segment
16:57:26: SSM CM: [SSS:AToM:86036] unprovision segment 2
16:57:26: SSM SM: [SSS:AToM:86036] event Unprovison segment
16:57:26: SSM CM: [SSS:AToM] shQ request send unprovision complete event
16:57:26: SSM CM: SM msg event send unprovision complete event
16:57:26: SSM SM: [SSS:AToM:86036] free segment class
16:57:26: SSM SM: [SSS:AToM:86036] free segment
16:57:26: SSM SM: [SSS:AToM:86036] event Free segment
16:57:26: SSM SM: last segment class freed
```

Related Commands

Command	Description
show ssm	Displays SSM information for switched Layer 2 segments.

port

To specify the port on which a device listens for RADIUS requests from configured RADIUS clients, use the **port** command in dynamic authorization local server configuration mode. To restore the default, use the **no** form of this command.

port *port-number*

no port *port-number*

Syntax Description

port-number	Port number. The default value is port 1700.

Command Default

The device listens for RADIUS requests on the default port (port 1700).

Command Modes

Dynamic authorization local server configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **port** command to specify the ports on which the router will listen for requests from RADIUS clients.

Examples

The following example specifies port 1650 as the port on which the device listens for RADIUS requests:

```
aaa server radius dynamic-author
 client 10.0.0.1
 port 1650
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures a device as a AAA server to facilitate interaction with an external policy server.

server-key

To configure the RADIUS key to be shared between a device and RADIUS clients, use the **server-key** command in dynamic authorization local server configuration mode. To remove this configuration, use the **no** form of this command.

server-key [**0** | **7**] *word*

no server-key [**0** | **7**] *word*

Syntax Description

0	(Optional) An unencrypted key will follow.
7	(Optional) A hidden key will follow.
word	Unencrypted server key.

Command Default

A server key is not configured.

Command Modes

Dynamic authorization local server configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **server-key** command to configure the key to be shared between the ISG and RADIUS clients.

Examples

The following example configures “cisco” as the shared server key:

```
aaa server radius dynamic-author
 client 10.0.0.1
 server-key cisco
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures a device as a AAA server to facilitate interaction with an external policy server.

show ssm

To display Segment Switching Manager (SSM) information for switched Layer 2 segments, use the **show ssm** command in privileged EXEC mode.

show ssm {**cdb** | **feature id** [*feature-id*] | **id** | **memory** [**chunk variable** {**feature** | **queue** | **segment**} | **detail**] | **segment id** [*segment-id*] | **switch id** [*switch-id*]}

Syntax Description

cdb	Displays information about the SSM capabilities database.
feature id	Displays information about SSM feature settings.
feature-id	(Optional) Displays information for a specific feature ID.
id	Displays information for all SSM IDs.
memory	Displays memory usage information.
chunk variable	(Optional) Displays memory usage information for memory consumed by variable chunks.
feature	Displays information about memory consumed by the feature.
queue	Displays information about memory consumed by the queue.
segment	Displays information about memory consumed by the segment.
detail	(Optional) Displays detailed memory usage information.
segment id	Displays information about SSM segment settings.
segment-id	(Optional) Displays information for a specific SSM segment.
switch id	Displays information about SSM switch settings.
switch-id	(Optional) Displays information for a specific SSM switch ID.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(22)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **show ssm** command to determine the segment ID for an active switched Layer 2 segment. The segment ID can be used with the **debug condition xconnect** command to filter debug messages by segment.

Examples

The following example shows sample output for the **show ssm cdb** command. The output for this command varies depending on the type of hardware being used.

```
Router# show ssm cdb

Switching paths active for class SSS:
-------------------------------------
```

```
        |FR |Eth|Vlan|ATM|HDLC|PPP/AC|L2TP|L2TPv3|L2F|PPTP|ATM/AAL5|ATM/VCC|
--------+---+---+----+---+----+------+----+------+---+----+--------+-------+
FR      | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
Eth     | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
Vlan    | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
ATM     |-/E|-/E|-/E |-/-|-/E | -/E  |-/E | -/E  |-/-|-/- |  -/E   |  -/E  |
HDLC    | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
PPP/AC  | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
L2TP    | E | E | E  |E/-| E  |  E   | E  | -/-  | E | E  |   E    |   E   |
L2TPv3  | E | E | E  |E/-| E  |  E   |-/- |  E   |-/-|-/- |   E    |   E   |
L2F     |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
PPTP    |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
ATM/AAL5| E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
ATM/VCC | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
ATM/VPC | E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
ATM/Cell| E | E | E  |E/-| E  |  E   | E  |  E   |-/-|-/- |   E    |   E   |
AToM    |-/E|-/E|-/E |-/-|-/E | -/E  |-/- | -/E  |-/-|-/- |  -/E   |  -/E  |
PPP     |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
PPPoE   |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
PPPoA   |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
Lterm   |-/-|-/-|-/- |-/-|-/- | -/-  | E  | -/-  | E | E  |  -/-   |  -/-  |
TC      |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-  |
IP-If   |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-  |
IP-SIP  |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-  |
VFI     |-/E|-/E|-/E |-/-|-/E | -/E  |-/- | -/E  |-/-|-/- |  -/E   |  -/E  |

        |ATM/Cell|AToM|PPP|PPPoE|PPPoA|Lterm|TC |IP-If|IP-SIP|VFI|
--------+--------+----+---+-----+-----+-----+---+-----+------+---+
FR      |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
Eth     |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
Vlan    |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
ATM     |  -/E   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
HDLC    |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
PPP/AC  |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
L2TP    |   E    |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
L2TPv3  |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
L2F     |  -/-   |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
PPTP    |  -/-   |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
ATM/AAL5|   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
ATM/VCC |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
ATM/VPC |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
ATM/Cell|   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
AToM    |  -/E   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|

PPP     |  -/-   |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
PPPoE   |  -/-   |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
PPPoA   |  -/-   |-/- | E |  E  |  E  |  E  |-/-| -/- | -/-  |-/-|
Lterm   |  -/-   |-/- | E |  E  |  E  |  E  | E |  E  |  E   |-/-|
TC      |  -/-   |-/- |-/-| -/- | -/- |  E  | E |  E  |  E   |-/-|
IP-If   |  -/-   |-/- |-/-| -/- | -/- |  E  | E |  E  | -/-  |-/-|
IP-SIP  |  -/-   |-/- |-/-| -/- | -/- |  E  | E | -/- |  E   |-/-|
VFI     |  -/E   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|

Switching paths active for class ADJ:
-------------------------------------

        |FR |Eth|Vlan|ATM|HDLC|PPP/AC|L2TP|L2TPv3|L2F|PPTP|ATM/AAL5|ATM/VCC|
--------+---+---+----+---+----+------+----+------+---+----+--------+-------+
FR      | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
Eth     | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
Vlan    | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
ATM     |-/E|-/E|-/E |-/-|-/E | -/E  |-/- | -/E  |-/-|-/- |  -/E   |  -/E  |
HDLC    | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
PPP/AC  | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
```

```
L2TP     |-/E|-/E|-/E |-/-|-/E | -/E  | E  | -/-  |E/-|E/- |  -/E   |  -/E  |
L2TPv3   | E | E | E  |E/-| E  |  E   |-/- |  E   |-/-|-/- |   E    |   E   |
L2F      |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-  |
PPTP     |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-  |
ATM/AAL5| E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
ATM/VCC  | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
ATM/VPC  | E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
ATM/Cell| E | E | E  |E/-| E  |  E   |E/- |  E   |-/-|-/- |   E    |   E   |
AToM     |-/E|-/E|-/E |-/-|-/E | -/E  |-/- | -/E  |-/-|-/- |  -/E   |  -/E  |
PPP      |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-  |
PPPoE    |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-  |
PPPoA    |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-  |
Lterm    |-/-|-/-|-/- |-/-|-/- | -/-  |-/E | -/-  |-/-|-/- |  -/-   |  -/-  |
TC       |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-  |
IP-If    |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-  |
IP-SIP   |-/-|-/-|-/- |-/-|-/- | -/-  |-/- | -/-  |-/-|-/- |  -/-   |  -/-  |
VFI      |E/-| E | E  |E/-|E/- | E/-  |-/- | -/E  |-/-|-/- |   E    |   E   |

         |ATM/Cell|AToM|PPP|PPPoE|PPPoA|Lterm|TC |IP-If|IP-SIP|VFI|
---------+--------+----+---+-----+-----+-----+---+-----+------+---+
FR       |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/E|
Eth      |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
Vlan     |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
ATM      |  -/E   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/E|
HDLC     |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/E|
PPP/AC   |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/E|
L2TP     |  -/E   |-/- |E/-| E/- | E/- | E/- |-/-| -/- | -/-  |-/-|
L2TPv3   |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |E/-|
L2F      |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
PPTP     |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
ATM/AAL5|   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
ATM/VCC  |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
ATM/VPC  |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
ATM/Cell|   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  | E |
AToM     |  -/E   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/E|
PPP      |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
PPPoE    |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
PPPoA    |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
Lterm    |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
TC       |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
IP-If    |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
IP-SIP   |  -/-   |-/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|
VFI      |   E    |E/- |-/-| -/- | -/- | -/- |-/-| -/- | -/-  |-/-|

Key:
  '-' - switching type is not available
  'R' - switching type is available but not enabled
  'E' - switching type is enabled
  'D' - switching type is disabled
```

The following example displays SSM output of the **show ssm id** command on a device with one active Layer 2 Tunnel Protocol Version 3 (L2TPv3) segment and one active Frame Relay segment. The segment ID field is in shown in bold.

```
Router# show ssm id

SSM Status: 1 switch
   Switch-ID 4096 State: Open
     Segment-ID: 8193 Type: L2TPv3[8]
       Switch-ID:                  4096
       Physical intf:              Remote
       Allocated By:               This CPU
       Class:                      SSS
```

```
      State:                        Active
      L2X switching  context:
      Session ID Local 16666 Remote 54742
      TxSeq 0 RxSeq 0
      Tunnel end-point addr Local 10.1.1.2 Remote 10.1.1.1
      SSS Info Switch Handle 0x98000000 Ciruit 0x1B19510
      L2X Encap [24 bytes]
       45 00 00 00 00 00 00 00 FF 73 B7 86 01 01 01 02
       01 01 01 01 00 00 D5 D6
    Class:                        ADJ
      State:                        Active
      L2X H/W Switching Context:
      Session Id Local 16666 Remote 54742
      Tunnel Endpoint Addr Local 10.1.1.2 Remote 10.1.1.1
      Adjacency 0x1513348 [complete] PW IP, Virtual3:16666
      L2X Encap [24 bytes]
       45 00 00 00 00 00 00 00 FF 73 B7 86 01 01 01 02
       01 01 01 01 00 00 D5 D6

  Segment-ID: 4096 Type: FR[1]
    Switch-ID:                    4096
    Physical intf:                Local
    Allocated By:                 This CPU
    Class:                        SSS
      State:                        Active
      AC Switching Context:         Se2/0:200
      SSS Info - Switch Handle=0x98000000 Ckt=0x1B194B0
      Interworking 0 Encap Len 0 Boardencap Len 0 MTU 1584
    Class:                        ADJ
      State:                        Active
      AC Adjacency context:
      adjacency = 0x1513618 [complete] RAW Serial2/0:200
```

Additional output displayed by this command is either self-explanatory or used only by Cisco engineers for internal debugging of SSM processes.

The following example shows sample output for the **show ssm memory** command:

```
Router# show ssm memory

  Allocator-Name                  In-use/Allocated            Count
  ------------------------------------------------------------------------------
  SSM CM API large segment  :        208/33600      (  0%) [      1] Chunk
  SSM CM API medium segment :        144/20760      (  0%) [      1] Chunk
  SSM CM API segment info c :        104/160        ( 65%) [      1]
  SSM CM API small segment  :          0/19040      (  0%) [      0] Chunk
  SSM CM inQ interrupt msgs :          0/20760      (  0%) [      0] Chunk
  SSM CM inQ large chunk ms :          0/33792      (  0%) [      0] Chunk
  SSM CM inQ msgs           :        104/160        ( 65%) [      1]
  SSM CM inQ small chunk ms :          0/20760      (  0%) [      0] Chunk
  SSM DP inQ msg chunks     :          0/10448      (  0%) [      0] Chunk
  SSM Generic CM Message    :          0/3952       (  0%) [      0] Chunk
  SSM HW Class Context      :         64/10832      (  0%) [      1] Chunk
  SSM ID entries            :        144/11040      (  1%) [      3] Chunk
  SSM ID tree               :         24/80         ( 30%) [      1]
  SSM INFOTYPE freelist DB  :       1848/2016       ( 91%) [      3]
  SSM SEG Base              :        240/34064      (  0%) [      2] Chunk
  SSM SEG freelist DB       :       5424/5592       ( 96%) [      3]
  SSM SH inQ chunk msgs     :          0/5472       (  0%) [      0] Chunk
  SSM SH inQ interrupt chun :          0/5472       (  0%) [      0] Chunk
  SSM SW Base               :         56/10920      (  0%) [      1] Chunk
  SSM SW freelist DB        :       5424/5592       ( 96%) [      3]
  SSM connection manager    :        816/1320       ( 61%) [      9]
  SSM seg upd info          :          0/2464       (  0%) [      0] Chunk
```

```
Total allocated: 0.246 Mb, 252 Kb, 258296 bytes
```

Related Commands

Command	Description
debug condition xconnect	Displays conditional xconnect debug messages.

show subscriber session

To display information about subscriber sessions on an Intelligent Service Gateway (ISG), use the **show subscriber session** command in privileged EXEC mode.

show subscriber session [**identifier** {**authen-status** {**authenticated** | **unauthenticated**} | **authenticated-domain** *domain-name* | **authenticated-username** *username* | **dnis** *dnis* | **media** *type* | **nas-port** *identifier* | **protocol** *type* | **source-ip-address** *ip-address subnet-mask* | **timer** *timer-name* | **tunnel-name** *name* | **unauthenticated-domain** *domain-name* | **unauthenticated-username** *username*} | **uid** *session-identifier* | **username** *username*] [**detailed**]

Syntax Description

identifier	(Optional) Displays information about subscriber sessions that match the specified identifier.
authen-status	(Optional) Displays information about sessions with a specified authentication status.
authenticated	(Optional) Displays information for sessions that have been authenticated.
unauthenticated	(Optional) Displays information for sessions that have not been authenticated.
authenticated-domain *domain-name*	(Optional) Displays information for sessions with a specific authenticated domain name.
authenticated-username *username*	(Optional) Displays information for sessions with a specific authenticated username.
dnis *dnis*	(Optional) Displays information for sessions with a specific Dialed Number Identification Service (DNIS) number.
media *type*	(Optional) Displays information for sessions that use a specific type of access media.
nas-port *identifier*	(Optional) Displays information for sessions with a specific network access server (NAS) port identifier. The *identifier* argument can be one or more of the following values: • **adapter** *adapter-number* • **channel** *channel-number* • **ipaddr** *ip-address* • **port** *port-number* • **shelf** *shelf-number* • **slot** *slot-number* • **sub-interface** *sub-interface-number* • **type** *interface-type* • **vci** *vci-number* • **vlan** *vlan-id* • **vpi** *vpi-number*
protocol *type*	(Optional) Displays information for sessions that use a specific type of access protocol.

source-ip-address *ip-address subnet-mask*	(Optional) Displays information for sessions associated with a specified source IP address.
timer *timer-name*	(Optional) Displays information for sessions that use a specified timer.
tunnel-name *name*	(Optional) Displays information for sessions associated with a specific VPDN tunnel.
unauthenticated-domain *domain-name*	(Optional) Displays information for sessions with a specific unauthenticated domain name.
unauthenticated-username *username*	(Optional) Displays information for sessions with a specific unauthenticated username.
uid *session-identifier*	(Optional) Displays information for sessions with a specific unique identifier.
username *username*	(Optional) Displays information for sessions associated with a specific username.
detailed	(Optional) Displayed detailed information about sessions.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

If the **show subscriber session** command is entered without any keywords or arguments, information is displayed for all sessions on the ISG. When an identifier is specified, information is displayed for only those sessions that match the identifier.

Examples

The following example shows sample output for the **show subscriber session** command:

```
Router# show subscriber session

Current Subscriber Information: Total sessions 1
Uniq ID Interface State Service Identifier Up-time
6 Traffic-Cl unauthen Ltm Internal rouble-pppoe 00:09:04
5 Vi3 authen Local Term rouble-pppoe 00:09:04
```

The following example shows sample output for the **show subscriber session** command with an identifier specified. In this case, information is displayed for the session with the session identifier 3.

```
Router# show subscriber session identifier uid 3

Current Subscriber Information: Total sessions 1
Uniq ID Interface State Service Identifier Up-time
-----------------------------------------------
Unique Session ID: 3
Identifier: 10.0.0.2
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:15, Last Changed: 00:00:15
```

```
Policy information:
Authentication status: authen
Rules, actions and conditions executed:
subscriber rule-map RULEB
condition always event session-start
1 authorize identifier source-ip-address

Configuration sources associated with this session:
Interface: Ethernet0/0, Active Time = 00:00:15
```

Table 2 describes the significant fields shown in the displays.

Table 2 show subscriber session Field Descriptions

Field	Description
Total Sessions	Number of main sessions on the ISG.
Uniq ID	Session identifier.
Interface	For main sessions, the interface is displayed. For traffic flows, the value “Traffic-Cl” is displayed.
State	Indicates whether the session has been authenticated or is unauthenticated.
Service	May be one of the following values: • Local Term—the session is terminated locally. • Ltm Internal—a flow that was created internally.
Identifier	Username that is used for authorization.
Up-time	Length of time the session has been up.
Unique Session ID	Session identifier.
SIP subscriber access type(s)	Subscriber’s access protocol.
Rules, actions and conditions executed:	Control policy rules, actions, and control class maps (conditions) that have been executed for the session.
Configuration sources associated with this session:	Sources of configuration that have been applied to the session.

Feature Information for RADIUS-Based Lawful Intercept

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

Feature Name	Releases	Feature Configuration Information
Radius-Based Lawful Intercept	12.2(28)SB	The RADIUS-Based Lawful Intercept feature provides a method of conducting lawful interception of data.