



PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer

Feature History

Release	Modification
12.2(4)T	This feature was introduced.
12.2(11)T	Support was added for the Cisco AS5300.
12.2(11)T1	This release provides accelerated access to Stream Control Transmission Protocol (SCTP) and Integrated Services Digital Network (ISDN) User Adaptation Layer (IUA) 0.4 on the Cisco AS5850.

This feature module describes PRI/Q.921 Signaling Backhaul for Call Agent Applications using IP transport protocol SCTP with the IUA. This feature is supported in Cisco IOS Release 12.2(4)T, 12.2(11)T, and 12.2(11)T1.

This document includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 6](#)
- [Supported Standards, MIBs, and RFCs, page 7](#)
- [Prerequisites, page 7](#)
- [Configuration Tasks, page 8](#)
- [Configuration Examples, page 14](#)
- [Command Reference, page 20](#)
- [Glossary, page 48](#)

Feature Overview

The *PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer* feature fulfills the need for a standards based PRI Signaling backhaul that works with third party Call Agents to enable solutions like Integrated Access, IP PBX, and Telecommuter.

This feature provides the following:

- **PRI Backhaul**—Specific implementation for backhauling PRI.
- **SCTP**—New general transport protocol that can be used for backhauling signaling messages.
- **IUA**—Mechanism for backhauling any Layer 3 protocol that normally uses Q.921.

These features do the following:

- Provide a configuration interface for Cisco IOS software implementation.
- Implement the protocol message flows for SCTP and IUA.

PRI Backhaul

The PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer feature provides standards-based ISDN signaling backhaul capability on Cisco IOS Gateways. Signaling backhaul is used in voice network architectures employing a Call Agent (also called Media Gateway Controller or MGC), where the call processing for voice calls is carried out by the call control servers, and the packet network connections are made using protocols such as the Media Gateway Control Protocol (MGCP) and the Simple Gateway Control Protocol (SGCP).

Signaling backhaul facilitates the handling of voice traffic coming from the signaling endpoints, which communicate using facility associated signaling. Facility associated signaling requires the signaling channel (a channel carrying call signaling information) to share a digital facility with the bearer channels. ISDN PRI is one example of facility associated signaling.

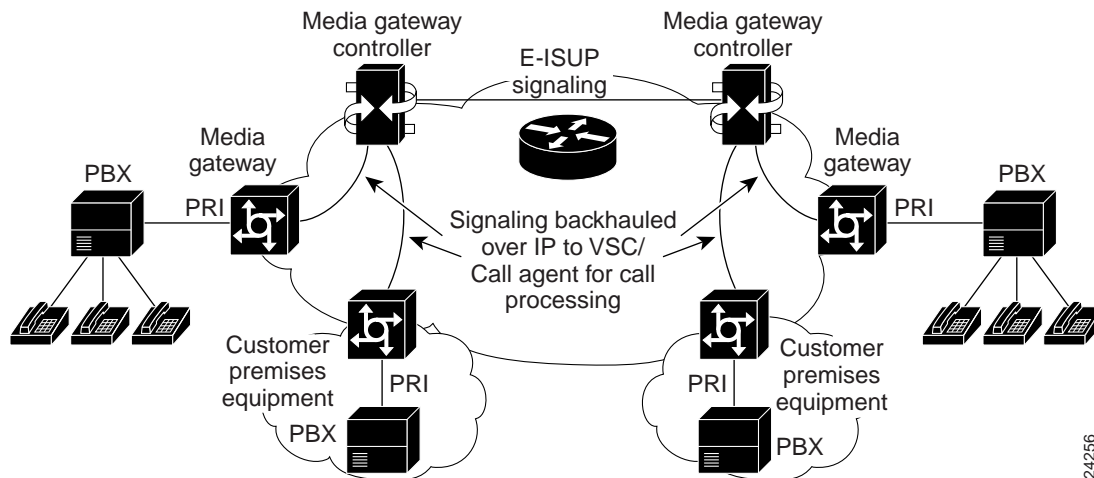
This feature implements the Internet Engineering Task Force (IETF) standards-based signaling backhaul protocols. This standards-based signaling transport support enables any third party Call Agent that supports the standards to work with Cisco gateways. ISDN signaling backhaul is required in the MGCP-based call control architecture to enable end-to-end voice solutions.

PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer migrates the proprietary PRI backhaul infrastructure to open standards. The backhauling is carried out using industry standard SCTPs and ISDN IUA protocols as defined by the SIGTRAN working group of the IETF.

This feature supports backhauling of the ISDN-based signaling protocols only.

Figure 1 shows an example of PRI signaling backhaul. The MGC provides call processing and gateway control.

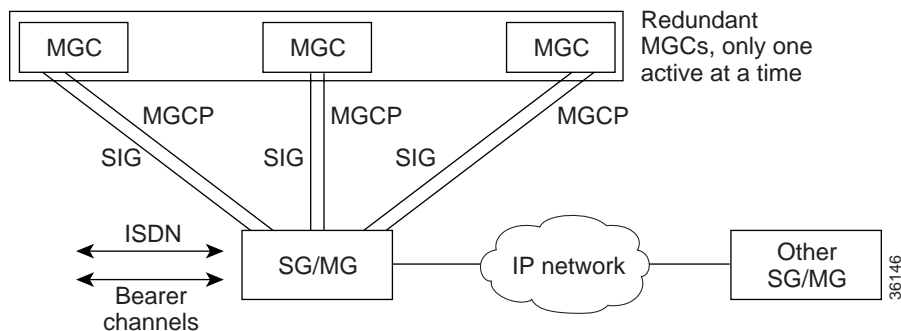
Figure 1 PRI Signaling Backhaul



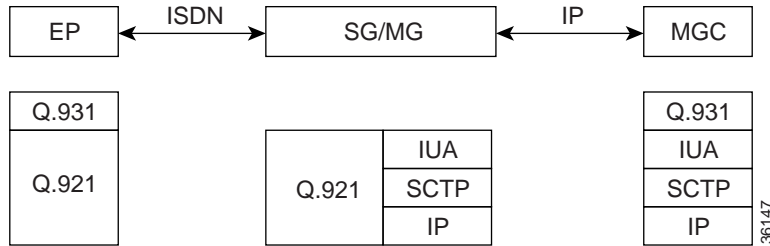
Ordinarily, signaling backhaul occurs at a common boundary for all protocols. For ISDN, the signaling backhaul takes place at the Layer 2 (Q.921) and Layer 3 (Q.931) boundaries. The lower layers of the protocol (Q.921) are terminated and processed on the gateway, while the upper layers (Q.931) are backhauled to the MGC using SCTP. Signaling backhaul provides the advantage of distributed protocol processing. This permits greater expandability and scalability while offloading lower layer protocol processing from the MGC.

The signaling transport between entities is applied to ensure that the signaling information is transported with the required functionality and performance. The SG/MG receives both the ISDN signaling and bearer channel data. The ISDN signaling is backhauled up to an MGC or Call Agent using the SIG protocol stack. Each SG can be configured to use up to three MGCs within an application server (AS) for redundancy. Multiple application servers can also be supported on an SG. MGCP is then used to control the bearer channels. Figure 2 shows the functional model for PRI signaling transport.

Figure 2 Signaling Transport Model



SCTP is a peer-to-peer protocol, while the IUA is a client-server protocol. Figure 3 shows the protocol flow from an ISDN endpoint, through the SG, and then to a Call Agent or MGC.

Figure 3 Protocol Flow

PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer on the Cisco 3660 supports the following:

- 20 calls per hour per DS-0 bearer circuit (3 minute average call duration)
- 460 calls per hour per PRI circuit (23 bearer channels): $20 \times 23 = 460$
- 5520 calls per hour per Cisco 3660 (12 PRI trunks): $460 \times 12 = 5520$
- 1.5333 calls per Cisco 3660 per second. 5520 divided by $(60 \times 60) = 1.5333$
- 7 signaling messages per call (both setup and tear down)
- 10.8 signaling messages per second per Cisco 3660: $7 \times 1.5333 = 10.8$

SCTP

Stream Control Transmission Protocol (SCTP) is the layer between the SCTP user application and an unreliable end-to-end datagram service such as IP. The basic service offered by SCTP is the reliable transfer of user datagrams between peer SCTP users. It performs this service within the context of an association between two SCTP hosts. SCTP is connection-oriented, but SCTP association is a broader concept than the Transmission Control Protocol (TCP) connection, for example.

SCTP provides the means for each SCTP endpoint to provide its peer with a list of transport addresses during association startup (address and UDP port combinations, for example) through which that endpoint can be reached and from which messages originate. The association spans transfer over all of the possible source and destination combinations that might be generated from the two endpoint lists (also known as multi-homing).

SCTP provides the following services and features:

- Acknowledged reliable non-duplicated transfer of user data.
- Application level segmentation to conform to the MTU size.
- Sequenced delivery of user datagrams within multiple streams.
- Optional multiplexing of user datagrams into SCTP datagrams.
- Enhanced reliability through support of multi-homing at either or both ends of the association.
- Congestion avoidance and resistance to flooding and masquerade attacks.

IUA

The IUA module creates the associations between the SG and MGC based on configuration requests. It also manages multiple application server processes as defined in the IETF IUA Specification. The IUA performs the following functions.

- Requests SCTP associations based on configuration information.
- Manages the destination address list, and requests a new primary destination in the event of a failure.
- Manages the application server process (ASP) state machine for each association.
- Manages the application server state machine across all ASPs associated with a single application.
- Provides service for multiple applications simultaneously to handle different Layer 3 signaling protocols (Q.931 and Q.SIG, for example), or to communicate with different sets of Call Agents.

Cisco AS5850 High Density PRI Business Trunking Gateway

This feature adds support for the Cisco AS5850 and adds the following:

- The Cisco AS5850 operates as a high density PRI Business Trunking Gateway.
- Multiple PRIs from terminals to a T1 M13 MUX and T3 from the M13 to the Cisco AS5850 CT3 card.
- All the individual T1 PRI D channels are backhauled to the IUA with SCTP supported session managers (SMs) using IUA backhaul. The rest of the B channels are defined as MGCP 1.0 endpoints under the Call Agent (CA).
- Outgoing PSTN voice calls travel through the PBX to the Cisco AS5850 and then to the terminating gateway on their way to customer telephone services.

Benefits

Third-Party Interoperability

This feature supports interoperability with third-party Call Agents.

Solutions Enabling

This feature supports the following solutions, which require signaling backhaul functionality:

- IP PBX
- IP Centrex
- Enterprise Toll Bypass
- IXC/Tandem Bypass

Restrictions

- This feature currently supports FAS and NFAS PRI D channel signaling only. No other signaling protocols are supported. NFAS with backup D channel signaling is not supported.
- Load balancing between ASPs on a per-call basis is not supported.
- This version supports two ASPs per application server and supports three explicit IP addresses per SCTP association endpoint.
- The IUA specification describes an optional feature known as New Traffic Failover. In this process, all the messages for calls pending completion during a failover are sent to the inactive MGC, and messages for new calls are sent to the newly active MGC. These IUA messages for new calls are not supported.

- Backhauling is not supported for Basic Rate Interface (BRI).

Related Documents

- Cisco 3600 Series Routers documentation index
- Cisco AS5300 documentation index
- ISDN Basic Rate Service Setup Commands
- Cisco IOS Release 12.2 master indexes
- Stream Control Transfer Protocol (SCTP), Release 2

Supported Platforms

- Cisco 3600 series
- Cisco AS5300
- Cisco AS5850

Table 1 Cisco IOS Release and Platform Support for this Feature

Platform	12.2(4)T	12.2(11)T	12.2(11)T1
Cisco 3600 series	X	X	X
Cisco AS5300	Not supported	X	X
Cisco AS5850	Not supported	Not supported	X

Determining Platform Support Through Cisco Feature Navigator

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

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

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

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

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

Availability of Cisco IOS Software Images

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

Supported Standards, MIBs, and RFCs

Standards

IUA draft, Version 4.

MIBs

There are no new or modified MIBs.

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

- RFC 2960 (SCTP)

Prerequisites

- You must be running Cisco IOS Release 12.2(4)T, Cisco IOS Release 12.2(11)T, or Cisco IOS Release 12.2(11)T1
- You must configure ISDN to backhaul Q.921 signaling to the MGC
- The Cisco AS5850 requires the following:
 - MGCP 1.0
 - IUA 0.4
 - ISDN network side support to terminate multiple voice PRIs

Configuration Tasks

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

- [Configuring IUA](#) (required)
- [Configuring ISDN Signaling Backhaul](#) (required)
- [Verifying Configuration](#)



Caution

When the Fast Ethernet interface is configured for auto negotiation, it can take up to two seconds to initialize. Two examples of the interface initializing is when the **no shut** command is entered, or if the cable is removed and then plugged back in. To avoid any problems, the Fast Ethernet interface should not be configured for auto negotiation. The duplex and speed parameters should be set according to the requirements of the network, and should not be set to auto.

Configuring IUA

To configure IUA, you must create the AS and the ASP. Each task in the list indicates if it is optional or required.

	Command	Purpose
Step 1	<code>Router(config)# iua</code>	(Required) The iua command specifies backhaul using SCTP and enters IUA configuration mode.
Step 2	<code>Router(config-<i>iua</i>)# as <i>as-name</i> {<i>localip</i>[<i>localip2</i>]} [<i>local-sctp-port</i>]</code>	<p>(Required) Defines an Application Server (AS). To disable, enter the no form of this command.</p> <p>The localip keyword specifies the local IP addresses for all the ASPs in this AS. The <i>local-sctp-port</i> parameter specifies the use of specific local SCTP port other than the IUA well-known port.</p> <p>Note This command defines an Application Server. A maximum of three local IP addresses can be specified (note that SCTP has built-in support for multi-homed machines). For the no form of the command, all the ASPs in this AS have to be removed first before the AS can be unconfigured.</p>

	Command	Purpose
Step 3	<pre>Router(config-iaua)# asp asp-name as as-name { remoteip [remoteip2] } [local-sctp-port]</pre>	<p>(Required) Defines an Application Server Process (ASP). To disable, use the no form of this command.</p> <p>The <i>asp-name</i> argument is the name for this ASP. The <i>as-name</i> argument is the name of the AS to which this ASP belongs.</p> <p>The remoteip keyword specifies the remote IP addresses for this SCTP association. The remote-sctp-port keyword specifies a connection to a specific remote SCTP port other than the IUA well-known port.</p> <p>Note This command establishes SCTP associations. There can be only a maximum of three ASPs configured per AS.</p>
Step 4	<pre>Router(config-iaua)# asp asp-name sctp keep-alive remote-ip-address</pre>	<p>(Optional) Specifies the IP address to enable and disable keep alives. Specifies the keep alive interval (in milliseconds) when an IP address has been selected. Controls SCTP keepalives on destination IP addresses. To disable, use the no form of this command. Keepalives are enabled by default.</p> <p>The <i>asp-name</i> argument specifies the name of the ASP. The <i>remote-ip-address</i> argument specifies the IP address of the remote end point (the address of MGC, for example).</p>
Step 5	<pre>Router(config-iaua)# asp asp-name ip-precedence remote-IPaddress number</pre>	<p>(Optional) Specifies the IP precedence level for protocol data units (PDUs). To disable, use the no form of this command.</p> <p>You can configure the precedence value in IUA in the range of 0 through 7 for a given IP address. Within IUA, the upper three bits representing the IP precedence in the ToS byte (used in the IP header) are set based on what you input before passing down the value to SCTP. In turn, SCTP passes the ToS byte value to IP. The default value is 0 for normal IP precedence handling.</p> <p>The <i>asp-name</i> argument specifies the name of this ASP. The ip-precedence keyword sets the precedence and ToS field. The <i>remote-ip_address</i> argument specifies the IP address of the remote end-point (the address of MGC, for example). The <i>number</i> argument can be any IP precedence bits in the range 0 through 7.</p> <p>Note The no form of the command results in precedence bits not being explicitly set by SCTP. The default is to set all bits in the ToS field to zero by SCTP.</p>

	Command	Purpose
Step 6	Router(config-iaa)# as <i>as-name</i> fail-over-timer <i>time</i>	<p>(Optional) Changes the failover timer value (1 to 10 seconds) in milliseconds. Valid ranges are from 1000-10000 msec. Default is 4000 msec. Find the failover timer value by examining the show iua as all command output.</p> <p>If the failover timer is not set, it assumes its default value of 4000 msec. Once you have set the failover timer to a value, you can return it to its default of 4000 msec by using the no form of this command.</p> <p>The <i>as-name</i> argument specifies the name of this AS. The <i>time</i> argument can be any value between 2000 and 10000 milliseconds. IUA waits for this amount of time for one ASP to take over from another ASP during failover.</p>
Step 7	Router(config-iaa)# exit	Exits IUA configuration mode.

Configuring ISDN Signaling Backhaul

Use the commands in this section to configure ISDN signaling backhaul.

	Command	Purpose
Step 1	Router(config)# controller t1 0 Router(config-control)#	(Required) Enters controller configuration mode.
Step 2	Router(config-control)# pri-group <i>timeslots</i> 1-24 service mgcp	<p>(Required) Specifies the control protocol used for backhaul (MGCP).</p> <p>The controller timeslots cannot be shared between backhaul and other Layer 3 protocols.</p>
Step 3	Router(config-control)# exit	(Required) Returns to configuration mode.
Step 4	Router(config)# interface serial 0:23 Router(config-if)#	(Required) Enters serial interface configuration mode.
Step 5	Router(config-if)# isdn <i>switch-type</i> primary-4ess	(Required) Configures the ISDN switch type. This can be done in either global configuration mode or interface mode.
Step 6	Router(config-if)# isdn <i>bind-13</i> IUA-backhaul as <i>as-name</i> Router(config-if)# exit	<p>(Required) Configures ISDN to backhaul Q.931 to the MGC.</p> <p>Repeat the steps above for each T1 interface on the Cisco 3660 that utilize backhaul.</p>

Verifying Configuration

Use the following **show** commands in privileged EXEC mode to verify your configuration.

	Command	Purpose
Step 1	Router# show iua as {all name as-name}	Displays the current state of the active AS and shows the PRI interfaces configured on the AS. If the all keyword is specified, information about all the configured AS are shown.
Step 2	Router# show iua asp {all name asp-name}	Displays the current state of the active ASP and shows information about the SCTP association being used by this ASP. If the all keyword is specified, information about all the configured ASPs are shown.
Step 3	Router# show isdn status	Displays status of ISDN backhaul. If the connection to the MGC is lost, the router shuts down Layer 2 so that it cannot receive more calls. When the MGC connection is back up, you can use this command to verify that Layer 2 was also brought back up correctly.

The following typical output for **show iua as all** shows that the current state of the AS (as1) is active and that there are four PRI interfaces configured to use this AS:

```
Router# show iua as all

Name of AS :as1
Total num of ASPs configured :2
Current state : ACTIVE
Active ASP :asp1
Number of ASPs up :1
Fail-Over time : 4000 milli seconds
Local address list : 10.21.0.2
Local port 9900
Interface IDs registered with this AS
      Interface ID      stream #
      256 (serial1/0:23)  1
      257 (serial1/1:23)  2
      512 (serial2/0:23)  3
      513 (serial2/1:23)  4
```

The following typical output for **show iua asp all** shows that the current state of the ASP (asp1) is active. This command also gives information about the SCTP association being used by this ASP.

```
Router# show iua asp all

Name of ASP :asp1
Current State of ASP:ASP-Active
Current state of underlying SCTP Association IUA_ASSOC_ESTAB , assoc id
0
SCTP Association information :
  Local Receive window :9000
  Remote Receive window :9000
  Primary Dest address requested by IUA 10.23.0.16
  Effective Primary Dest address 10.23.0.16
Remote address list : 10.23.0.16
Remote Port :9900
Statistics :
  Invalid SCTP signals Total :0 Since last 0
```

```
SCTP Send failures :0
```

```
Name of ASP :asp2
Current State of ASP:ASP-Down
Current state of underlying SCTP Association IUA_ASSOC_INIT , assoc id
0
Remote address list : 10.23.0.16
Remote Port :9911
Statistics :
    Invalid SCTP signals Total :0 Since last 0
    SCTP Send failures :0
```

The following is typical output for the **show isdn status** command. In this example, Layer 2 status is defined by the **MULTIPLE_FRAME_ESTABLISHED** message, which indicates that Layer2 is up. The L3 protocol and State status are highlighted:

```
Router# show isdn status
Global ISDN Switchtype = primary-5ess
ISDN Serial1/0:23 interface
    dsl 0, interface ISDN Switchtype = primary-5ess
    L2 Protocol = Q.921 L3 Protocol(s) = IUA BACKHAUL
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBS = 0
    The Free Channel Mask: 0x807FFFFFFF
ISDN Serial1/1:23 interface
    dsl 1, interface ISDN Switchtype = primary-5ess
    L2 Protocol = Q.921 L3 Protocol(s) = IUA BACKHAUL
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 1 CCBS = 0
    The Free Channel Mask: 0x807FFFFFFF
ISDN Serial2/0:23 interface
    dsl 2, interface ISDN Switchtype = primary-5ess
    L2 Protocol = Q.921 L3 Protocol(s) = IUA BACKHAUL
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 2 CCBS = 0
    The Free Channel Mask: 0x807FFFFFFF
ISDN Serial2/1:23 interface
    dsl 3, interface ISDN Switchtype = primary-5ess
    L2 Protocol = Q.921 L3 Protocol(s) = IUA BACKHAUL
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 3 CCBS = 0
    The Free Channel Mask: 0x807FFFFFFF
    Total Allocated ISDN CCBS = 0
```

Troubleshooting Tips

This section describes the debug commands available for SCTP. For more information, refer to the *Stream Control Transmission Protocol (SCTP), Release 2* feature.



Caution

Many SCTP **debug** commands should be used with extreme caution or not at all in live systems, depending on the amount of traffic, because the extra messages they generate may cause associations to fail. This caution is repeated in descriptions of the commands that may cause disruption to live systems.



Note

SCTP **debug** commands display information for all current SCTP associations and cannot be limited to particular associations.

Debugs are often used with time stamps enabled to see the relevant timing of the events indicated. Use the **service timestamps** commands to add time stamps to debug output in the format MMM DD HH:MM:SS, which indicates the date and time according to the system clock. If the system clock has not been set, the date and time are preceded by an asterisk (*) to indicate that the date and time are probably not correct. To activate millisecond time stamps for debugs, use the following commands in global configuration mode:

```
Router(config)# service timestamps debug datetime msec
Router(config)# service timestamps log datetime msec
```

For more information, see the **service timestamps** command reference entry in the “[Troubleshooting and Fault Management Commands](#)” chapter in the “[System Management Commands](#)” part of the *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2.

The following debug commands are available for SCTP:

- **debug ip sctp api**
- **debug ip sctp congestion**
- **debug ip sctp init**
- **debug ip sctp multihome**
- **debug ip sctp performance**
- **debug ip sctp rcvchunks**
- **debug ip sctp rto**
- **debug ip sctp segments**
- **debug ip sctp segmentv**
- **debug ip sctp signal**
- **debug ip sctp sndchunks**
- **debug ip sctp state**
- **debug ip sctp timer**
- **debug ip sctp warnings**

In a live system, the **debug** commands for performance, state, signal, and warnings are the most useful. These **debug** commands show any association or destination address failures and can be used to monitor the stability of any established associations.

**Note**

Debug commands other than those for performance, state, signal, and warnings can generate a great deal of output and therefore can cause associations to fail. These commands should be used only in test environments or when there are very low amounts of traffic.

Configuration Examples

The following section shows configuration examples for this feature:

- [AS and ASP Example Configuration](#)
- [Configuring ISDN Signaling Backhaul Example](#)

AS and ASP Example Configuration

The following is an example of an AS configuration on a gateway:

```
AS as-name 10.4.8.69 10.4.9.69 2577
```

In the configuration above, an AS named *as-name* is configured to use two local IP addresses and a port number of 2577. IP address values that are set apply to all IP addresses of the ASP.

An ASP can be viewed as a local representation of an SCTP association since it specifies a remote end point that will be in communication with an AS local end point. An ASP is defined for a given AS. For example, the following configuration defines a remote signaling controller *asp-name* at two IP addresses for AS *as-name*. The remote SCTP port number is 2577:

```
AS as-name 10.4.8.69 10.4.9.69 2477
```

```
ASP asp-name AS as-name 10.4.8.68 10.4.9.68 2577
```

Multiple ASPs can be defined for a single AS for the purpose of redundancy, but only one ASP can be active. The other ASP is inactive and only becomes active after fail-over.

In the Cisco MGC solution, a signaling controller is always the client that initiates the association with a gateway. During the initiation phase, you can request outbound and inbound stream numbers, but the gateway only allows a number that is at least one digit higher than the number of interfaces (T1/E1) allowed for the platform.

The number of streams to assign to a given association is implementation dependent. During the initialization of the IUA association, you need to specify the total number of streams that can be used. Each D channel is associated with a specific stream within the association. With multiple trunk group support, every interface can potentially be a separate D channel.

At start-up the IUA code checks for all the possible T1, E1, or T3 interfaces and sets the total number of inbound and outbound streams supported accordingly. In most cases, there is only a need for one association between the GW and the MGC. For the rare case that you are configuring multiple AS associations to various MGCs, the overhead from the unused streams would have minimal impact. The NFAS D channels are configured for one or more interfaces, where each interface is assigned a unique stream ID.

The total number of streams for the association needs to include an additional stream for the SCTP management messages. So during start-up the IUA code adds one to the total number of interfaces (streams) found.

You have the option to manually configure the number of streams per association. In the backhaul scenario, if the number of D channel links is limited to one, allowing the number of streams to be configurable avoids the unnecessary allocation of streams in an association that will never be used. For multiple associations between a GW and multiple MGCs, the configuration utility is useful in providing only the necessary number of streams per association. The overhead from the streams allocated but not used in the association is negligible.

If the number of streams is manually configured through the CLI, the IUA code cannot distinguish between a start-up event, which automatically sets the streams to the number of interfaces, or if the value is set manually during runtime. If you are configuring the number of SCTP streams manually, you must add one plus the number of interfaces using the **sctp-streams** keyword. Otherwise, IUA needs to always add one for the management stream, and the total number of streams increments by one after every reload.

When you set the SCTP stream with CLI, you cannot change the inbound and outbound stream support once the association is established with SCTP. The value takes effect when you first remove the IUA AS configuration and then configure it back as the same AS or a new one. The other option is to reload the router.

The following shows sample SCTP configuration options using using the help menu for the **as** and **asp** commands:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# iua
Router(config-iaa)# as as1 ?

  A.B.C.D          Specify (up to two) Local IP address
  Fail-Over-Timer  Configure the Fail-Over timer for this AS
  sctp-startup-rtx Configure the SCTP max startup retransmission timer
  sctp-streams     Configure the number of SCTP streams for this AS
  sctp-tlinit      Configure the SCTP T1 init timer

Router(config-iaa)# as as1 sctp-startup-rtx ?

  <2-20> Set SCTP Maximum Startup Retransmission Interval

Router(config-iaa)# as as1 sctp-streams ?

  <1-56> Specify number of SCTP streams for association

Router(config-iaa)# as as1 sctp-tlinit ?

  <1000-60000> Set SCTP T1 init timer (in milliseconds)

Router(config-iaa)# asp asp1 as as1 ?

  A.B.C.D Specify (up to two) IP addresses of the call-agent

Router(config-iaa)# asp asp1 ?

  AS              Specify which AS this ASP belongs to
  IP-Precedence   Set IP precedence bits for a IP address in this ASP
  sctp-keepalives Modify the keep-alive behaviour of an IP address in this
                  ASP
  sctp-max-assoc  Set SCTP max association retransmissions for this ASP
  sctp-path-retran Set SCTP path retransmissions for this ASP
  sctp-t3-timeout Set SCTP T3 retransmission timeout for this ASP

Router(config-iaa)# asp asp1 sctp-keep ?
```

```

A.B.C.D specify the IP address to enable/disable keep alives
Router(config-iaa)# asp asp1 sctp-keepalive 10.10.10.10 ?

<1000-60000> specify keep alive interval (in milliseconds)

Router(config-iaa)# asp asp1 sctp-max-assoc ?

A.B.C.D specify the IP address

Router(config-iaa)# asp asp1 sctp-max-assoc 10.10.10.10 ?

<2-20> specify maximum associations
default use default value of max associations for this address

Router(config-iaa)# asp asp1 sctp-path-retran ?

A.B.C.D specify the IP address

Router(config-iaa)# asp asp1 sctp-path-retran 10.10.10.10 ?

<2-10> specify maximum path retransmissions
default use default value of max path retrans for this address

Router(config-iaa)# asp asp1 sctp-t3-timeout ?

A.B.C.D specify the IP address

Router(config-iaa)# asp asp1 sctp-t3-timeout 10.10.10.10 ?

<300-60000> specify T3 retransmission timeout (in milliseconds)
default use default value of T3 for this address

```

The following example shows a running AS configuration with IUA configured with one AS (as1) and two ASPs (asp1 and asp2). Four T1s (T1 1/0, 1/1, 2/0, 2/1) are configured to use IUA backhaul.

```

Router# show run
Building configuration...

Current configuration :2868 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname iua_3660_b
!
logging rate-limit console 10 except errors
!
!
!
memory-size iomem 30
voice-card 1
!
voice-card 2
!
voice-card 3
!
voice-card 4
!
voice-card 5

```

```
!
voice-card 6
!
ip subnet-zero
!
!
no ip domain-lookup
!
no ip dhcp-client network-discovery
iua
  AS as1 10.21.0.2 9900
  ASP asp1 AS as1 10.23.0.16 9900
  ASP asp2 AS as1 10.23.0.16 9911
isdn switch-type primary-5ess
!
!
!
!
!
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
!
controller T1 1/0
  framing esf
  clock source line primary
  linecode b8zs
  pri-group timeslots 1-24 service mgcp
!
controller T1 1/1
  framing esf
  linecode b8zs
  pri-group timeslots 1-24 service mgcp
!
controller T1 2/0
  framing esf
  linecode b8zs
  pri-group timeslots 1-24 service mgcp
!
controller T1 2/1
  framing esf
  linecode b8zs
  pri-group timeslots 1-24 service mgcp
!
controller T1 3/0
  framing sf
  linecode ami
!
controller T1 3/1
  framing sf
  linecode ami
!
controller T1 4/0
  framing sf
  linecode ami
!
controller T1 4/1
  framing sf
  linecode ami
!
controller T1 5/0
  framing sf
  linecode ami
```

```

!
controller T1 5/1
  framing sf
  linecode ami
!
controller T1 6/0
  framing sf
  linecode ami
!
controller T1 6/1
  framing sf
  linecode ami
!
!
!
interface FastEthernet0/0
  ip address 10.21.0.3 255.255.0.0 secondary
  ip address 10.21.0.2 255.255.0.0
  speed 10
  half-duplex
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial1/0:23
  no ip address
  ip mroute-cache
  no logging event link-status
  isdn switch-type primary-5ess
  isdn incoming-voice voice
  isdn bind-13 iua-backhaul as1
  no cdp enable
!
interface Serial1/1:23
  no ip address
  ip mroute-cache
  no logging event link-status
  isdn switch-type primary-5ess
  isdn incoming-voice voice
  isdn guard-timer 3000
  isdn T203 10000
  isdn bind-13 iua-backhaul as1
  no cdp enable
!
interface Serial2/0:23
  no ip address
  ip mroute-cache
  no logging event link-status
  isdn switch-type primary-5ess
  isdn incoming-voice voice
  isdn guard-timer 3000
  isdn T203 10000
  isdn bind-13 iua-backhaul as1
  no cdp enable
!
interface Serial2/1:23
  no ip address
  ip mroute-cache
  no logging event link-status
  isdn switch-type primary-5ess
  isdn incoming-voice voice

```

```
isdn T203 10000
isdn bind-13 iua-backhaul as1
no cdp enable
!
ip classless
ip route 10.0.0.0 255.0.0.0 10.21.0.17
ip route 11.0.0.10 255.255.255.255 FastEthernet0/0
ip route 172.0.0.0 255.0.0.0 172.18.194.1
ip http server
!
!
!
!
snmp-server manager
!
call rsvp-sync
!
voice-port 1/0:23
!
voice-port 1/1:23
!
voice-port 2/0:23
!
voice-port 2/1:23
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
line con 0
  transport input none

line aux 0
line vty 0 4
  login
!
!
end
```

Configuring ISDN Signaling Backhaul Example

Enter the `show isdn status` command to verify successful ISDN configuration for backhaul. The following output shows that Layers 1, 2, 3 are enabled and active. Layer 3 shows the number of active ISDN calls.

In the example below, notice that the Layer 2 protocol is Q.921, and the Layer 3 protocol is BACKHAUL. This verifies that it is configured to backhaul ISDN. Also, if you are connected to a live line, you should see Layer 1 status is active, and layer 2 state is MULTIPLE_FRAME_ESTABLISHED. This means that the ISDN line is up and active.

```
Router# show isdn status
*00:03:34.423 UTC Sat Jan 1 2000
Global ISDN Switchtype = primary-net5
ISDN Serial1:23 interface
    dsl 0, interface ISDN Switchtype = primary-net5
```

```
L2 Protocol = Q.921 L3 Protocol(s) = BACKHAUL
Layer 1 Status:
  ACTIVE
Layer 2 Status:
  TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
Layer 3 Status:
  NLCB:callid=0x0, callref=0x0, state=31, ces=0 event=0x0
  NLCB:callid=0x0, callref=0x0, state=0, ces=1 event=0x0
  0 Active Layer 3 Call(s)
Activated dsl 0 CCBs = 0
Number of active calls = 0
Number of available B-channels = 23
Total Allocated ISDN CCBs = 0
Router#
```

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.

- [as](#)
- [asp](#)
- [clear ip sctp statistics](#)
- [debug iua as](#)
- [debug iua asp](#)
- [isdn bind-L3 iua-backhaul](#)
- [iua](#)
- [show ip sctp association list](#)
- [show ip sctp association statistics](#)
- [show ip sctp errors](#)
- [show ip sctp instances](#)
- [show ip sctp statistics](#)
- [show iua as](#)
- [show iua asp](#)

as

To define an application server for backhaul, use the **as** command in IUA configuration mode. To disable, use the **no** form of this command.



Note

All of the application server processes (ASPs) in an AS must be removed before an AS can be unconfigured.

```
as as-name {localip1 [localip2]} [local-sctp-port]
```

```
no as name
```

Syntax Description

<i>as-name</i>	Defines the protocol name (only ISDN is supported).
<i>localip1</i>	Defines the local IP address(es) for all the ASPs in a particular AS.
<i>localip2</i>	(Optional) Defines the local IP address(es) for all the ASPs in a particular AS.
local-sctp-port	(Optional) Defines a specific local Simple Control Transmission Protocol (SCTP) port rather than an ISDN Q.921 User Adaptation Layer (IUA) well-known port.

Defaults

No default behavior or values.

Command Modes

IUA configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300.
12.2(11)T1	Support was added on the Cisco AS5850.

Usage Guidelines

A maximum of two local IP addresses can be specified. (Note that SCTP has built-in support for multihomed machines.)

Examples

The following output shows that the AS (as1) is defined for backhaul:

```
AS as1 10.21.0.2 9900
```

Related Commands

Command	Description
asp	Defines an ASP for backhaul.

asp

To define an application server process (ASP) for backhaul, use the **asp** command in IUA configuration mode. To disable, use the **no** form of this command.



Note

All of the ASPs in an application server (AS) must be removed before an application server can be unconfigured.

```
asp asp-name as as-name [remoteip1 [remoteip2]] [remote-sctp-port] [ip-precedence
sctp-keepalives] [sctp-max-associations] [sctp-path-retransmissions] [sctp-t3-timeout]
```

```
no asp asp-name
```

Syntax Description

<i>asp-name</i>	Names the current ASP.
as	The application server to which the ASP belongs.
<i>as-name</i>	Name of the application server to which the ASP belongs.
<i>remoteip1</i>	Designates the remote IP address for this Simple Control Transmission Protocol (SCTP) association.
<i>remoteip2</i>	Designates the remote IP address for this SCTP association.
remote-sctp-port	Connects to a remote SCTP port rather than the IUA well-known port.
ip-precedence	(Optional) Sets IP Precedence bits for protocol data units (PDUs). <ul style="list-style-type: none"> IP precedence is expressed in the type of service (ToS) field of the show ip sctp association parameters output. The default type of service (ToS) value is 0. Valid precedence values range from 0 to 7. You can also use the default IP precedence value for this address by choosing the default option.
sctp-keepalives	(Optional) Modifies the keepalive behavior of an IP address in a particular ASP. <ul style="list-style-type: none"> Valid keepalive interval values range from 1000 to 60000. The default value is 500 ms (see the show ip sctp association parameters output under heartbeats).
sctp-max-associations	(Optional) Sets the SCTP maximum association retransmissions for a particular ASP. Valid values range from 2 to 20. The default is 3.
sctp-path-retransmissions	(Optional) Sets the SCTP path retransmissions for a particular ASP. Valid values range from 2 to 10. The default is 10.
sctp-t3-timeout	(Optional) Sets the SCTP T3 retransmission timeout for a particular ASP. The default value is 900 ms. Valid timeout values range from 300 to 60000. Default is 60000.

Defaults

No default behavior or values.

Command Modes

IUA configuration

Command History	Release	Modification
	12.2(4)T	This command was introduced.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and support was added for the Cisco AS5300.
	12.2(11)T	This command was implemented on the Cisco AS5300.
	12.2(11)T1	This command was implemented on the Cisco AS5850.

Usage Guidelines This command establishes SCTP associations. There can be only a maximum of three ASPs configured per AS.

Examples An ASP can be viewed as a local representation of an SCTP association because it specifies a remote endpoint that will be in communication with an AS local endpoint. An ASP is defined for a given AS. For example, the following configuration defines a remote signaling controller *asp-name* at two IP addresses for AS *as1*. The remote SCTP port number is 2577:

```
as as1 10.4.8.69, 10.4.9.69 2477
asp asp1 as as1 10.4.8.68 10.4.9.68 2577
```

Multiple ASPs can be defined for a single AS for the purpose of redundancy, but only one ASP can be active. The ASPs are inactive and only become active after fail-over.

Related Commands	Command	Description
	as	Defines an application server for backhaul.

clear ip sctp statistics

To clear statistics counts for SCTP, enter the **clear ip sctp statistics** command in privileged EXEC mode.

clear ip sctp statistics

Syntax Description There are no arguments or keywords for this command.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300.
	12.2(11)T1	Supported was added for the Cisco AS5850.

Usage Guidelines This command clears both individual and overall statistics.

Examples The following command shows how to empty the buffer that holds SCTP statistics. No output is generated from this command.

```
Router# clear ip sctp statistics
```

Related Commands	Command	Description
	show ip sctp association list	Shows a list of all current SCTP associations.
	show ip sctp association parameters	Shows the parameters configured for the association defined by the association ID.
	show ip sctp association statistics	Shows the current statistics for the association defined by the association ID.
	show ip sctp errors	Shows error counts logged by SCTP.
	show ip sctp instances	Shows all currently defined SCTP instances.
	show ip sctp statistics	Shows overall statistics counts for SCTP.
	show iua as	Shows information about the current condition of an AS.
	show iua asp	Shows information about the current condition of an ASP.

debug iua as

To display debug messages for the IUA AS, use the **debug iua as** command in privileged EXEC mode. To disable, use the **no** form of this command.

```
debug iua as {user | state} {all | name as-name}
```

```
no debug iua as
```

Syntax Description	Parameter	Description
	user	Displays information about the usage of APIs and events between the ISDN layer and IUA.
	state	Displays information about AS state transitions.
	all	Enables debug for all the configured Application Servers.
	name <i>as-name</i>	Defines the name of the AS.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300.
	12.2(11)T1	Supported was added for the Cisco AS5850.

Examples The following example shows debug output when an ISDN backhaul connection is initially established:

```
Router# debug iua as state all
IUA :state debug turned ON for ALL AS

00:11:52:IUA:AS as1 number of ASPs up is 1
00:11:57:IUA:AS as1 xsition AS-Up --> AS-Active, cause - ASP aspl
```

Related Commands	Command	Description
	debug iua asp	Displays debug messages for the IUA ASP

debug iua asp

To display debug messages for the IUA ASP, use the **debug iua asp** command in privileged EXEC mode. To disable, use the **no** form of this command.

debug iua asp {**pak** | **peer-msg** | **sctp-sig** | **state**} {**all** | **name** *asp-name*}

no debug iua as

Syntax Description

pak	Displays information about ALL packets.
peer-msg	Displays information about IUA peer-to-peer messages.
sctp-sig	Displays information about the signals being sent by the SCTP layer.
state	Displays information about ASP state transition.
all	Enables debug for all configured ASPs.
name <i>asp-name</i>	Defines the name of the ASP.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300.
12.2(11)T1	Supported was added for the Cisco AS5850.

Examples

The following example shows debug output when an ISDN backhaul connection is initially established.

```
Router# debug iua asp peer-msg all
IUA :peer message debug turned ON for ALL ASPs

Router#
00:04:58:IUA :recieved ASP_UP message on ASP asp1
00:04:58:IUA:ASP asp1 xsition ASP-Down --> ASP-Up , cause - rcv peer
msg
ASP-UP
00:04:58:IUA:sending ACK of type 0x304 to asp asp1
00:05:03:IUA:rcv ASP_ACTIVE message for ASP asp1
00:05:03:IUA:ASP asp1 xsition ASP-Up --> ASP-Active, cause - rcv peer
msg
ASP-Active
```

Related Commands

Command	Description
debug iua as	Displays debug messages for the IUA AS.

isdn bind-L3 iua-backhaul

To specify ISDN backhaul using Stream Control Transmission Protocol (SCTP) for an interface, use the **isdn bind-L3 iua-backhaul** command in interface configuration mode. To disable the backhaul capability, use the **no** form of this command.

isdn bind-L3 iua-backhaul [*application-server-name*]

no isdn bind-L3 iua-backhaul



Note

In the command documentation, the capital “L” is used for clarity. You can enter a lowercase “l”.

Syntax Description

application-server-name (Optional) Name of the application server (AS) to use for backhauling the interface.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300.
12.2(11)T1	Supported was added for the Cisco AS5850.

Examples

The following example shows IUA backhaul on the application server “as1”:

```
interface Serial1/0:23
  no ip address
  ip mroute-cache
  no logging event link-status
  isdn switch-type primary-5ess
  isdn incoming-voice voice
  isdn bind-L3 iua-backhaul as1
```

Related Commands

Command	Description
as	Defines an AS for backhaul.
asp	Defines an ASP for backhaul.

iua

To specify backhaul using Stream Control Transmission Protocol (SCTP) and to enter ISDN User Adaptation Layer (IUA) configuration mode, use the **iua** command in terminal configuration mode.

iua

Syntax Description There are no arguments or keywords for this command.

Defaults No default behavior or values.

Command Modes Terminal configuration

Command History	Release	Modification
	12.2(4)T	This command was introduced.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300.
	12.2(11)T1	Supported was added for the Cisco AS5850.

Usage Guidelines You must first enter IUA configuration mode to access SCTP configuration mode. First enter IUA configuration mode by using the example below and then enter **sctp** at the Router(config-iua)#prompt to bring up SCTP configuration mode. See the **sctp** command.

Examples The following example shows how to enter iua configuration mode:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# iua
Router(config-iua)#
```

Related Commands	Command	Description
	isdn bind-L3 iua-backhaul	Specifies ISDN backhaul using SCTP for an interface.
	show iua as	Shows information about the current condition of an AS.
	show iua asp	Shows information about the current condition of an ASP.

show ip sctp association list

To display identifiers and information for current Stream Control Transmission Protocol (SCTP) associations and instances, use the **sctp-association list** command in privileged EXEC mode.

show sctp-association list

Syntax Description There are no arguments or keywords for this command.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(2)MB	This command was introduced as part of the show ip sctp command.
	12.2(2)T	This command was introduced as the show ip sctp association list command.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(8)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300 is not included in this release.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300.
	12.2(11)T1	Supported was added for the Cisco AS5850.

Usage Guidelines Use this command to display the current SCTP association and instance identifiers, the current state of SCTP associations, and the local and remote port numbers and addresses that are used in the associations.

Examples The following is sample output from this command for three association identifiers:

```

*** Sctp Association List ***

AssocID:0, Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8989, Addrs:10.6.0.4 10.5.0.4

AssocID:1, Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8990, Addrs:10.6.0.4 10.5.0.4

AssocID:2, Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8991, Addrs:10.6.0.4 10.5.0.4

```

Table 2 describes significant fields in this output.

Table 2 *show ip sctp association list Field Descriptions*

Field	Description
Assoc ID	SCTP association identifier.
Instance ID	SCTP association instance identifier.
Current State	SCTP association state, which can be ESTABLISHED, CLOSED, COOKIE-WAIT, and COOKIE-ECHOED.
Local Port, Addr	Port and IP address for the local SCTP endpoint.
Remote Port, Addr	Port and IP address for the remote SCTP endpoint.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
show ip sctp association parameters	Shows the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Shows the current statistics for the association defined by the association ID.
show ip sctp errors	Shows error counts logged by SCTP.
show ip sctp instances	Shows the currently defined SCTP instances.
show ip sctp statistics	Shows the overall statistics counts for SCTP.
show iua as	Shows information about the current condition of an AS.
show iua asp	Shows information about the current condition of an ASP.

show ip sctp association parameters

To display configured and calculated parameters for the specified Stream Control Transmission Protocol (SCTP) association, use the **show ip sctp association parameters** command in privileged EXEC mode.

show ip sctp association parameters [*assoc-id*]

Syntax Description	<i>assoc-id</i>	(Optional) Association identifier. Shows the associated ID statistics for the SCTP association.
---------------------------	-----------------	---

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(2)MB	This command was introduced as part of the show ip sctp command.
	12.2(2)T	This command was introduced as the show ip sctp association parameters command.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(8)T	Three new output fields were added to this command: Outstanding bytes, per destination address; Round trip time (RTT), per destination address; and Smoothed round trip time (SRTT), per destination address.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300.
	12.2(11)T1	Supported was added for the Cisco AS5850.

Usage Guidelines The **show ip sctp association parameters** command displays parameter values for the specified association. It requires an association identifier as an argument. Association identifiers can be obtained from the output of the **show ip sctp association list** command.

This command provides information to determine the stability of SCTP associations, dynamically calculated statistics about destinations, and values to assess network congestion.

There are many parameters that are defined for each association. Some are configured parameters, and others are calculated. There are three main groupings of parameters displayed by this command:

- Association configuration parameters
- Destination address parameters
- Association boundary parameters

The association configuration section displays information similar to that in the **show ip sctp association list** command, including association identifiers, state, and local and remote port and address information. The current primary destination is also displayed.

The destination address parameters section displays information associated with each destination address. Many of the address parameters are dynamically calculated and therefore give an indication of the state of the network for each destination. The state of the destination address is either ACTIVE or FAILED, depending on whether this destination address is currently accessible. The heartbeats and timeout are configured values (configured by the application using SCTP), as is the TOS (type of service,

or IP precedence) value. The TOS value shows the bits that are used in the IP header of each datagram sent out. The maximum transmission unit (MTU) field shows the currently configured MTU value from the corresponding interface that is used to reach the destination address. The values for congestion window (cwnd), slow-start threshold (ssthresh), and retransmission timeout (RTO) are calculated values, continually updated based on feedback from the network, as specified in RFC2960. The cwnd parameter indicates how much data can be outstanding in the network for that particular destination. The RTO parameter is the retransmit timeout value. Finally, the num retrans and num times failed parameters give the current number for how many times data has been retransmitted to that address and how many times the address has been marked as failed, respectively. These parameters give an indication of how steady that particular address is and has been.

The third group of parameters are boundary parameters that usually don't change over the life of an association, although the calling application can change some of them if it wants. The verification tags (vertags) are chosen during association initialization and don't change. The number of inbound and outbound streams also don't change. The max retrans numbers show the maximum number of times chunks are retransmitted. The association retransmit limit is the number of times any particular chunk are retransmitted before a declaration is made that the association failed. The declaration indicates that the chunk could not be delivered on any address. Init retrans is the number of times the chunks for initialization are retransmitted before a declaration that the attempt to establish the association failed. And the path retrans value is the maximum number of times that chunks are transmitted to any particular destination address before that address is declared failed. The cumulative SACK (cumsack) timeout specifies the maximum time that a SACK is delayed while waiting to bundle with data chunks. The bundle timeout value is the maximum time that data chunks are delayed during attempts to bundle with other data chunks. And finally, the min and max RTO values define the minimum and maximum retransmit timeout values that are allowed for the association.

Examples

The following example shows the IP SCTP association ID parameters:

```
Router# show ip sctp association parameters 0

*** SCTP Association Parameters ***

AssocID: 0 Context: 0 InstanceID: 1
Assoc state: ESTABLISHED Uptime: 19:05:57.425
Local port: 8181
Local addresses: 10.1.0.3 10.2.0.3

Remote port: 8181
Primary dest addr: 10.5.0.4
Effective primary dest addr: 10.5.0.4
Destination addresses:

10.5.0.4: State: ACTIVE
Heartbeats: Enabled Timeout: 30000 ms
RTO/RTT/SRTT: 1000/16/38 ms TOS: 0 MTU: 1500
cwnd: 5364 ssthresh: 3000 outstand: 768
Num retrans: 0 Max retrans: 5 Num times failed: 0

10.6.0.4: State: ACTIVE
Heartbeats: Enabled Timeout: 30000 ms
RTO/RTT/SRTT: 1000/4/7 ms TOS: 0 MTU: 1500
cwnd: 3960 ssthresh: 3000 outstand: 0
Num retrans: 0 Max retrans: 5 Num times failed: 0

Local vertag: 9A245CD4 Remote vertag: 2A08D122
Num inbound streams: 10 outbound streams: 10
Max assoc retrans: 5 Max init retrans: 8
CumSack timeout: 200 ms Bundle timeout: 100 ms
```

```

Min RTO: 1000 ms  Max RTO: 60000 ms
LocalRwnd: 18000  Low: 13455  RemoteRwnd: 15252  Low: 13161
Congest levels: 0  current level: 0  high mark: 325

```

Table 3 describes significant fields in this output.

Table 3 *show ip sctp association parameters Field Descriptions*

Field	Description
AssocID	SCTP association identifier.
Context	Internal upper-layer handle.
InstanceID	SCTP association instance identifier.
Assoc state	SCTP association state, which can be ESTABLISHED, CLOSED, COOKIE-WAIT, and COOKIE-ECHOED.
Uptime	Duration of time for which the association has been active.
Local port	Port number for the local SCTP endpoint.
Local addresses	IP addresses for the local SCTP endpoint.
Remote port	Port number for the remote SCTP endpoint.
Primary dest addr	Primary destination address.
Effective primary dest addr	Current primary destination address.
Heartbeats	Status of heartbeats.
Timeout	Heartbeat timeout.
RTO/RTT/SRTT	Retransmission timeout, round trip time, and smoothed round trip time, calculated from network feedback.
TOS	IP precedence setting.
MTU	Maximum transmission unit size, in bytes, that a particular interface can handle.
cwnd	Congestion window value calculated from network feedback. The amount of data that can be outstanding in the network for that particular destination.
ssthresh	Slow-start threshold value calculated from network feedback.
outstand	Number of outstanding bytes.
Num retrans	Current number of times that data has been retransmitted to that address.
Max retrans	Maximum number of times that data has been retransmitted to that address.
Num times failed	Number of times that the address has been marked as failed.
Local vertag, Remote vertag	Verification tags (vertags). Tags are chosen during association initialization and do not change.
Num inbound streams, Num outbound streams	Maximum inbound and outbound streams. This number does not change.
Max assoc retrans	Maximum association retransmit limit. Number of times that any particular chunk may be retransmitted before a declaration that the association failed, which indicates that the chunk could not be delivered on any address.
Max init retrans	Maximum initial retransmit limit. Number of times that the chunks for initialization may be retransmitted before declaring that the attempt to establish the association failed.

■ show ip sctp association parameters

Table 3 *show ip sctp association parameters Field Descriptions (continued)*

Field	Description
CumSack timeout	Cumulative selective acknowledge (SACK) timeout. The maximum time that a SACK may be delayed while attempting to bundle together with data chunks.
Bundle timeout	Maximum time that data chunks may be delayed while attempting to bundle with other data chunks.
Min RTO, Max RTO	Minimum and maximum retransmit timeout values allowed for the association.
LocalRwnd, RemoteRwnd	Local and remote receive windows.
Congest levels: current level, high mark	Current congestion level and highest number of packets queued.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
show ip sctp association list	Shows a list of all current SCTP associations.
show ip sctp association parameters	Shows the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Shows the current statistics for the association defined by the association ID.
show ip sctp errors	Shows error counts logged by SCTP.
show ip sctp instances	Shows all currently defined SCTP instances.
show ip sctp statistics	Shows overall statistics counts for SCTP.
show iua as	Shows information about the current condition of an AS.
show iua asp	Shows information about the current condition of an ASP.

show ip sctp association statistics

To display statistics that have accumulated for the specified Stream Control Transmission Protocol (SCTP) association, enter the **show ip sctp association statistics** privileged EXEC command.

show ip sctp association statistics *associd*

Syntax Description	<i>associd</i>	(Optional) Association identifier. Shows the associated ID statistics for the SCTP association.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.2(2)MB	This command was introduced as part of the show ip sctp command.
	12.2(2)T	This command was introduced as the show ip sctp association statistics command.
	12.2(4)T	This command was introduced.
	12.2(8)T	Two new output fields were added to this command: Number of unordered data chunks sent and Number of unordered data chunks received.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300.
	12.2(11)T1	Supported was added for the Cisco AS5850.

Usage Guidelines The **show ip sctp association statistics** command requires an association identifier argument. The association identifier can be obtained from the output of the **show ip sctp association list** command. This command shows only the information that has become available since the last time a **clear ip sctp statistics** command was input.

This command displays various statistics about the specified association. The first numbers show the total number of chunks, both data and control, sent and received. The second group of numbers focuses on just the data chunks, showing the following statistics:

- number of data chunks received in and out of sequence
- total number of data chunks sent and received
- number of bytes sent and received in those data chunks
- number of data chunks discarded or retransmitted.

The average chunks bundled shows how many chunks have been bundled together in each datagram on average. The last section indicates how many datagrams have been sent, have been received, and are ready to be received by the calling application or Upper Layer Process (ULP). The ULP statistics may be different from the chunk statistics if the datagrams are large and have been segmented by SCTP.

The second group of statistics focuses on the data chunks sent, showing the total number sent, the number retransmitted, the number that were ordered and unordered, the average number that were bundled together, and the total bytes sent. The third group of statistics focuses on the data chunks received. It displays the total number received and the number discarded (due to duplicates), the number of ordered and unordered chunks received, the average number of chunks that were bundled, the number of bytes received, and the number of sequenced chunks that were received out of order. The last section indicates how many datagrams have been sent, received, or are ready to be received by the calling application or ULP. The ULP statistics may be different from the chunk statistics if the datagrams are large and have been segmented by SCTP.

Examples

The following example was taken from a network with known dropped packets in one direction. The number of total chunks sent and received is larger than the number of data chunks sent and received because it also includes the control chunks sent. The number of chunks received out of sequence and the number of chunks discarded indicate that there are problems in the network. Some chunks are being dropped and multiple copies of others are being received. However, no chunks have been retransmitted, indicating that traffic in that direction is running much more cleanly. If the network is completely clean, you see zero chunks received out of sequence and zero chunks discarded or retransmitted.

```
Router# show ip sctp association statistics 0

*** SCTP Association Statistics ***

AssocID/InstanceID:          0/0
Current State:                ESTABLISHED
Chunks Sent:                  74596995
Chunks Rcvd:                  74049518

Data Chunks Rcvd In Seq:      61627732
Data Chunks Rcvd Out of Seq: 8555308
Data Chunks Sent:             70183891
Data Chunks Rcvd:             70200197
Data Bytes Sent:              2723421804
Data Bytes Rcvd:              2725052404
Data Chunks Discarded:        17157
Data Chunks Retrans:          0
Average chunks bundled:       10

ULP Dgrams Sent:              70183040
ULP Dgrams Ready:             70183040
ULP Dgrams Rcvd:              70183040
```

Table 4 describes significant fields in this output.

Table 4 *show ip sctp association statistics Field Descriptions*

Field	Description
AssocID/InstanceID	SCTP association identifier and instance identifier.
Current State	State of SCTP association.
Control Chunks	SCTP control chunks sent and received.
Data Chunks Sent	SCTP data chunks sent, ordered and unordered.
Data Chunks Rcvd	SCTP data chunks received, ordered and unordered.
ULP Dgrams	Number of datagrams sent, ready, and received by the Upper-Layer Protocol (ULP).

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
show ip sctp association list	Shows a list of all current SCTP associations.
show ip sctp association parameters	Shows the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Shows the current statistics for the association defined by the association ID.
show ip sctp errors	Shows error counts logged by SCTP.
show ip sctp instances	Shows all currently defined SCTP instances.
show ip sctp statistics	Shows overall statistics counts for SCTP.
show iua as	Shows information about the current condition of an AS.
show iua asp	Shows information about the current condition of an ASP.

show ip sctp errors

To show the error counts logged by SCTP, enter the **show ip sctp errors** privileged EXEC command.

show ip sctp errors

Syntax Description There are no arguments or keywords with this command.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(2)MB	This command was introduced as part of the show ip sctp command.
	12.2(2)T	This command was introduced as the show ip sctp errors command.
	12.2(4)T	This command was introduced.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300.
	12.2(11)T1	Support was added for the Cisco AS5850.

Usage Guidelines This command displays all errors across all associations that have been logged since the last time that the SCTP statistics were cleared with the **clear ip sctp statistics** command. If no errors have been logged, this is indicated in the output.

Examples The following output shows one example in which no errors have been logged, and another in which there have been several different types of errors.

```
Router# show ip sctp errors

*** SCTP Error Statistics ****

No SCTP errors logged.

Router# show ip sctp errors

*** SCTP Error Statistics ****

Communication Lost:           95
Unknown INIT params rcvd:    8
Missing parameters:          18
```

Related Commands	Command	Description
	clear ip sctp statistics	Clears statistics counts for SCTP.
	show ip sctp association list	Shows a list of all current SCTP associations.
	show ip sctp association parameters	Shows the parameters configured for the association defined by the association ID.
	show ip sctp association statistics	Shows the current statistics for the association defined by the association ID.
	show ip sctp instances	Shows the currently defined SCTP instances.
	show ip sctp statistics	Shows the overall statistics counts for SCTP.
	show iua as	Shows information about the current condition of an AS.
	show iua asp	Shows information about the current condition of an ASP.

show ip sctp instances

To display information for each of the currently configured Stream Control Transmission Protocol (SCTP) instances, enter the **show ip sctp instances** privileged EXEC command.

show ip sctp instances

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(2)MB	This command was introduced as part of the show ip sctp command.
	12.2(2)T	This command was introduced as the show ip sctp instances command.
	12.2(4)T	This command was introduced.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
	12.2(11)T	This command was implemented on the Cisco AS5300 .
	12.2(11)T1	Supported was added for the Cisco AS5850.

Usage Guidelines The **show ip sctp instances** command displays information for each of the currently configured instances. The instance number, local port, and address information is displayed. The instance state is either *available* or *deletion pending*. An instance enters the deletion pending state when a request is made to delete it but there are currently established associations for that instance. The instance cannot be deleted immediately and instead enters the pending state. No new associations are allowed in this instance, and when the last association is terminated or fails, the instance is deleted.

The default inbound and outbound stream numbers are used for establishing incoming associations, and the maximum number of associations allowed for this instance is shown. Finally, a snapshot of each existing association is shown, if any exist.

Examples The following example shows available IP SCTP instances. In this example, two current instances are active and available. The first is using local port 8989, and the second is using 9191. Instance identifier 0 has three current associations, and instance identifier 1 has no current associations.

```
Router# show ip sctp instances

*** SCTP Instances ***

Instance ID:0 Local port:8989
Instance state:available
Local addrs:10.1.0.2 10.2.0.2
Default streams inbound:1 outbound:1
Current associations: (max allowed:6)
AssocID:0 State:ESTABLISHED Remote port:8989
```

```

    Dest addr:10.6.0.4 10.5.0.4
    AssocID:1 State:ESTABLISHED Remote port:8990
    Dest addr:10.6.0.4 10.5.0.4
    AssocID:2 State:ESTABLISHED Remote port:8991
    Dest addr:10.6.0.4 10.5.0.4

Instance ID:1 Local port:9191
Instance state:available
Local addr:10.1.0.2 10.2.0.2
Default streams inbound:1 outbound:1

No current associations established for this instance.
Max allowed:6

```

Related Commands-

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
show ip sctp association list	Shows a list of all current SCTP associations.
show ip sctp association parameters	Shows the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Shows the current statistics for the association defined by the association ID.
show ip sctp errors	Shows error counts logged by SCTP.
show ip sctp statistics	Shows the overall statistics counts for SCTP.
show iua as	Shows information about the current condition of an AS.
show iua asp	Shows information about the current condition of an ASP.

show ip sctp statistics

To display the overall statistics counts for Stream Control Transmission Protocol (SCTP) activity, enter the **show ip sctp statistics** privileged EXEC command.

show ip sctp statistics

Syntax Description There are no arguments or keywords with this command.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(2)MB	This command was introduced as part of the show ip sctp command.
	12.2(2)T	This command was introduced as the show ip sctp statistics command.
	12.2(4)T	This command was introduced.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
	12.2(11)T	This command was implemented on the Cisco AS5300.
	12.2(11)T1	Supported was added for the Cisco AS5850.

Usage Guidelines This command displays the overall SCTP statistics accumulated since the last **clear ip sctp statistics** command. It includes numbers for all currently established associations, as well as for any that have been terminated. The statistics indicated are similar to those shown for individual associations.

Examples The following example shows IP SCTP statistics and are similar to those shown for individual associations:

```
Router# show ip sctp statistics

*** SCTP Overall Statistics ***

Total Chunks Sent:          2097
Total Chunks Rcvd:         2766

Data Chunks Rcvd In Seq:   538
Data Chunks Rcvd Out of Seq: 0
Total Data Chunks Sent:    538
Total Data Chunks Rcvd:    538
Total Data Bytes Sent:     53800
Total Data Bytes Rcvd:     53800
Total Data Chunks Discarded: 0
Total Data Chunks Retrans: 0

Total SCTP Dgrams Sent:    1561
Total SCTP Dgrams Rcvd:    2228
Total ULP Dgrams Sent:     538
```

```
Total ULP Dgrams Ready:    538
Total ULP Dgrams Rcvd:    538:
```

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
show ip sctp association list	Shows a list of all current SCTP associations.
show ip sctp association parameters	Shows the parameters configured for the association defined by the association ID.
show ip sctp errors	Shows error counts logged by SCTP.
show ip sctp instances	Shows all currently defined SCTP instances.
show iua as	Shows information about the current condition of an AS.
show iua asp	Shows information about the current condition of an ASP.

show iua as

To show information about the current condition of an application server (AS), use the **show iua as** command in privileged EXEC mode.

```
show iua as {all | name as-name}
```

Syntax Description	all	Output displays information about all configured ASs.
	name <i>as-name</i>	Name of a particular AS. Output displays information about just that AS.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(4)T	This command was introduced.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
	12.2(11)T	This command was implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines	Use the show iua as all command to find the failover timer value. You will need to know the failover timer value currently set before you use the as <i>as-name</i> fail-over-timer command to set the failover timer value to fit your application.
------------------	--

Examples	The following typical output for show iua as all shows that the current state of the AS (as1) is active and that there are four PRI interfaces configured to use this AS:
----------	--

```
Router# show iua as all

Name of AS :as1
  Total num of ASPs configured :2
  Current state : ACTIVE
  Active ASP :asp1
  Number of ASPs up :1
  Fail-Over time : 4000 milli seconds
  Local address list : 10.21.0.2
  Local port 9900
  Interface IDs registerd with this AS
    Interface ID      stream #
    256 (serial1/0:23) 1
    257 (serial1/1:23) 2
    512 (serial2/0:23) 3
    513 (serial2/1:23) 4
```

[Table 5](#) shows important fields in the output.

Table 5 *show iua as all Field Descriptions*

Field	Description
Name of AS: 1	Name of the AS.
Total num of ASPs configured :2 asp1 asp2	Total number of application server processes (ASPs) configured.
Current state : ACTIVE	The possible states are ACTIVE, INACTIVE, and DOWN.
Active ASP :asp1	Shows the active ASP.
Number of ASPs up :1	If two ASPs are up, then the one that is not active is in standby mode.
Fail-Over time : 4000 milliseconds	Default is 4000 milliseconds, though the value can also be configured through the CLI under AS.
Local address list : 10.1.2.345 10.2.3.456	Configured by the user.
Local port:2139	Configured by the user.
Interface IDs registered with this AS Interface id 0 (Dchannel0) 3 (Dchannel3) 2 (Dchannel2) 1 (Dchannel1)	The D channels that are bound to this AS.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
show ip sctp association list	Shows a list of all current SCTP associations.
show ip sctp association parameters	Shows the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Shows the current statistics for the association defined by the association ID.
show ip sctp errors	Shows error counts logged by SCTP.
show ip sctp instances	Shows the currently defined SCTP instances.
show ip sctp statistics	Shows the overall statistics counts for SCTP.
show iua asp	Shows information about the current condition of an ASP.

show iua asp

To provide information about the current condition of an application server process (ASP), use the **show iua asp** privileged EXEC command.

```
show iua asp { all | name name asp-name }
```

Syntax Description	all	Output displays information about all configured ASPs.
	name <i>asp-name</i>	Name of a particular ASP. Output displays information about just that ASP.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)T	This command was introduced.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
	12.2(11)T	This command was implemented on the Cisco AS5300.
	12.2(11)T1	Supported was added for the Cisco AS5850.

Usage Guidelines This command establishes Stream Control Transmission Protocol (SCTP) associations. There can only be a maximum of two ASPs configured per application server (AS).

Examples The following typical output for **show iua asp all** shows that the current state of the ASP (asp1) is active. This command also gives information about the SCTP association being used by this ASP.

```
Router# show iua asp all

Name of ASP :asp1
Current State of ASP:ASP-Active
Current state of underlying SCTP Association IUA_ASSOC_ESTAB , assoc id
0
SCTP Association information :
    Local Recieve window :9000
    Remote Recieve window :9000
    Primary Dest address requested by IUA 10.23.0.16
    Effective Primary Dest address 10.23.0.16
Remote address list : 10.23.0.16
Remote Port :9900
Statistics :
    Invalid SCTP signals Total :0 Since last 0
    SCTP Send failures :0

Name of ASP :asp2
Current State of ASP:ASP-Down
Current state of underlying SCTP Assocaition IUA_ASSOC_INIT , assoc id
0
```

```

Remote address list : 10.23.0.16
Remote Port :9911
Statistics :
    Invalid Sctp signals Total :0 Since last 0
    Sctp Send failures :0

```

Table 6 describes significant fields shown in this output.

Table 6 *show iua asp all Field Descriptions*

Field	Description
Name of ASP: 1	Name of the application server process (ASP).
Current State of ASP: ASP-Active	The possible states are ACTIVE, INACTIVE, and DOWN.
Current state of underlying Sctp Association IUA_ASSOC_ESTAB , assoc id 0	States used for underlying Sctp association: IUA_ASSOC_ESTAB (association established) or IUA_ASSOC_INIT (association not established...attempting to initiate).
Sctp Association information : Local Receive window :9000 Remote Receive window :9000	Configured by the user.
Primary Dest address requested by IUA 10.11.2.33	The IP address through which the current link is established.
Remote address list :10.22.3.44 Remote Port :9900	Configured by the user.
Statistics : Invalid Sctp signals Total :0 Since last 0 Sctp Send failures :0	Information useful for seeing if errors are happening with the Sctp connection.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for Sctp.
show ip sctp association list	Shows a list of all current Sctp associations.
show ip sctp association parameters	Shows the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Shows the current statistics for the association defined by the association ID.
show ip sctp errors	Shows error counts logged by Sctp.
show ip sctp instances	Shows the currently defined Sctp instances.
show ip sctp statistics	Shows the overall statistics counts for Sctp.
show iua as	Shows information about the current condition of an AS.

Glossary

API—Application Programming Interface.

AS—application server. A logical entity serving a specific application instance. An example of an application server is an MGC handling the Q.931 and call processing for D channels terminated by the signaling gateways.

ASP—application server process. A process instance of an application server. Examples of application server processes are primary or backup MGC instances.

backhaul—A process in which telephony signaling is passed from a gateway to a separate control for processing. With such a scheme, the gateway does not need to interpret the signaling information.

BRI—Basic Rate Interface. ISDN interface composed of two B channels and one D channel for circuit-switched communication of voice, video, and data.

DS-0—digital signal level 0. Framing specification used in transmitting digital signals over a single channel at 64-kbps on a T1 facility. Compare with DS-1 and DS-3.

failover—The capability to re-route signaling traffic as required between related ASPs in the event of failure or if the currently used ASP is unavailable (from primary MGC to backup MGC, for example). Failover also applies to the return to service of a previously unavailable process.

IETF—Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC.

ISDN—Integrated Services Digital Network.

IUA—ISDN Q.921 User Adaptation Layer. Provides for the transport of signaling protocol between a SG and MGC including transporting Q.921/Q.931 boundary primitives, communication between layer management modules, and management of active associations.

Layer 1—physical layer of the OSI reference model defined in ITU X.200. It is responsible for the electric signal being sent and received. This can be viewed as a bit stream coming in, and going out, of the system. Scope must be considered when using this term. For example, Layer 1 on a T1 is 1.544 Mbps but Layer 1 on a DS-0 timeslot in the T1 is 64 kbps.

Layer 2—datalink layer of the OSI reference model defined in ITU X.200. It is responsible for point-to-point delivery of a PDU. Layer 2 protocols have two basic classes: reliable (meaning delivery is guaranteed or an error is reported) and unreliable (meaning delivery might not occur with no indication to the upper layers).

Layer 3—network layer of the OSI reference model defined in ITU X.200. It is responsible for the network routing and delivery of messages. Examples of Layer 3 protocols include the X.25 packet level protocol and the Internet Protocol. Q.931 is not considered a Layer 3 protocol because it does not route or deliver messages.

MG—media gateway. A media gateway terminates PSTN facilities (trunks), packetizes the PCM stream into IP/ATM and/or forwards packets into the IP/ATM network. Optionally, media gateways can provide signaling backhaul.

MGC—Media Gateway Controller. A Media Gateway Controller provides call control capability to handle signaling traffic from a variety of sources. It also manages connections and resources of its media gateways. Can also be called a Call Agent.

MGCP—Media Gateway Control Protocol.

NFAS—Non-Facility Associated Signaling. This is a classification of signaling protocols that provide the signaling channel in a separate physical line from the bearer channels.

PRI—Primary Rate Interface.

Q.921, Q.931—ITU-T specifications for the ISDN UNI data link layer.

SAP—Service Access Point.

SCN—Switched Circuit Network. A network that carries traffic within channelized bearers of pre-defined sizes.

SCTP—Stream Control Transmission Protocol. General IP transport protocol defined by the SIGTRAN working group of the IETF.

SG—signaling gateway. A signaling gateway transmits PSTN signaling at the edge of an IP/ATM network. It backhauls the signaling to a Media Gateway Controller.

SGCP—Simple Gateway Control Protocol.

SIGTRAN—One of the working groups of the IETF.

SM—session manager.

TCP—Transmission Control Protocol.

TEI—terminal endpoint identifier.

T1-CAS—T1 Channel Associated Signaling.

UAL—User Adaptation Layer.

ULP—Upper Layer Protocol. The logical higher-layer application which uses the services of SCTP.

VoIP—Voice over IP. The ability to carry normal telephone-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality.

