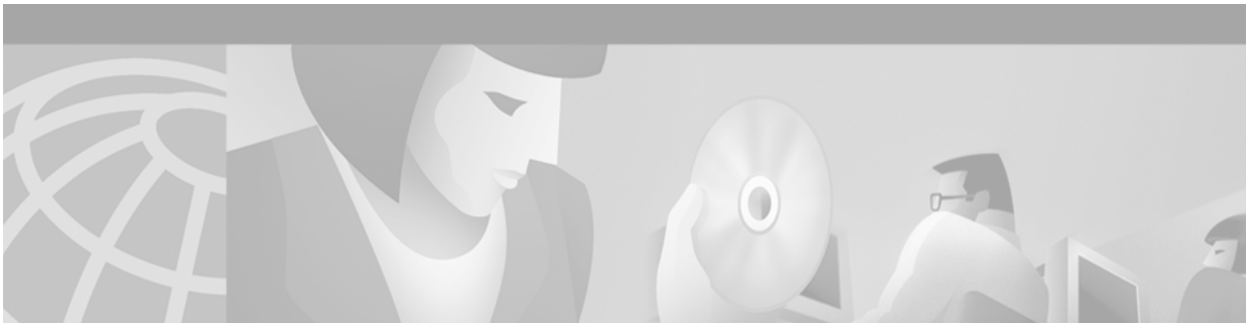


QSIG Backhaul (RUDP based) for Cisco IOS Gateways Configuration Note

Feature History

Release	Modification
12.2(11)T	This feature was introduced on the Cisco IAD2420 series, Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(11)ZC	This feature was introduced on the Catalyst 6500 series and Cisco 7600 series Communication Media Module (CMM).

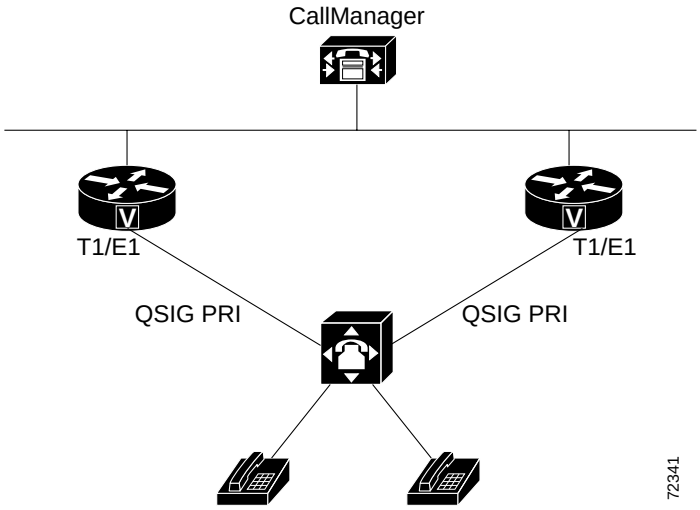
The QSIG Backhaul (RUDP based) for Cisco IOS Gateways feature describes the implementation of the PRI/Q.931 Signaling Backhaul for the Call Agent Applications. It includes information on the benefits of the new feature, supported platforms, related documents, and configuring the feature.

This document includes the following sections:

Feature Overview

PRI/Q.931 signaling backhaul is the transport of PRI signaling (Q.931 and above layers) between a media gateway (such as a Cisco access server, router, or concentrator) and a media gateway controller (specifically, the Cisco VSC3000). The Media Gateway Controller can also be referred to as a *Virtual Switch Controller* (VSC). Communication between the media gateway and the media gateway controller is managed by the Media Gateway Control Protocol (MGCP). Figure 1 shows signaling backhaul paths in a typical packet voice network.

Figure 1 PRI Signaling Backhaul



The signaling backhaul takes place between a media gateway and a Cisco VSC3000. A media gateway is an access server, router, or access concentrator that provides an interface between the Public Switched Telephone Network (PSTN) and the packet network world (IP or ATM). The VSC provides call processing and gateway control.

The general principle behind signaling backhaul is to pass as many layers of a protocol stack as possible through a gateway directly to the VSC.

Signaling backhaul usually occurs at a common boundary for all protocols. For ISDN, the signaling backhaul takes place at the boundary between Layer 2 (Q.921) and Layer 3 (Q.931). The lower layers of the protocol are terminated and processed on the gateway. The upper layers of the protocol are backhauled, or transported, to the VSC using Cisco Reliable User Datagram Protocol (RUDP) over IP. RUDP provides autonomous notification of connected and failed sessions and guarantees delivery of signaling protocols across an IP network.

Signaling backhaul provides the additional advantage of distributed protocol processing. This permits greater expandability and scalability, while offloading lower-layer protocol processing from the VSC.

Signaling Backhaul and Backhaul Session Manager

The backhaul session manager is a software function that resides on the Cisco media gateway and manages RUDP sessions on the VSC and gateway.

The backhaul session manager enables signaling applications to backhaul signaling information to a remote or local VSC and provides redundancy and transparent management of transport paths. The backhaul session manager also combines sessions between endpoints into session groups and combines session groups into session sets. In this process the session manager establishes a selection priority for the sessions.

To configure the backhaul session manager, you must create a new session-set, add session-groups to that session-set, and then add sessions to the session-group.

A session is an RUDP connection between two endpoints. An endpoint is defined by the IP address and the User Datagram Protocol (UDP) port.

A session-group is a logically ordered list of sessions based on priority of the sessions. All of the sessions in the session-group *must* be configured to connect the same physical machines and, for reliability, these sessions can be defined to take different paths through the network. The backhaul session manager always uses the highest priority session available in the session-group to transport all PRI signaling traffic, regardless of the number of sessions configured in the session-group (note that RUDP keepalive traffic would exist on all sessions).

If a session fails while in use, or a higher priority session within the same session group gets established, the backhaul session manager and RUDP support a function in which messages waiting to be transmitted on the current session are transferred to another session automatically, while maintaining guaranteed, in-sequence delivery. This function is sometimes referred to as *session failover*. Thus, a session-group enables network path redundancy between the gateway and the VSC. A session-group cannot be deleted unless the sessions associated with it are deleted first.

A session-set is a collection of session-groups. A session-set enables VSC redundancy and is used to implement VSC switchover. A session-set cannot be deleted unless the groups associated with it are deleted first.

In a fault-tolerant configuration, a session-set on the media gateway can have more than one session-group, with each session-group connecting the gateway to a different VSC. In a non-fault-tolerant configuration, a session-set on the gateway contains only one session-group, because there is only one VSC available.

Each session-set on the VSC always has one session-group, regardless of the configuration being used.

Benefits

Call Control

Signaling backhaul integrates gateways into a virtual switch with the call control centralized in the Cisco VSC.

Signaling Protocols

The QSI Backhaul (RUDP based) for Cisoc IOS Gateways feature provides the infrastructure to support the backhaul of the ISDN signaling protocol in a non-fault-tolerant manner.

Restrictions

On the Cisco 2600 and Cisco 3600 series, this feature supports FAS D-Channel signaling only.

Related Features and Technologies

The PRI/Q.932 Signaling Backhaul for Call Agent Applications feature is supported by the Media Gateway Control Protocol technology, which is documented in the *Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*

Related Documents

- *Cisco Media Gateway Controller Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for Cisco Media Gateway Controller*
- *Cisco MGC Software Release 7 Reference Guide, version 2*
- *Cisco MGC Release 7 Provisioning Guide (-02)*
- *Cisco MGC Software Release 7 Operations, Maintenance, and Troubleshooting Guide*
- *Cisco MGC Software Release 7 Installation and Configuration Guide*
- *Cisco Media Gateway Controller Software Release Notes (version 7)*
- *Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*
- *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2*
- *Catalyst 6500 Series and Cisco 7600 Series Communication Media Module Installation and Configuration Note*
- *Release Notes for Catalyst 6500 Series and Cisco 7600 Series Communication Media Module Software Release 12.2(11)ZC*

Supported Platforms

Supported Platforms

- Cisco IAD2420 series
- Cisco 2600 series
- Cisco 3600 series
- VG200
- Catalyst 6500 series and Cisco 7600 series CMM

Determining Platform Support Through Cisco Feature Navigator

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

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

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

http://www.cisco.com/register

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

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

Availability of Cisco IOS Software Images

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

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

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

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

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

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

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

http://www.cisco.com/register

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

- If there are multiple Cisco VSC3000s in the network, E-ISUP signaling connectivity must be in place between them.
- Data connectivity must be in place between the media gateways in the network.
- Cisco 2600 and 3600 series media gateways must have a high-density voice network module installed for interface to the PSTN.
- Cisco CallManager Version 3.3 or a later release.
- Cisco IOS Release 12.2(11)T or a later release must be running.
- For the Catalyst 6500 series and Cisco 7600 series CMM, Cisco IOS Release 12.2(11)ZC or a later release must be running.

Configuration Tasks

See the following sections for configuration tasks for the PRI/Q.931 Signaling Backhaul for Call Agent Applications feature. Each task in the list is identified as either required or optional:

- Configuring Backhaul Session Manager (required)
- Configuring ISDN Signaling Backhaul (required)
- Configuring Fast Ethernet for Signaling Backhaul Compatibility (required)
- Configuring the Cisco VSC3000 (required)
- Configuring MGCP (required)
- Verifying the Configuration (optional)

Configuring Backhaul Session Manager

The backhaul session manager operates on the media gateway and enables signaling applications to backhaul signaling information to a remote or local virtual switch controller (VSC), and also provides redundancy and transparent management of transport paths.

To configure the backhaul session manager, log onto the media gateway and complete the following tasks as required for your application:

- Creating Session-Sets, Session-Groups, and Sessions (required?)
- Changing the Values of Session-Group Parameters (optional)

Creating Session-Sets, Session-Groups, and Sessions

To create session-sets, session-groups, and sessions on the Cisco media gateway, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# backhaul-session-manager`	Enters backhaul session manager configuration mode.
Step 2	`Router(config-bsm)# set` *set-name* `client {ft | nft}`	Creates a session-set and specifies its parameters: • *set-name*—A word you select to identify the session-set • **client**—Required for PRI backhaul; specifies that the session-set function as a client • Fault-tolerance option: – **ft** = Fault-tolerant – **nft** = Non-fault-tolerant **Note** For fault-tolerant operation, you must configure more than one group in this session-set. If only one group is configured in this session-set, you must specify **nft**. **Note** If you configure the session-set for non-fault-tolerant operation, you should also configure the VSC for non-fault-tolerant operation. See the "Configuring the Cisco VSC3000" section on page 13.
Step 3	`Router(config-bsm)# group` *group-name* `set` *set-name*	Adds a new session-group to a specified session-set. • *group-name*—A word you select to identify the new session-group • *set-name*—The session-set to which you are adding the new session-group Repeat this step to add additional session-groups to a session-set.

	Command	Purpose
Step 4	`Router(config-bsm)# session group group-name remote_ip remote_port local_ip local_port priority`	Adds a session to a session-group and specifies the interfaces and selection priority for the session. • *group-name*—The session-group to which you are adding this session • *remote_ip*—IP address of the VSC server at the remote end of this backhaul link • *remote_port*—The UDP port number on the VSC server at the remote end of this backhaul link; The range is from 1024 to 9999; Make sure that this number is not already being used by another service on the VSC, such as Media Gateway Control Protocol (MGCP). • *local_ip*—The IP address of the media gateway port used for signaling backhaul. • *local_port*—The UDP port number of the media gateway port used for signaling backhaul; The range is from 1024 to 9999. • *priority*—The priority within the session-group; The range is from 0 to 9999; 0 is the highest priority. **Note** Although the Cisco IOS software allows you to configure multiple sessions with the same priority in a session-group, Cisco Systems recommends that the priority of each session be unique within a session-group.
Step 5	Repeat Step 4 to create additional sessions in a session-group.	**Note** To support session failover (fault tolerance), you must configure at least two sessions in a session-group.

Changing the Values of Session-Group Parameters

If you need to change the default values of session-group parameter, use the following commands as required, in backhaul session manager configuration mode:

Caution Do not change the session-group parameters unless instructed to do so by Cisco technical support. There are relationships between the parameters that can cause sessions to fail if not set correctly.

Command	Purpose
`Router(config-bsm)# group` *group-name* `auto-reset` *number-of-auto-resets*	Specifies the maximum number of auto resets before the connection is considered failed. The range is from 0 to 255. The default is 5.
`Router(config-bsm)# group` *group-name* `cumulative-ack` *number-of-segments*	Specifies the maximum number of RUDP segments that will be received before sending an acknowledgment. The range is from 0 to 255. The default is 3.
`Router(config-bsm)# group` *group-name* `out-of-sequence` *number-of-segments*	Specifies the maximum number of out-of-sequence segments that will be received before an error acknowledgment (EACK) is sent. The range is from 0 to 255. The default is 3.
`Router(config-bsm)# group` *group-name* `receive` *window-size*	Specifies the maximum window size for the receiver. The range is from 1 to 65. The default is 32.
`Router(config-bsm)# group` *group-name* `retransmit` *resend-attempts*	Specifies the maximum number of times RUDP will attempt to resend a segment before declaring the connection broken. The range is from 0 to 255. The default is 2.
`Router(config-bsm)# group` *group-name* `timer cumulative-ack` *milliseconds*	Specifies the maximum number of milliseconds RUDP will delay before sending an acknowledgment for a received segment. The range is from 100 to 65535. The default is 300.
`Router(config-bsm)# group` *group-name* `timer keepalive` *milliseconds*	Specifies the number of milliseconds RUDP will wait before sending a keepalive segment. The range is from 0 to 65535. The default is 200.
`Router(config-bsm)# group` *group-name* `timer retransmit` *milliseconds*	Specifies the number of milliseconds RUDP will wait to receive an acknowledgment for a segment. The range is from 100 to 65535. The default is 600.
`Router(config-bsm)# group` *group-name* `timer transfer-state` *milliseconds* `Router(config-bsm)# exit`	Specifies the number of milliseconds RUDP will wait to receive the selection of a new session from the application during a transfer state. The range is from 0 to 65535. The default is 600.

Configuring ISDN Signaling Backhaul

To configure ISDN to backhaul Q.931 signaling, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# controller {t1 | e1} slot/port`	Enters controller configuration mode.
Step 2	`Router(config-controller)# clock source [internal | line]`	Configures the clock source used by the T1 or E1 controller. The keywords are as follows: • **internal** (Optional)—Specifies that the clocking source is obtained from the port adapter line. • **line** (Optional)—Specifies that the clocking source is obtained from the network.
Step 3	`Router(config-controller)# cablelength long {0db | -7.5db | -15db | -22.5db}`	Specifies the cable length longer than 600 feet for a T1 link. The cable length must conform to the actual cable length that you are using. For example, if you attempt to enter the **cablelength short** command on a long-haul T1 link, the command is rejected. The keywords are as follows: • **0db**—Specifies the decibel pulse level at 0 dB. This is the default pulse rate. • **-7.5db**—Specifies the decibel pulse level at -7.5 dB. • **-15db**—Specifies the decibel pulse level at -15 dB. • **-22.5db**—Specifies the decibel pulse level at -22.5 dB.
	or `Router(config-controller)# cablelength short {110ft | 220ft | 330ft | 440ft | 550ft | 600ft}`	Specifies a cable length 600 feet or less for a T1 link. The keywords are as follows. • **110ft**—Specifies a cable length from 0 to 110 feet. • **220ft**—Specifies a cable length from 111 to 220 feet. • **330ft**—Specifies a cable length from 221 to 330 feet. • **440ft**—Specifies a cable length from 331 to 440 feet. • **550ft**—Specifies a cable length from 441 to 550 feet. • **600ft**—Specifies a cable length from 551 to 600 feet. If you do not set the cable length, the system defaults to a setting of cablelength long 0 dB.
Step 4	`Router(config-controller)# pri-group timeslots list-of-timeslots service mgcp`	Specifies MGCP as the control protocol used for backhaul. The controller time slots cannot be shared between backhaul and other Layer 3 protocols.

	Command	Purpose
Step 5	`Router(config-controller)# framing {esf | sf | crc4 | no-crc4 | mp-crc4} [australia]`	Specifies the framing type on a DS1 link for T1 and E1 PRI. The keywords are as follows: • **esf**—Specifies extended Super Frame as the T1 frame type. • **sf**—Specifies Super Frame as the T1 frame type. This is the default. • **crc4**—Specifies CRC4 frame as the E1 frame type. This is the default for Australia. • **no-crc4**—Specifies no CRC4 frame as the E1 frame type. • **australia**—(Optional) Specifies the E1 frame type used in Australia.
Step 6	`Router(config-controller)# linecode {ami | b8zs | hdb3}`	Specifies the line encoding method for a DS1 link. The keywords are as follows: • **ami**—Specifies alternate mark inversion (AMI) as the line-code type. Valid for T1 or E1 controllers. This is the default for T1 lines. • **b8zs**—Specifies B8ZS as the line-code type. Valid for T1 controller only. • **hdb3**—Specifies high-density bipolar 3 (hdb3) as the line-code type. Valid for E1 controller only. This is the default for E1 lines.
Step 7	`Router(config-controller)# exit`	Returns to global configuration mode.
Step 8	`Router(config)# interface serial` *slot/port*`:`*timeslot number*	Enters serial interface configuration mode. The arguments and keywords are as follows: • *slot/port***:**—Specifies the slot number and port number where the channelized E1 or T1 controller is located. • *timeslot*—Specifies, for ISDN, the D channel time slot, which is the 23 channel for T1 and the 15 channel for E1. PRI time slots are range from 0 to 23 for channelized T1 and range from 0 to 30 for channelized E1. On a dual port card, it is possible to run channelized on one port and primary rate on the other port. **Note** The colon (:) is required. • *number*—Specifies the channelized E1 or T1 controller number.

	Command	Purpose
Step 9	`Router(config-if)# isdn switch-type [primary-4ess | primary-5ess | primary-dms100 | primary-ni | primary-net5 | primary-ntt | primary-qsig | primary-ts014]`	Configures the ISDN switch type. This configuration can be done in global configuration mode or interface configuration mode. The keywords are as follows: • **primary-4ess** (Optional)—Specifies electronic switching system (ESS) 4. • **primary-5ess** (Optional)—Specifies ESS 5 that works with T1. • **primary-dms-100** (Optional)—Specifies the DMS 100 switch that works with T1 and E1 PRI. • **primary-ni** (Optional)—Specifies an NI switch that works with T1. • **primary-net5** (Optional)—Specifies a Net5 switch that works with E1. • **primary-ntt** (Optional)—Specifies the Japanese T1 and E1 PRI switch. • **primary-qsig** (Optional)—Supports QSIG signaling per Q.931. Network side functionality is assigned with the **isdn protocol-emulate** command.
Step 10	`Router(config-if)# isdn protocol-emulate {user | network}`	Specifies the ISDN protocol emulation. The default is the user-side ISDN protocol. The keywords are as follows: • **user**—Specifies Layer 2 and Layer 3 port protocol operation as TE (port functions as QSIG slave). • **network**—Specifies Layer 2 and Layer 3 port protocol operation as NT (port functions as QSIG master).

Repeat this procedure for each T1 interface on the media gateway that will utilize backhaul.

Configuring Fast Ethernet for Signaling Backhaul Compatibility

If your media gateway has 10/100 Base T Fast Ethernet capability, configure the Fast Ethernet interface not to use auto-negotiation.

Caution When the Fast Ethernet interface is configured for autonegotiation, it can take as much as two seconds for this interface to be enabled when the interface has to initialize. Two examples of when the interface initializes are the running of the **no shut** command and disconnection or reconnection of the Ethernet cable. Autonegotiation affects the traffic flow on the Ethernet interface, and can therefore interrupt the traffic flow on existing RUDP connections, causing them to fail. To avoid these problems, the Fast Ethernet interface should not be configured for autonegotiation. Instead, the duplex and speed parameters should be set according to the requirements of the network.

To reconfigure the Fast Ethernet interface for specified duplex and speed operation, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface Ethernet-port-number`	Enters Ethernet interface configuration mode for the specified Ethernet port.
Step 2	`Router(config-if)# duplex {full | half}`	Configures the Ethernet port for full-duplex or half-duplex operation.
Step 3	`Router(config-if)# speed {10 | 100}`	Configures the Ethernet port to operate at 10 Mbps or 100 Mbps.
Step 4	`Router(config-if)# exit`	Exits from interface configuration mode.

Configuring the Cisco VSC3000

The Cisco VSC3000 is the signaling controller software that provides call control and runs on a UNIX server such as a Sun Netra 1800. Man Machine Language (MML) is the user interface into the signaling controller software. You use this interface to configure parameters of your signaling controller software and to display information about the current settings.

To configure the Cisco VSC3000 to perform signaling backhaul, log onto the UNIX server and complete the MGCP service provisioning procedure as follows:

	Command	Purpose
Step 1	`mml> prov-add:extnode:name=media-gateway-name,`	Assigns a name to the media gateway (the external node) at the far end of a backhaul link.
	`desc=media-gateway-name`	Provides a description of the media gateway.
Step 2	`mml> prov-add:ipfaspath:name=ipfaspath-name,`	Adds an IP path for D-channel transport (ipfaspath) from the Cisco VSC3000 to a media gateway and assigns it a path name.
	`extnode=media-gateway-name,`	Specifies the media gateway (external node) at the opposite end of the IP path; the name must match the media gateway name assigned in Step 1.

	Command	Purpose
	mdo=*ISDN-varient*,	Specifies the ISDN variant. Options include: • **ETSI_300_102** • **ETSIS_300_102_C1** • **ATT_41459** • **ATT_41459_C2** • **BELL_1268** • **ETSI_300_172** • **BELL_1268_C3** • **NTT_INS_1500** • **ETS_300_121**.
	custgrpid=*customer-group-ID*,	Assigns a customer group ID (the dial plan to use for this connection).
	side=*equipment-location*,	Defines the Cisco VSC3000 as network side or user side. The Cisco VSC3000 is normally network side, opposite to the PBX, which is normally the user side. Enter **network**, or **user**,.
	desc=*description*	Describes the function of this IP path (backhaul service to a specified media gateway.
Step 3	mml> **prov-add:iplnk:name=***iplink-name*,	Adds an IP link for the PRI D-channel and assigns it a name.
	if=enif*interface-number*,	The Ethernet interface name for the Cisco VSC3000 Ethernet card (typically **enif1**).
	ipaddr=IP_Addr*number*,	The IP address of the Cisco VSC3000 Ethernet port as defined in ../etc/XECfgParm.dat (for example, **IP_Addr1**).
	port=*port-number*,	The port number on the Cisco VSC3000.
	pri=*priority-number*,	The selection priority of this IP link. (**1**, **2**, etc.; this should match the selection priority specified on the media gateway for this IP link.)
	peeraddr=*IP-address*,	The IP address of the media gateway.
	peerport=*port-number*,	The port number on the media gateway; does not have to match the VSC port.
	sigslot=*slot-number*,	The physical card slot in the media gateway.
	sigport=*port-number*,	The PRI port number in the media gateway (same as the T1/E1 controller number).
	svc=*ipfaspath-name*,	The IP path that this IP link is assigned to, which matches the *ipfaspath-name* assigned in Step 2.
	desc=*description*	Optional description of this IP link.
Step 4	mml>**prov-add:mgcppath:name=***MGCP-path-name*,	Defines an MGCP control path.
	extnode=*ipfaspath-name*,	Associates the MGCP control path with an IP path for D-channel transport. The *ipfaspath-name* must match the *ipfaspath-name* specified in Step 2.
	desc=*description*	Optional description of this MGCP control path.
Step 5	mml>**prov-add:iplnk:name=***clink6*,	Adds an IP link for the MGCP control path.

Command	Purpose
if=*enif1*,	The Ethernet interface name for the Cisco VSC3000 Ethernet card (typically **enif1**).
ipaddr=IP_Addr*number*,	The IP address of the Cisco VSC3000 Ethernet port as defined in `../etc/XECfgParm.dat` (for example, **IP_Addr1**).
port=2427,	The port used by the IP link for the MGCP control path on the Cisco VSC3000 (**2427** is predefined for MGCP use).
peeraddr=*IP-address*,	The IP address of the media gateway connected to this IP link.
peerport=2427,	The IP port at the media gateway for this IP link (**2427** is predefined for MGCP use).
svc=*mgcp-service-name*,	A name of the MGCP signaling service supported by this IP link.
pri=1,	Selection priority for this IP link(**1**, **2**, etc.)
desc=*description*	Optional description of the IP link for the MGCP control path.

Note If the Cisco VSC3000 is set up for fault-tolerant operation, configure the backhaul session manager also for fault-tolerant operation. For more information, refer to the *Cisco MGC Software Release 7 Provisioning Guide*.

Configuring MGCP

To configure Media Gateway Control Protocol (MGCP) on the Cisco media gateway, perform the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# mgcp`	Starts the MGCP daemon.
Step 2	`Router(config)# mgcp request timeout` *timeout*	Specifies how long the gateway should wait for a response to a request.
Step 3	`Router(config)# mgcp request retries` *count*	Specifies the number of times to retry sending the **mgcp** command.
Step 4	`Router(config)# mgcp call-agent` {*ipaddr* | *hostname*} [*port*]	Configures the address of the call agent.
Step 5	`Router(config)# mgcp max-waiting-delay` *value*	Configures the maximum waiting delay to be used in an RSIP message as restart instructions for the call agent.
Step 6	`Router(config)# mgcp restart-delay` *value*	(Optional) Configures the restart delay value to be used in an RSIP message as graceful tear down instructions for the gateway connection.
Step 7	`Router(config)# mgcp vad`	(Optional) Configures voice activity detection.

	Command	Purpose
Step 8	`Router(config)# mgcp package-capability {as-package | atm-package | ddtmf-package | gm-package | rtp-package | trunk-package}`	Specifies an MGCP package capability.
Step 9	`Router(config)# mgcp default-package {as-package | atm-package | dtmf-package | gm-package | rtp-package | trunk-package}`	Configures the default package capability type.
Step 10	`Router(config)# mgcp quality-threshold {hwm-jitter-buffer value | hwm-latency value | hwm-packet-loss value | lwm-jitter-buffer value | lwm-latency value | lwm-packet-loss value}`	(Optional) Configures the jitter buffer size, packet-loss threshold, and latency threshold.
Step 11	`Router(config)# mgcp playout {adaptive init-value min-value max-value} | {fixed init-value}`	(Optional) Tunes the jitter buffer packet size used for MGCP connections.
Step 12	`Router(config)# mgcp codec type [packetization-period value]`	(Optional) Configures the default codec type.
Step 13	`Router(config)# mgcp ip-tos {high-reliability | high-throughput | low-cost | low-delay | precedence value}`	(Optional) Enables the IP Type of Service for MGCP connections.
Step 14	`Router(config)# controller T1 0`	Selects the T1 controller 0.
Step 15	`Router(config-controller)# mode atm`	Specifies that the controller will support ATM encapsulation and create ATM interface 0. When the controller is set to ATM mode, the following takes place: • Controller framing is automatically set to Extended SuperFrame (ESF). • The linecode is automatically set to B8ZS.
Step 16	`Router(config-controller)# no shutdown`	Activates the controller.
Step 17	`Router(config-controller)# exit`	Exit controller configuration mode.
Step 18	`Router(config)# controller T1 1`	(For CAS PBX Scenarios only) Selects the T1 controller 1.
Step 19	`Router(config-controller)# mode cas`	(For CAS PBX Scenarios only) Specifies that the controller will support CAS.
Step 20	`Router(config-controller)# ds0-group channel-number timeslots range type signaling-type tone type addr info service service-type`	(For CAS PBX Scenarios only) Configures the T1 timeslots for CAS calls. The scenarios use the following three DS0 definitions: ds0-group 1 timeslots 1-8 type e&m-immediate-start ds0-group 2 timeslots 9-16 type e&m-wink-start ds0-group 3 timeslots 17-24 type fxs-ground-start
Step 21	`Router(config-controller)# exit`	(For CAS PBX Scenarios only) Exits controller configuration mode.
Step 22	`Router(config)# interface atm0 [subinterface-number [multipoint | point-to-point]]`	Enters interface configuration mode to configure ATM interface 0 or an ATM subinterface. The default for subinterfaces is **multipoint.** (For all Scenarios) Set up three subinterfaces for **point-to-point**.

	Command	Purpose
Step 23	`Router(config-if)# pvc [name] vpi/vci`	Creates an ATM PVC for voice traffic and enter ATM virtual circuit configuration mode. **Note** The **ilmi** and **qsaal** options are not supported for AAL2.
Step 24	`Router(config-if-atm-vc)# encapsulation aal-encap`	Sets the encapsulation of the PVC for voice traffic. **aal2** automatically creates channel identifiers (CIDs) 1 through 255. Some of the scenarios use **aal5snap** for ATM0.1 and ATM0.3. Use **aal2** for ATM0.2.

	Command	Purpose
Step 25	`Router(config-if-atm-vc)# vbr-rt peak-rate average-rate [burst]`	Configures the PVC for the variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • Peak rate — If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM). • Average rate — Calculate according to the maximum number of calls the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: **For VoIP** G.711 with 40 or 80 byte sample size — max calls x 128K G.726 with 40 byte sample size: — max calls x 85K G.729a with 10 byte sample size — max calls x 85K **For VoAAL2** G.711 with 40 byte sample size — max calls x 85K G.726 with 40 byte sample size — max calls x 43K G.729a with 10 byte sample size — max calls x 43K If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • Burst size — Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier.
Step 26	`Router(config-if-atm-vc)# vcci pvc-identifier`	Assigns a unique identifier to the PVC.
Step 27	`Router(config-if-atm-vc)# exit`	Exits ATM virtual circuit configuration mode.
Step 28	`Router(config-if)# exit`	Exits interface configuration mode.
Step 29	`Router(config)# dial-peer voice number pots`	Enters dial peer configuration mode for the POTS dial peer.
Step 30	`Router(config-dial-peer)# application MGCPAPP`	Initiates the MGCP protocol for the voice ports.

Verifying the Configuration

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

In the following example, notice that the Layer 2 protocol is Q.921, and the Layer 3 protocol is BACKHAUL. This verifies that the Cisco VSC3000 is configured to backhaul ISDN. Also, if you are connected to a live line, you should see that 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
```

Step 2 Enter the **show backhaul-session-manager set all** command to display all session-sets. This set contains one group called “grp1” and it is configured in fault-tolerant mode.

```
Router# show backhaul-session-manager set all
Session-Set
   Name   :set1
   State  :BSM_SET_OOS
   Mode   :Fault-Tolerant(FT)
   Option :Option-Client
   Groups :1
   statistics
        Successful switchovers:0
        Switchover Failures:0
        Set Down Count 0
        Group:grp1
```

Possible states include the following:

SESS_SET_IDLE—A session-set has been created.

SESS_SET_OOS—A session has been added to a session-group. An ACTIVE notification has not been received from the Cisco VSC3000.

SESS_SET_ACTIVE_IS—An ACTIVE notification has been received over one in-service session-group. STANDBY notification has not been received on any available session-group(s).

SESS_SET_STNDBY_IS—A STANDBY notification has been received, but there is no in-service active session-group available.

SESS_SET_FULL_IS—A session-group in-service that has ACTIVE notification and at least one session-group in-service that has STANDBY notification.

SESS_SET_SWITCH_OVER—An ACTIVE notification is received on session-group in-service, which has received STANDBY notification.

Step 3 Enter the **show backhaul-session-manager group status all** command to display the state of all session-groups.

The Status is either Group-OutOfService (no session in the group has been established) or Group-InService (at least one session in the group has been established).

The Status(use) is either Group-Standby (the Cisco VSC3000 connected to the other end of this group goes into standby mode), Group-Active (the Cisco VSC3000 connected to the other end of this group is the active Cisco VSC3000), or Group-None (the Cisco VSC3000 has not declared its intent).

```
Router# show backhaul-session-manager group status all
Session-Group
Group Name   :grp1
   Set Name     :set1
   Status       :Group-OutOfService
   Status (use) :Group-None
```

Step 4 Enter the **show backhaul-session-manager session all** command to display all sessions.

The State will be OPEN (the connection is established), OPEN_WAIT (the connection is waiting for establishment), OPEN_XFER (session failover is in progress for this session, which is a transient state), or CLOSE (this session is down, also a transient state). The session will move to OPEN_WAIT after waiting a fixed amount of time.

The Use-status field indicates whether PRI signaling traffic is being transported over this session. The field is either OOS (this session is not being used to transport signaling traffic) or IS (this session is being used to transport all PRI signaling traffic). The User-status field indicates the connection status.

```
Router# show backhaul-session-manager session all

Session information --
Session-id:35
  Group:grp1
Configuration:
     Local:10.1.2.15      , port:8303
    Remote:10.5.0.3       , port:8303
  Priority:2
  RUDP Option:Client, Conn Id:0x2
State:
  Status:OPEN_WAIT, User-status:OOS
```

```
Statistics:
  # of resets:0
  # of auto_resets 0
  # of unexpected RUDP transitions (total) 0
  # of unexpected RUDP transitions (since last reset) 0
  Receive pkts -  Total:0 , Since Last Reset:0
  Recieve failures -  Total:0 ,Since Last Reset:0
  Transmit pkts - Total:0, Since Last Reset:0


  Transmit Failures (PDU Only)
         Due to Blocking (Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  Transmit Failures (NON-PDU Only)
         Due to Blocking(Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  RUDP statistics
         Open failures:0
         Not ready failures:0
         Conn Not Open failures:0
         Send window full  failures:0
         Resource unavailble failures:0
         Enqueue failures:0
```

Monitoring and Maintaining Signaling Backhaul and MGCP

See the following sections to monitor and maintain your signaling backhaul and MGCP configurations.

Monitoring and Maintaining Signaling Backhaul

To monitor and maintain the signaling backhaul sessions and the connection to the Cisco VSC3000, use the following commands as needed:

Command	Purpose
`Router# clear backhaul-session-manager group`	Resets the statistics for all available session-groups or for a specified session-group.
`Router# show backhaul-session-manager set`	Displays status, statistics, or configuration of all available session-sets.
`Router# show backhaul-session-manager group`	Displays status, statistics, or configuration of all available session-groups.
`Router# show backhaul-session-manager session`	Displays status, statistics, or configuration of all available sessions.
`Router# show isdn status`	Displays status of ISDN backhaul. If the connection to the Cisco VSC3000 is lost, the router shuts down Layer 2 so that it cannot receive more calls. When the Cisco VSC3000 connection is back up, you can use this command to verify that Layer 2 has also been brought back up correctly.

Monitoring and Maintaining MGCP

Use these commands at any time to monitor the MGCP configuration and status:

Command	Purpose
`Router# show mgcp [all | events | errors | packets]`	Displays all active MGCP connections on the router.
`Router# debug mgcp [all | errors | events | packets | parser]`	Turns on debugging for the gateway.
`Router# clear mgcp statistics`	Resets the MGCP statistical counters.

Configuration Examples

This section provides the following configuration examples:

- Configuring the Cisco Media Gateway
- .Figure 2 shows the network elements, paths, and connections in the previous example.
- Configuring the Cisco VSC3000

Configuring the Cisco Media Gateway

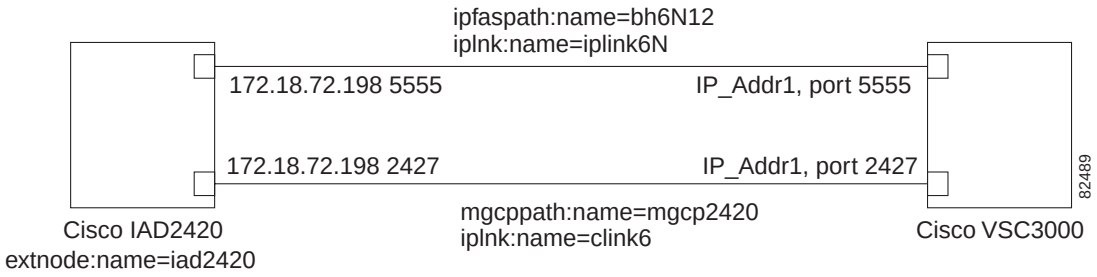
The following example configures a Cisco IAD2420 for signaling backhaul to a Cisco VSC3000 in the configuration shown in Figure 2:

```
Router(config)# network-clock base-rate 56k
Router(config)# ip subnet-zero
.
.
.
Router(config)# mgcp
Router(config)# mgcp call-agent 172.18.72.200 service-type mgcp version 0.1
Router(config)# mgcp sdp simple
Router(config)# mgcp default-package dt-package
Router(config)# no mgcp timer receive-rtcp
Router(config)# backhaul-session-manager
Router(config-bsm)# set vsc1_set client nft
Router(config-bsm)# group vsc1_grp set vsc1_set
Router(config-bsm)# session group vsc1_grp 172.18.72.200 5555 172.18.72.198 5555 1
Router(config-bsm)# exit
Router(config)# isdn switch-type primary-5ess
Router(config)# call rsvp-sync
.
.
.
Router(config)# controller T1 1
Router(config-controller)# framing esf
Router(config-controller)# linecode b8zs
Router(config-controller)# pri-group timeslots 1-24 service mgcp
Router(config-controller)# exit
Router(config)#
.
.
.
```

```
Router(config)# interface Ethernet0
Router(config-if)# ip address 172.18.72.198 255.255.0.0
Router(config-if)# ip route-cache
Router(config-if)# no ip mroute-cache
Router(config-if)# exit
Router(config)#
.
.
.
Router(config)# interface Serial1:23
Router(config-if)# no ip address
Router(config-if# ip mroute-cache
Router(config-if)# no logging event link-status
Router(config-if)# isdn switch-type primary-5ess
Router(config-if)# isdn incoming-voice voice
Router(config-if)# isdn T306 30000
Router(config-if)# isdn bind-l3 backhaul vsc1_set
Router(config-if)# no cdp enable
Router(config-if)# exit
Router(config)#
```

.Figure 2 shows the network elements, paths, and connections in the previous example.

Figure 2 PRI Signaling Backhaul Configuration Example



- iplnk "iplink6N" is RUDP/IP link for signaling backhaul
- ipfaspath "bh6N12" is IP path for D-channel transport
- iplnk "clink6" is UDP/IP link for MGCP control
- mgcppath "mgcp2420" is IP path for MGCP control

Configuring the Fast Ethernet Interface for Signaling-Backhaul Compatibility

The following example configures a Fast Ethernet interface f0 for full duplex operation at 10 Mbps, so that auto-negotiation is disabled. This procedure might be required for Cisco 2600 or Cisco 3600 series routers.

```
Router(config)# interface f0
Router(config-if)# duplex full
Router(config-if)# speed 10
Router(config-if)# exit
```

Configuring the Cisco VSC3000

The following example configures the Cisco VSC3000 to perform signaling backhaul between a Cisco IAD2420 and a Cisco VSC3000, where the network elements, paths, and connections are defined as follows (See Figure 2):

- Cisco IAD2420—**extnode:name=iad2420**
- Path name for D-channel transport (ipfaspath)—**bh6NI2**
- IP link name for the D-channel path—**iplink6N**
- Path name for MGCP control transport—**mgcp2420**
- IP link name for MGCP control path—**clink6**

```
mml> prov-add:extnode:name=iad2420,desc=iad2420-Spans

mml> prov-add:ipfaspath:name=bh6NI2,extnode=iad2420,mdo=BELL_1268,
custgrpid=1111,side=network,desc=Backhaulservice to iad2420

mml> prov-add:iplnk:name=iplink6N,if=enif1,ipaddr=IP_Addr1,port=5555,pri=1,
peeraddr=172.18.72.198,peerport=5555,sigslot=0,sigport=0,svc=bh6NI2,
desc=IP link-backhaul svc iad2420

mml>prov-add:mgcppath:name=mgcp2420,extnode=iad2420,
desc=MGCP service to iad2420

mml>prov-add:iplnk:name=clink6,if=enif1,ipaddr=IP_Addr1,port=2427,peeraddr=
172.18.72.198,peerport=2427,svc=mgcp2420,pri=1,desc=MGCP link to iad2420
```

Command Reference

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

- **backhaul-session-manager**
- **clear backhaul-session-manager group**
- **clear rudpv1 statistics**
- **debug backhaul-session-manager session**
- **debug backhaul-session-manager set**
- **debug rudpv1**
- **group auto-reset**
- **group cumulative-ack**
- **group out-of-sequence**
- **group receive**
- **group retransmit**
- **group set**
- **group timer cumulative-ack**
- **group timer keepalive**
- **group timer retransmit**
- **group timer transfer**
- **isdn bind-L3**
- **isdn protocol-emulate**
- **session group**
- **set**
- **show backhaul-session-manager group**
- **show backhaul-session-manager session**
- **show backhaul-session-manager set**
- **show rudpv1**

backhaul-session-manager

To enter backhaul-session-manager configuration mode, use the **backhaul-session-manager** command in global configuration mode.

backhaul-session-manager

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Usage Guidelines

Use the backhaul-session-manager global configuration command to switch to the backhaul-session-manager configuration mode from the global configuration mode. Use the **exit** command to exit the backhaul-session-manager configuration mode and return to the global configuration mode.

Examples

The following example enters backhaul-session-manager configuration mode:

```
Router(config)# backhaul-session-manager
Router(config-bsm)#
```

clear backhaul-session-manager group

To reset the session-group statistics or traffic counters, use the **clear backhaul-session-manager group** command in privileged EXEC mode.

clear backhaul-session-manager group stats {**all** | **name** *group-name*}

Syntax Description

all	Resets all available session-groups.
name	Resets one session-group.
group-name	Specifies the session-group to reset.

Defaults

The statistical information accumulates.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Usage Guidelines

A session is the connection between a client and a server, and a session-group is a collection of sessions in a group to implement switchover in case of a session failure. This command clears all statistics that pertain to the backhaul session manager group.

Examples

The following example clears all statistics for all available session-groups:

```
Router# clear backhaul-session-manager group stats all
```

Related Commands

Command	Description
show backhaul-session-manager group	Displays status, statistics, or configuration of a specified or all session-groups.

clear rudpv1 statistics

To clear the counters that track RUDP statistics for a specified session-group, use the **clear rudpv1 statistics** command in privileged EXEC mode.

clear rudpv1 statistics

Syntax Description

This command has no arguments or keywords.

Defaults

The statistical information accumulates.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Usage Guidelines

This command clears all statistics.

Examples

The following example clears all RUDP statistics for all available session-groups:

```
Router# clear rudpv1 statistics
```

Related Commands

Command	Description
debug rudpv1	Displays debugging information for RUDP.
show rudpv1	Displays RUDP statistics.

debug backhaul-session-manager session

To debug all the available sessions or a specified session, use the **debug backhaul-session-manager session** command in privileged EXEC mode. To turn off debugging, use the **no** form of this command.

debug backhaul-session-manager session {**state** {**all** | *session-id*}} | {**xport** {**all** | *session-id*}} | **all**

no debug backhaul-session-manager session

Caution Use caution when enabling this **debug** command in a live system. This command produces large amounts of output which could lead to a disruption of service.

Syntax Description

state	Shows information about state transitions. Possible states are as follows: SESS_SET_IDLE—A session-set has been created. SESS_SET_OOS—A session has been added to a session-group. No ACTIVE notification has been received from the Cisco VSC3000. SESS_SET_ACTIVE_IS—An ACTIVE notification has been received over one in-service session-group. STANDBY notification has not been received on any available session-group. SESS_SET_STNDBY_IS—A STANDBY notification is received, but there is no in-service active session-group available. SESS_SET_FULL_IS—A session-group is in-service that has ACTIVE notification and at least one session-group is in service that has STANDBY notification. SESS_SET_SWITCH_OVER—An ACTIVE notification is received on an in-service session-group that had received STANDBY notification.
all	All available sessions.
session-id	A specified session.
xport	Provides traces for all PDUs (packets), application PDUs, and also session-manager messages. Use caution while enabling this **debug** command in a live system.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example shows output for the **debug backhaul-session-manager session all** command.

```
Router# debug backhaul-session-manager session all
Router# debug_bsm_command:DEBUG_BSM_SESSION_ALL

23:49:14:SESSION:XPORT:sig rcvd. session = 34, connid = 0x80BA12FC, sig = 5 (CONN-RESET)

23:49:14:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:CLOSE
23:49:14:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS

23:49:14:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:OPEN_WAIT
23:49:14:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS

23:49:19:SESSION:XPORT:sig rcvd. session = 34, connid = 0x80BA12FC, sig = 5 (CONN-RESET)

23:49:19:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:CLOSE
23:49:19:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS

23:49:19:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:OPEN_WAIT
23:49:19:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS

23:49:24:SESSION:XPORT:sig rcvd. session = 34, connid = 0x80BA12FC, sig = 5 (CONN-RESET)

23:49:24:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:CLOSE
23:49:24:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS

23:49:24:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:OPEN_WAIT
23:49:24:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS

23:49:29:SESSION:XPORT:sig rcvd. session = 34, connid = 0x80BA12FC, sig = 5 (CONN-RESET)

23:49:29:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:CLOSE
23:49:29:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS

23:49:29:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:OPEN_WAIT
23:49:29:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS

23:49:34:SESSION:XPORT:sig rcvd. session = 34, connid = 0x80BA12FC, sig = 5 (CONN-RESET)

23:49:34:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:CLOSE
23:49:34:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS

23:49:34:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:OPEN_WAIT
23:49:34:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS

23:49:34:SESSION:XPORT:sig rcvd. session = 33, connid = 0x80BA14EC, sig = 1 (CONN-FAILED)

23:49:34:SESSION:STATE:(33) old-state:OPEN, new-state:CLOSE_WAIT
```

The following example shows output for the **debug backhaul-session-manager session state all** command.

```
Router# debug backhaul-session-manager session state all
Router# debug_bsm_command:DEBUG_BSM_SESSION_STATE_ALL

23:50:54:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:CLOSE
23:50:54:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS

23:50:54:SESSION:STATE:(34) old-state:OPEN_WAIT, new-state:OPEN_WAIT
23:50:54:SESSION:STATE:(34) state:OPEN_WAIT, use-state:OOS
```

The following example shows output for the **debug backhaul-session-manager session xport all** command.

```
Router# debug backhaul-session-manager session xport all
Router# debug_bsm_command:DEBUG_BSM_SESSION_XPORT
23:51:39:SESSION:XPORT:sig rcvd. session = 34, connid = 0x80BA12FC, sig = 5 (CONN-RESET)

23:51:42:SESSION:XPORT:sig rcvd. session = 33, connid = 0x80BA14EC, sig = 5 (CONN-RESET)

23:51:44:SESSION:XPORT:sig rcvd. session = 34, connid = 0x80BA12FC, sig = 5 (CONN-RESET)
```

Related Commands

Command	Description
debug backhaul-session-manager set	Traces state changes and receives messages and events for all available session-sets or a specified session-set.

debug backhaul-session-manager set

To trace state changes and receive messages and events for all the available session-sets or a specified session-set, use the **debug backhaul-session-manager set** command in privileged EXEC mode. To turn off debugging, use the **no** form of this command.

debug backhaul-session-manager set {**all** | **name** *set-name*}

no debug backhaul-session-manager set

Syntax Description

all	All available session-sets.
name *set-name*	A specified session-set.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example shows output for the **debug backhaul-session-manager set all** command:

```
Router# debug backhaul-session-manager set all
Router# debug_bsm_command:DEBUG_BSM_SET_ALL

 Function set_proc_event() is called
Session-Set :test-set
Old State   :BSM_SET_OOS
New State   :BSM_SET_OOS
   Active-Grp  :NONE
   Session-Grp :g-11
   Old State   :Group-None
   New State   :Group-None
   Event rcvd  :EVT_GRP_INS

BSM:Event BSM_SET_UP is sent to user
Session-Set :test-set
Old State   :BSM_SET_OOS
New State   :BSM_SET_ACTIVE_IS
   Active-Grp  :g-11
   Session-Grp :g-11
   Old State   :Group-None
   New State   :Group-Active
   Event rcvd  :BSM_ACTIVE_TYPE
```

The following example shows output for the **debug backhaul-session-manager set** command for the session-set named **set1**:

```
Router# debug backhaul-session-manager set name set1
Router# debug_bsm_command:DEBUG_BSM_SET_NAME

Router# Function set_proc_event() is called
Session-Set :test-set
Old State   :BSM_SET_OOS
New State   :BSM_SET_OOS
   Active-Grp  :NONE
   Session-Grp :g-11
   Old State   :Group-None
   New State   :Group-None
   Event rcvd  :EVT_GRP_INS
```

```
Router#BSM:Event BSM_SET_UP is sent to user
Session-Set :test-set
Old State   :BSM_SET_OOS
New State   :BSM_SET_ACTIVE_IS
   Active-Grp  :g-11
   Session-Grp :g-11
   Old State   :Group-None
   New State   :Group-Active
   Event rcvd  :BSM_ACTIVE_TYPE
```

Related Commands

Command	Description
debug backhaul-session-manager session	Debugs all available sessions or a specified session.

debug rudpv1

For debug information for RUDP, use the **debug rudpv1** command in privileged EXEC mode. To turn off debugging, use the **no** form of this command.

debug rudpv1 {**application** | **performance** | **retransmit** | **segment** | **signal** | **state** | **timer** | **transfer**}

no debug rudpv1

Caution Use this command only during times of low traffic.

Syntax Description

application	Application debugging.
performance	Performance debugging.
retransmit	Retransmit/soft reset debugging.
segment	Segment debugging.
signal	Signals sent to applications.
state	State transitions.
timer	Timer debugging.
transfer	Transfer state information.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example shows output for the **debug rudpv1 application** command:

```
Router# debug rudpv1 application
Rudpv1:Turning application debugging on
*Jan  1 00:20:38.271:Send to appl (61F72B6C), seq 12
*Jan  1 00:20:48.271:Send to appl (61F72B6C), seq 13
*Jan  1 00:20:58.271:Send to appl (61F72B6C), seq 14
*Jan  1 00:21:08.271:Send to appl (61F72B6C), seq 15
*Jan  1 00:21:18.271:Send to appl (61F72B6C), seq 16
*Jan  1 00:21:28.271:Send to appl (61F72B6C), seq 17
*Jan  1 00:21:38.271:Send to appl (61F72B6C), seq 18
*Jan  1 00:21:48.275:Send to appl (61F72B6C), seq 19
*Jan  1 00:21:58.275:Send to appl (61F72B6C), seq 20
*Jan  1 00:22:08.275:Send to appl (61F72B6C), seq 21
*Jan  1 00:22:18.275:Send to appl (61F72B6C), seq 22
*Jan  1 00:22:28.275:Send to appl (61F72B6C), seq 23
*Jan  1 00:22:38.275:Send to appl (61F72B6C), seq 24
*Jan  1 00:22:48.279:Send to appl (61F72B6C), seq 25
*Jan  1 00:22:58.279:Send to appl (61F72B6C), seq 26
*Jan  1 00:23:08.279:Send to appl (61F72B6C), seq 27
*Jan  1 00:23:18.279:Send to appl (61F72B6C), seq 28
*Jan  1 00:23:28.279:Send to appl (61F72B6C), seq 29
```

The following example shows output for the **debug rudpv1 performance** command:

```
Router# debug rudpv1 performance
Rudpv1:Turning performance debugging on
corsair-f#
*Jan  1 00:44:27.299:
*Jan  1 00:44:27.299:Rudpv1 Sent:Pkts 11,  Data Bytes 236,  Data Pkts 9
*Jan  1 00:44:27.299:Rudpv1 Rcvd:Pkts 10,  Data Bytes 237,  Data Pkts 9
*Jan  1 00:44:27.299:Rudpv1 Discarded:0,  Retransmitted 0
*Jan  1 00:44:27.299:
*Jan  1 00:44:37.299:
*Jan  1 00:44:37.299:Rudpv1 Sent:Pkts 11,  Data Bytes 236,  Data Pkts 9
*Jan  1 00:44:37.299:Rudpv1 Rcvd:Pkts 10,  Data Bytes 237,  Data Pkts 9
*Jan  1 00:44:37.299:Rudpv1 Discarded:0,  Retransmitted 0
*Jan  1 00:44:37.299:
*Jan  1 00:44:47.299:
*Jan  1 00:44:47.299:Rudpv1 Sent:Pkts 11,  Data Bytes 236,  Data Pkts 9
*Jan  1 00:44:47.299:Rudpv1 Rcvd:Pkts 11,  Data Bytes 236,  Data Pkts 9
*Jan  1 00:44:47.299:Rudpv1 Discarded:0,  Retransmitted 0
*Jan  1 00:44:47.299:
```

The following example shows output for the **debug rudpv1 retransmit** command:

```
Router# debug rudpv1 retransmit
Rudpv1:Turning retransmit/softreset debugging on
*Jan  1 00:52:59.799:Retrans timer, set to ack 199
*Jan  1 00:52:59.903:Retrans timer, set to ack 200
*Jan  1 00:53:00.003:Retrans timer, set to ack 201
*Jan  1 00:53:00.103:Retrans timer, set to ack 202
*Jan  1 00:53:00.203:Retrans timer, set to ack 203
*Jan  1 00:53:00.419:Retrans timer, set to ack 97
*Jan  1 00:53:00.503:Retrans handler fired, 203
*Jan  1 00:53:00.503:Retrans:203:205:
*Jan  1 00:53:00.503:
*Jan  1 00:53:00.607:Retrans timer, set to ack 207
*Jan  1 00:53:00.907:Retrans timer, set to ack 210
*Jan  1 00:53:01.207:Retrans handler fired, 210
*Jan  1 00:53:01.207:Retrans:210:211:212:
*Jan  1 00:53:01.207:
*Jan  1 00:53:01.207:Retrans timer, set to ack 213
*Jan  1 00:53:01.311:Retrans timer, set to ack 214
*Jan  1 00:53:01.419:Retrans timer, set to ack 98
*Jan  1 00:53:01.611:Retrans timer, set to ack 215
*Jan  1 00:53:01.711:Retrans timer, set to ack 218
*Jan  1 00:53:01.811:Retrans timer, set to ack 219
*Jan  1 00:53:01.911:Retrans timer, set to ack 220
*Jan  1 00:53:02.011:Retrans timer, set to ack 221
*Jan  1 00:53:02.311:Retrans handler fired, 221
*Jan  1 00:53:02.311:Retrans:221:
*Jan  1 00:53:02.311:
*Jan  1 00:53:02.311:Retrans timer, set to ack 222
*Jan  1 00:53:02.415:Retrans timer, set to ack 225
```

The following example shows output for the **debug rudpv1 segment** command:

```
Router# debug rudpv1 segment
Rudpv1:Turning segment debugging on
*Jan  1 00:41:36.359:Rudpv1: (61F72DAC) Rcvd ACK 61..198 (32)
*Jan  1 00:41:36.359:Rudpv1: (61F72DAC) Send ACK 199..61 (32)
*Jan  1 00:41:36.459:Rudpv1: (61F72DAC) Rcvd ACK 62..199 (8)
*Jan  1 00:41:36.459:Rudpv1: (61F72DAC) Rcvd ACK 62..199 (32)
*Jan  1 00:41:36.459:Rudpv1: (61F72DAC) Send ACK 200..62 (32)
*Jan  1 00:41:36.559:Rudpv1: (61F72DAC) Rcvd ACK 63..200 (32)
*Jan  1 00:41:36.559:Rudpv1: (61F72DAC) Send ACK 201..63 (32)
*Jan  1 00:41:36.659:Rudpv1: (61F72DAC) Rcvd ACK 64..201 (32)
*Jan  1 00:41:36.659:Rudpv1: (61F72DAC) Send ACK 202..64 (32)
*Jan  1 00:41:36.759:Rudpv1: (61F72DAC) Rcvd ACK 65..202 (32)
*Jan  1 00:41:36.759:Rudpv1: (61F72DAC) Send ACK 203..65 (32)
*Jan  1 00:41:36.859:Rudpv1: (61F72DAC) Rcvd ACK 66..202 (32)
*Jan  1 00:41:36.859:Rudpv1: (61F72DAC) Send ACK 204..66 (32)
*Jan  1 00:41:36.959:Rudpv1: (61F72DAC) Rcvd ACK 67..202 (32)
*Jan  1 00:41:36.959:Rudpv1: (61F72DAC) Rcvd ACK EAK 68..202 (9)
*Jan  1 00:41:36.959:Rudpv1: (61F72DAC) Send ACK 203..67 (32)
*Jan  1 00:41:36.963:Rudpv1: (61F72DAC) Send ACK 205..67 (32)
*Jan  1 00:41:36.963:Rudpv1: (61F72DAC) Rcvd ACK 68..204 (8)
*Jan  1 00:41:37.051:Rudpv1: (61F72B6C) Send ACK NUL 118..96 (8)
*Jan  1 00:41:37.051:Rudpv1: (61F72B6C) Rcvd ACK 97..118 (8)
*Jan  1 00:41:37.059:Rudpv1: (61F72DAC) Rcvd ACK 68..205 (32)
*Jan  1 00:41:37.063:Rudpv1: (61F72DAC) Send ACK 206..68 (32)
*Jan  1 00:41:37.263:Rudpv1: (61F72DAC) Rcvd ACK 70..206 (32)
*Jan  1 00:41:37.363:Rudpv1: (61F72DAC) Send ACK EAK 207..68 (9)
*Jan  1 00:41:37.363:Rudpv1: (61F72DAC) Rcvd ACK 71..206 (32)
*Jan  1 00:41:37.363:Rudpv1: (61F72DAC) Rcvd ACK 69..206 (32)
*Jan  1 00:41:37.363:Rudpv1: (61F72DAC) Send ACK 207..71 (8)
*Jan  1 00:41:37.363:Rudpv1: (61F72DAC) Send ACK 207..71 (32)
```

```
*Jan  1 00:41:37.363:Rudpv1: (61F72DAC) Send ACK 208..71 (32)
*Jan  1 00:41:37.363:Rudpv1: (61F72DAC) Send ACK 209..71 (32)
*Jan  1 00:41:37.367:Rudpv1: (61F72DAC) Rcvd ACK 72..209 (8)
*Jan  1 00:41:37.463:Rudpv1: (61F72DAC) Rcvd ACK 72..209 (32)
*Jan  1 00:41:37.463:Rudpv1: (61F72DAC) Send ACK 210..72 (32)
*Jan  1 00:41:37.563:Rudpv1: (61F72DAC) Rcvd ACK 73..210 (32)
*Jan  1 00:41:37.563:Rudpv1: (61F72DAC) Send ACK 211..73 (32)
```

The following example shows output for the **debug rudpv1 signal** command:

```
Router# debug rudpv1 signal
Rudpv1:Turning signal debugging on
*Jan  1 00:39:59.551:Rudpv1:Sent CONN_FAILED to connID 61F72DAC, sess 33
*Jan  1 00:39:59.551:
*Jan  1 00:39:59.551:Rudpv1:Sent CONN_TRANS_STATE to connID 61F72B6C, sess 34
*Jan  1 00:39:59.551:
*Jan  1 00:39:59.551:Rudpv1:Sent CONN_TRANS_STATE to connID 61F72DAC, sess 33
*Jan  1 00:39:59.551:
*Jan  1 00:39:59.551:Rudpv1:Sent CONN_OPEN to connID 61F72B6C, sess 34

*Jan  1 00:39:59.551:Rudpv1:Sent AUTO_RESET to connID 61F72DAC, sess 33
*Jan  1 00:39:59.551:
*Jan  1 00:40:00.739:%LINK-5-CHANGED:Interface FastEthernet0, changed state
to administratively down
*Jan  1 00:40:01.739:%LINEPROTO-5-UPDOWN:Line protocol on Interface
FastEthernet0, changed state to down
*Jan  1 00:40:04.551:Rudpv1:Sent CONN_RESET to connID 61F72DAC, sess 33
*Jan  1 00:40:04.551:
*Jan  1 00:40:05.051:Rudpv1:Clearing conn rec values, index 2, connid
61F72DAC
*Jan  1 00:40:10.051:Rudpv1:Sent CONN_RESET to connID 61F72DAC, sess 33
*Jan  1 00:40:10.051:
*Jan  1 00:40:10.551:Rudpv1:Clearing conn rec values, index 2, connid
61F72DAC
*Jan  1 00:40:15.551:Rudpv1:Sent CONN_RESET to connID 61F72DAC, sess 33
*Jan  1 00:40:15.551:
*Jan  1 00:40:16.051:Rudpv1:Clearing conn rec values, index 2, connid
61F72DAC

*Jan  1 00:40:21.051:Rudpv1:Sent CONN_RESET to connID 61F72DAC, sess 33
*Jan  1 00:40:21.051:
*Jan  1 00:40:21.551:Rudpv1:Clearing conn rec values, index 2, connid
61F72DAC
*Jan  1 00:40:25.587:%LINK-3-UPDOWN:Interface FastEthernet0, changed state
to up
*Jan  1 00:40:26.551:Rudpv1:Sent CONN_RESET to connID 61F72DAC, sess 33
*Jan  1 00:40:26.551:
*Jan  1 00:40:26.587:%LINEPROTO-5-UPDOWN:Line protocol on Interface
FastEthernet0, changed state to up
*Jan  1 00:40:27.051:Rudpv1:Clearing conn rec values, index 2, connid
61F72DAC
*Jan  1 00:40:28.051:Rudpv1:Sent CONN_OPEN to connID 61F72DAC, sess 33
```

The following example shows output for the **debug rudpv1 state** command:

```
Router# debug rudpv1 state
Rudpv1:Turning state debugging on

*Jan  1 00:38:37.323:Rudpv1: (61F72DAC) State Change:OPEN -> CONN_FAILURE
*Jan  1 00:38:37.323:Rudpv1: (61F72B6C) State Change:OPEN -> TRANS_STATE
*Jan  1 00:38:37.323:Rudpv1: (61F72DAC) State Change:CONN_FAILURE ->
TRANS_STATE
*Jan  1 00:38:37.323:Rudpv1: (61F72B6C) State Change:TRANS_STATE -> OPEN
*Jan  1 00:38:37.323:Rudpv1: (61F72DAC) State Change:TRANS_STATE -> SYN_SENT
```

```
*Jan  1 00:38:37.455:%LINK-5-CHANGED:Interface FastEthernet0, changed state
to administratively down
*Jan  1 00:38:38.451:%LINEPROTO-5-UPDOWN:Line protocol on Interface
FastEthernet0, changed state to down
*Jan  1 00:38:42.323:Rudpv1: (61F72DAC) State Change:SYN_SENT -> CLOSED
*Jan  1 00:38:42.823:Rudpv1: (61F72DAC) State Change:INACTIVE -> SYN_SENT
*Jan  1 00:38:47.823:Rudpv1: (61F72DAC) State Change:SYN_SENT -> CLOSED
*Jan  1 00:38:48.323:Rudpv1: (61F72DAC) State Change:INACTIVE -> SYN_SENT
*Jan  1 00:38:53.323:Rudpv1: (61F72DAC) State Change:SYN_SENT -> CLOSED
*Jan  1 00:38:53.823:Rudpv1: (61F72DAC) State Change:INACTIVE -> SYN_SENT
*Jan  1 00:38:56.411:%LINK-3-UPDOWN:Interface FastEthernet0, changed state
to up
*Jan  1 00:38:57.411:%LINEPROTO-5-UPDOWN:Line protocol on Interface
FastEthernet0, changed state to up
*Jan  1 00:38:57.823:Rudpv1: (61F72DAC) State Change:SYN_SENT -> OPEN
```

The following example shows output for the **debug rudpv1 timer** command:

```
Router# debug rudpv1 timer
Rudpv1:Turning timer debugging on
*Jan  1 00:53:40.647:Starting Retrans timer for connP = 61F72B6C, delay = 300
*Jan  1 00:53:40.647:Stopping SentList timer for connP = 61F72B6C
*Jan  1 00:53:40.747:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
*Jan  1 00:53:40.747:Stopping Retrans timer for connP = 61F72B6C
*Jan  1 00:53:40.747:Starting Retrans timer for connP = 61F72B6C, delay = 300
*Jan  1 00:53:40.747:Stopping SentList timer for connP = 61F72B6C
*Jan  1 00:53:40.847:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
*Jan  1 00:53:40.847:Stopping Retrans timer for connP = 61F72B6C
*Jan  1 00:53:40.847:Starting Retrans timer for connP = 61F72B6C, delay = 300
*Jan  1 00:53:40.847:Stopping SentList timer for connP = 61F72B6C
*Jan  1 00:53:40.947:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
*Jan  1 00:53:40.947:Stopping Retrans timer for connP = 61F72B6C
*Jan  1 00:53:40.947:Starting Retrans timer for connP = 61F72B6C, delay = 300
*Jan  1 00:53:40.947:Stopping SentList timer for connP = 61F72B6C
*Jan  1 00:53:41.047:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
*Jan  1 00:53:41.147:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
*Jan  1 00:53:41.151:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
*Jan  1 00:53:41.151:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
*Jan  1 00:53:41.151:Stopping Retrans timer for connP = 61F72B6C
*Jan  1 00:53:41.151:Starting SentList timer for connP = 61F72B6C, delay = 300
*Jan  1 00:53:41.419:Timer Keepalive (NullSeg) triggered for conn = 61F72DAC
*Jan  1 00:53:41.419:Starting Retrans timer for connP = 61F72DAC, delay = 300
*Jan  1 00:53:41.419:Stopping SentList timer for connP = 61F72DAC
*Jan  1 00:53:41.419:Starting NullSeg timer for connP = 61F72DAC, delay = 1000
*Jan  1 00:53:41.419:Stopping Retrans timer for connP = 61F72DAC
*Jan  1 00:53:41.451:Timer SentList triggered for conn = 61F72B6C
*Jan  1 00:53:41.451:Starting SentList timer for connP = 61F72B6C, delay = 300
*Jan  1 00:53:41.451:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
*Jan  1 00:53:41.451:Stopping SentList timer for connP = 61F72B6C
*Jan  1 00:53:41.551:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
*Jan  1 00:53:41.551:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
*Jan  1 00:53:41.551:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
*Jan  1 00:53:41.551:Starting NullSeg timer for connP = 61F72B6C, delay = 1000
```

The following example shows output for the **debug rudpv1 transfer** command:

```
Router# debug rudpv1 transfer
Rudpv1:Turning transfer debugging on
*Jan  1 00:37:30.567:Rudpv1:Send TCS, connId 61F72B6C, old connId 61F72DAC
*Jan  1 00:37:30.567:Rudpv1:Initiate transfer state, old conn 61F72DAC to
new conn 61F72B6C
*Jan  1 00:37:30.567:Rudpv1:Old conn send window 51 .. 52
*Jan  1 00:37:30.567:Rudpv1:New conn send window 255 .. 2
*Jan  1 00:37:30.567:Rudpv1:Rcvd TCS 142, next seq 142
```

```
*Jan  1 00:37:30.567:Rudpv1:Rcv'ing trans state, old conn 61F72DAC to new
conn 61F72B6C
*Jan  1 00:37:30.567:Rudpv1:Seq adjust factor 148
*Jan  1 00:37:30.567:Rudpv1:New rcvCur 142
*Jan  1 00:37:30.567:Rudpv1:Send transfer state, old conn 61F72DAC to new
conn 61F72B6C
*Jan  1 00:37:30.567:Rudpv1:Send TCS, connId 61F72B6C, old connId 61F72DAC,
seq adjust 208, indication 0
*Jan  1 00:37:30.567:Rudpv1:Transfer seg 51 to seg 3 on new conn
*Jan  1 00:37:30.567:Rudpv1:Finishing transfer state, old conn 61F72DAC to
new conn 61F72B6C
*Jan  1 00:37:30.567:Rudpv1:Send window 2 .. 4
```

Related Commands

Command	Description
clear rudpv1 statistics	Clears RUDP statistics and failure counters.
show rudpv1	Displays RUDP failures, parameters, and statistics.

group auto-reset

To specify the maximum number of auto-resets for a session group, use the **group auto-reset** command in backhaul session manager configuration mode. To restore the default number, use the **no** form of this command.

group *grp-name* **auto-reset** *count*

no group *grp-name* **auto-reset**

Caution Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

grp-name	Session-group name.
count	Maximum number of auto-resets before the connection is considered failed. The range is from 0 to 255. The default is 5.

Defaults 5 auto-resets

Command Modes Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example specifies a maximum of six auto-resets for session group 5:

```
Router(config-bsm)# group group5 auto-reset 6
```

Related Commands

Command	Description
group cumulative-ack	Configures the maximum number of segments that are received in a session group before an acknowledgment is sent.
group out-of-sequence	Configures the maximum out-of-sequence segments that are received before an error acknowledgment (EACK) is sent.
group receive	Configures the maximum number of segments in the receive window of a session group.
group retransmit	Configures the maximum number of retransmits.

group cumulative-ack

To configure the maximum number of segments that are received in a session group before an acknowledgment is sent, use the **group cumulative-ack** command in backhaul session manager configuration mode. To restore the default number, use the **no** form of this command.

group *grp-name* **cumulative-ack** *count*

no group *grp-name* **cumulative-ack**

Caution Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

grp-name	Session-group name.
count	Maximum number of segments received before acknowledgment. The range is from 0 to 255. The default is 3.

Defaults 3 segments

Command Modes Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples The following example configures session group 5 to send acknowledgment after four segments have been received:

```
Router(config-bsm)# group group5 cumulative-ack 4
```

Related Commands

Command	Description
group auto-reset	Specifies the maximum number of auto-resets for a session group.
group out-of-sequence	Configures the maximum out-of-sequence segments that are received before an error acknowledgment (EACK) is sent.
group receive	Configures the maximum number of segments in the receive window of a session group.
group retransmit	Configures the maximum number of retransmits.

group out-of-sequence

To configure the maximum number of out-of-sequence segments that can be received in a session group before an acknowledgment (ACK) is sent, use the **group out-of-sequence** command in backhaul session manager configuration mode. To restore the default number, use the **no** form of this command.

group *grp-name* **out-of-sequence** *count*

no group *grp-name* **out-of-sequence**

Caution Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

grp-name	Session-group name.
count	Maximum number of out-of-sequence segments that can be received in a session-group before an ACK is sent. The range is from 0 to 255. The default is 3.

Defaults

3 segments

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example configures session group 5 to send acknowledgment after four out-of-sequence segments have been received:

```
Router(config-bsm)# group group5 out-of-sequence 4
```

Related Commands

Command	Description
group auto-reset	Specifies the maximum number of auto-resets for a session group.
group cumulative-ack	Configures the maximum number of segments that are received in a session group before an acknowledgment is sent.
group receive	Configures the maximum number of segments in the receive window of a session group.
group retransmit	Configures the maximum number of retransmits.

group receive

To configure the maximum number of segments in the receive window of a session group, use the **group receive** command in backhaul session manager configuration mode. To restore the default number, use the **no** form of this command.

group *grp-name* **receive** *count*

no group *grp-name* **receive**

Caution Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

grp-name	Session-group name.
count	Maximum number of segments in the receive window of the media gateway. This is the maximum number of segments the media gateway is allowed to receive before it sends an ACK. The range is from 1 to 64. The default is 32.

Defaults

32 segments

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example configures session group 5 to receive a maximum of 10 segments before the Cisco VSC3000 receives an acknowledgment:

```
Router(config-bsm)# group group5 receive 10
```

Related Commands

Command	Description
group auto-reset	Specifies the maximum number of auto-resets for a session group.
group cumulative-ack	Configures the maximum number of segments that are received in a session group before an acknowledgment is sent.
group out-of-sequence	Configures the maximum number of out-of-sequence segments that are received before an ACK is sent.
group retransmit	Configures the maximum number of retransmits.

group retransmit

To configure the maximum number of retransmits in a session group, use the **group retransmit** command in backhaul session manager configuration mode. To restore the default number, use the **no** form of this command.

group *grp-name* **retransmit** *count*

no group *grp-name* **retransmit**

Caution Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

grp-name	Session-group name.
count	Maximum number of retransmits allowed in a session group. The range is from 0 to 255. The default is 2.

Defaults

2 retransmits

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example configures session group 5 to allow as many as 3 retransmits:

```
Router(config-bsm)# group group5 retrans 3
```

Related Commands

Command	Description
group auto-reset	Specifies the maximum number of auto-resets for a session group.
group cumulative-ack	Configures the maximum number of segments that are received in a session group before an acknowledgment is sent.
group out-of-sequence	Configures the maximum number of out-of-sequence segments that are received before an ACK is sent.
group receive	Configures the maximum number of segments in the receive window of a session group.

group set

To create a session-group and associate it with a specified session-set, use the **group** command in backhaul session manager configuration mode. To delete the group, use the **no** form of this command.

group *grp-name* **set** *set-name*

no group *grp-name*

Syntax Description

grp-name	Session-group name.
set-name	Session-set name.

Defaults

No default behavior or values.

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example associates session-group **group5** with session-set **set1**:

```
Router(config-bsm)# group group5 set set1
```

Related Commands

Command	Description
group auto-reset	Specifies the maximum number of auto-resets for a session group.
group cumulative-ack	Configures the maximum number of segments that are received in a session group before an acknowledgment is sent.
group out-of-sequence	Configures the maximum out-of-sequence segments that are received before an error acknowledgment (EACK) is sent.
group receive	Configures the maximum number of segments in the receive window of a session group.
group retransmit	Configures the maximum number of retransmits.
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer retransmit	Configures retransmission timeout.
group timer transfer	Configures state transfer timeout.
group auto-reset	Specifies the maximum number of auto-resets for a session group.

group timer cumulative-ack

To configure the maximum number of milliseconds Reliable User Datagram Protocol (RUDP) delays before sending an acknowledgment for a received segment, use the **group timer cumulative-ack** command in backhaul session manager configuration mode. To restore the default value, use the **no** form of this command.

group *group-name* **timer cumulative-ack** *time*

no group *group-name* **timer cumulative-ack**

Caution Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

group-name	Session-group name.
time	Number of milliseconds that RUDP delays before sending an acknowledgment for a received segment. The range is from 100 to 65535. The default is 100.

Defaults 100 milliseconds

Command Modes Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples The following example specifies 325 milliseconds as the maximum acknowledgment delay for session group 5:

```
Router(config-bsm)# group group5 timer cumulative-ack 325
```

Related Commands

Command	Description
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer retransmit	Configures retransmission timeout.
group timer transfer	Configures state transfer timeout.

group timer keepalive

To configure the number of milliseconds that Reliable User Datagram Protocol (RUDP) waits before sending a keepalive segment, use the **group timer keepalive** command in backhaul session manager configuration mode. To restore the default value, use the **no** form of this command.

group *grp-name* **timer keepalive** *time*

no group *grp-name* **timer keepalive**

Caution Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

grp-name	Session-group name.
time	Number of milliseconds before RUDP sends a keepalive segment when no RUDP packets are received or sent. The range is from 100 to 65535. The default is 1000.

Defaults

1000 milliseconds

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example configures RUDP to send keepalive segments if no RUDP packets are received or sent for 2.5 seconds (2500 milliseconds) in session group 5.

```
Router(config-bsm)# group group5 timer keepalive 2500
```

Related Commands

Command	Description
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer retransmit	Configures retransmission timeout.
group timer transfer	Configures state transfer timeout.

group timer retransmit

To configure the number of milliseconds that Reliable User Datagram Protocol (RUDP) waits to receive an acknowledgment for a segment before retransmitting the segment, use the **group timer retransmit** command in backhaul session manager configuration mode. To restore the default value, use the **no** form of this command.

group *grp-name* **timer retransmit** *time*

no group *grp-name* **timer retransmit**

Caution Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

grp-name	Session-group name.
time	Number of milliseconds RUDP waits before retransmitting the segment. The range is from 100 to 65535. The default is 300.

Defaults

300 milliseconds

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Usage Guidelines

The retransmit timer must be greater than the cumulative-ack timer set using the **group timer cumulative-ack** command.

Examples

The following example sets a retransmit time of 650 milliseconds for session group 5:

```
Router(config-bsm)# group group5 timer retransmit 650
```

Related Commands

Command	Description
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer transfer	Configures state transfer timeout.

group timer transfer

To configure the number of milliseconds Reliable User Datagram Protocol (RUDP) will wait for a transfer request, use the **group timer transfer** command in backhaul session manager configuration mode. To restore the default value, use the **no** form of this command.

group *grp-name* **timer transfer** *time*

no group *grp-name* **timer transfer**

Caution Do not change this parameter unless instructed to do so by Cisco technical support. There are relationships between group parameters that can cause sessions to fail if not set correctly.

Syntax Description

grp-name	Session-group name.
time	The number of milliseconds RUDP waits to receive a selection of a new session from the application during a transfer state. The range is from 0 to 65535. The default is 600.

Defaults

600 milliseconds

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example sets a state transfer time of 1800 milliseconds for session group 5:

```
Router(config-bsm)# group group5 timer transfer-state 1800
```

Related Commands

Command	Description
group timer cumulative-ack	Configures cumulative acknowledgment timeout.
group timer keepalive	Configures keepalive (or null segment) timeout.
group timer retransmit	Configures retransmission timeout.

isdn bind-L3

To configure an ISDN D-channel serial interface for signaling backhaul and associate it with a session-set, use the **isdn bind-L3** interface configuration command. To disable signaling backhaul on an ISDN D-channel serial interface, use the **no** form of this command.

isdn bind-L3 *set-name*

no isdn bind-L3

Note In the command, the capital "L" is shown here for clarity. You can enter a lowercase "l".

Syntax Description

set-name	Specifies the session-set with which you are associating this D-channel interface.

Defaults

The ISDN D-channel is not configured for signaling backhaul and not associated with a session-set.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example configures T1 signaling channel serial 0:23 for signaling backhaul and associates the D-channel with the session-set named Set1:

```
Router(config)# interface s0:23
Router(config-if)# isdn bind-L3 set1
Router(config-if)# exit
```

The following example configures E1 signaling channel serial 0:15 for signaling backhaul and associates the D-channel with the session-set named Set3:

```
Router(config)# interface s0:15
Router(config-if)# isdn bind-L3 set3
Router(config-if)# exit
```

isdn protocol-emulate

To configure an ISDN D-channel serial interface to emulate the network side or user side protocol of an ISDN configuration for a Net5 switch type, use the **isdn protocol-emulate** command in interface configuration mode. To restore the default emulation configuration, use the **no** form of this command.

isdn protocol-emulate {**network** | **user**}

no isdn protocol-emulate

Syntax Description

network	The network side of an ISDN configuration.
user	The user side of an ISDN configuration.

Defaults

ISDN D-channel serial interfaces emulate the user side protocol of an ISDN configuration for a Net5 switch type.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Usage Guidelines

The current ISDN signaling stack can emulate the ISDN network side, but it does not conform to the specifications of the various switch types when emulating the network side. This command enables the Cisco IOS software to replicate the public switched network interface to a PBX. This feature is supported only for the PRI Net5 switch type.

Examples

The following example configures T1 signaling channel serial 0:23 (configured for Net5) to emulate the network-side ISDN:

```
Router(config)# interface s0:23
Router(config-if)# isdn protocol-emulate network
Router(config-if)# exit
```

The following example configures E1 signaling channel serial 0:15 (configured for Net5) to emulate the network-side ISDN:

```
Router(config)# interface s0:15
Router(config-if)# isdn protocol-emulate network
Router(config-if)# exit
```

session group

To add a transport session to a specified session-group, use the **session group** command in backhaul session manager configuration mode. To delete a transport session from a specified session-group, use the **no** form of this command.

session group *group-name remote_ip remote_port local_ip local_port priority*

no session group *group-name remote_ip remote_port local_ip local_port*

Syntax Description

group-name	Name of the session-group to which this session is added.
remote_ip	IP address of the Cisco VSC3000 server at the remote end of this backhaul link.
remote_port	UDP port number on the Cisco VSC3000 server at the remote end of this backhaul link. The range is from 1024 to 9999.
local_ip	IP address of the media gateway port used for signaling backhaul.
local_port	UDP port number of the media gateway port used for signaling backhaul. The range is from 1024 to 9999.
priority	Priority of this session within its session-group. The range is from 0 to 9999; 0 is the highest priority.

Command Types

No default behavior or values.

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Usage Guidelines

The Cisco VSC3000 server is assumed to be located on a remote machine.

Examples

The following example adds a transport session to session-group “group 5” and specifies the remote and local IP addresses and ports, and specifies a priority of 1 within the session group:

```
Router(config-bsm)# session group group5 192.168.2.72 5555 172.18.72.198 5555 1
```

set

To create a fault-tolerant or non-fault-tolerant session-set with the client or server option, use the **set** command in backhaul session manager configuration mode. To delete a session-set, use the **no** form of this command.

set *set-name* {**client** | **server**} {**ft** | **nft**}

no set *set-name*

Syntax Description

set-name	Session-set name.
client	The session-set operates as a client. Select this option for signaling backhaul.
server	The session-set operates as a server.
ft	Fault-tolerant operation. Select fault-tolerant if this session-set can contain more than one session-group, with each session-group connecting the gateway to a different Cisco VSC3000. Fault-tolerance allows the system to operate properly if a session-group in the session-set fails.
nft	Non-fault-tolerant operation. Select non-fault-tolerant if this session-set contains only one session-group (which connects the gateway to a single Cisco VSC3000).

Defaults

No session-set is configured.

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Usage Guidelines

Multiple session-groups can be associated with a session-set.

For signaling backhaul, session-sets should be configured to operate as clients.

A session-set cannot be deleted unless all session-groups associated with the session-set are deleted first.

Examples

The following example creates a session-set named “Set1”, operating as a client and fault-tolerant:

```
Router(config-bsm)# set set1 client ft
```

show backhaul-session-manager group

To display status, statistics, or configuration for session-groups, use the **show backhaul-session-manager group** command in privileged EXEC mode.

show backhaul-session-manager group {**status** | **stats** | **cfg**} {**all** | **name** *group-name*}

Syntax Description

status	Status.
stats	Statistics.
cfg	Configuration.
all	Displays output for all configured session-groups.
name	Displays output for the designated session-group only.
group-name	Name of a session-group.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example displays statistics for all session-groups:

```
Router# show backhaul-session-manager group stats all

Session-Group grp1 statistics
   Successful Fail-Overs      :0
   Un-Successful Fail-Over attempts:0
   Active Pkts receive count  :0
   Standby Pkts receive count :0
   Total PDUs dispatch err    :0
```

The following example displays the current configuration for all session-groups:

```
Router# show backhaul-session-manager group cfg all
Session-Group
   Group Name :grp1
   Set Name   :set1
   Sessions   :3
    Dest:10.5.0.3 8304  Local:10.1.2.15 8304  Priority:0
    Dest:10.5.0.3 8300  Local:10.1.2.15 8300  Priority:2
    Dest:10.5.0.3 8303  Local:10.1.2.15 8303  Priority:2
    RUDP Options
      timer cumulative ack :100
      timer keepalive      :1000
      timer retransmit     :300
      timer transfer state :2000
      receive max          :32
      cumulative ack max   :3
      retrans max          :2
      out-of-sequence max  :3
      auto-reset max       :5
```

The following example displays the current state of all session-groups. This group named “grp1” belongs to the set named “set1”.

The Status is either Group-OutOfService (no session in the session-group has been established) or Group-InService (at least one session in the session-group has been established).

The Status (use) is either Group-Standby (the Cisco VSC3000 connected to the other end of this session-group goes into standby mode), Group-Active (the Cisco VSC3000 connected to the other end of this session-group is the active Cisco VSC3000), or Group-None (the Cisco VSC3000 has not declared its intent).

```
Router# show backhaul-session-manager group status all

Session-Group
Group Name   :grp1
   Set Name     :set1
   Status       :Group-OutOfService
   Status (use) :Group-None
```

Related Commands

Command	Description
show backhaul-session- manager set	Displays session-groups associated with a specific or all session-sets.
show backhaul-session- manager session	Displays status, statistics, or configuration of sessions.

show backhaul-session-manager session

To display various information for about a session or sessions, use the **show backhaul-session-manager session** command in privileged EXEC mode.

show backhaul-session-manager session {**all** | **ip** *ip-address*}

Syntax Description

all	Information is displayed about all available sessions.
ip	Information is displayed about the session associated with this IP address only.
ip-address	The IP address of the local or remote session.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example displays information for all available sessions.

The State is OPEN (the connection is established), OPEN_WAIT (the connection is waiting for establishment), OPEN_XFER (session failover is in progress for this session, which is a transient state), or CLOSE (this session is down, also a transient state).

The Use-status field indicates whether PRI signaling traffic is being transported over this session. The field is either OOS (this session is not being used to transport signaling traffic) or IS (this session is being used to transport all PRI signaling traffic). OOS does not indicate if the connection is established and IS indicates that the connection is established.

```
Router# show backhaul-session-manager session all

Session information --
Session-id:35
  Group:grp1  /*this session belongs to the group named 'grp1' */
Configuration:
     Local:10.1.2.15      , port:8303
    Remote:10.5.0.3       , port:8303
  Priority:2
  RUDP Option:Client, Conn Id:0x2
State:
  Status:OPEN_WAIT, Use-status:OOS,  /*see explanation below */
Statistics:
  # of resets:0
  # of auto_resets 0
  # of unexpected RUDP transitions (total) 0
  # of unexpected RUDP transitions (since last reset) 0
  Receive pkts -  Total:0 , Since Last Reset:0
  Recieve failures -  Total:0 ,Since Last Reset:0
  Transmit pkts - Total:0, Since Last Reset:0
  Transmit Failures (PDU Only)
         Due to Blocking (Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  Transmit Failures (NON-PDU Only)
         Due to Blocking(Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  RUDP statistics
         Open failures:0
         Not ready failures:0
         Conn Not Open failures:0
         Send window full  failures:0
         Resource unavailble failures:0
         Enqueue failures:0
```

Related Commands

Command	Description
show backhaul-session-manager set	Displays session-groups associated with a specified or all session-sets.
show backhaul-session-manager group	Displays status, statistics, or configuration of a specified or all session-groups.

show backhaul-session-manager set

To display session-groups associated with a specified session-set or all session-sets, use the **show backhaul-session-manager set** command in privileged EXEC mode.

show backhaul-session-manager set {**all** | **name** *session-set-name*}

Syntax Description

all	All available session-sets are displayed.
name	A specified session-set is displayed.
session-set-name	Specifies a session-set to display.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example shows session-groups associated with all session-sets:

```
Router# show backhaul-session-manager set all
```

Related Commands

Command	Description
show backhaul-session-manager group	Displays status, statistics, or configuration of a specified session-group or all session-groups.
show backhaul-session-manager session	Displays status, statistics, or configuration of a specified session or all sessions.

show rudpv1

To display Reliable User Datagram Protocol (RUDP) information, use the **show rudpv1** command in privileged EXEC mode.

show rudpv1 {**failures** | **parameters** | **statistics**}

Syntax Description

failures	RUDP failure statistics.
parameters	RUDP connection parameters.
statistics	RUDP internal statistics.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300 access server.
12.2(4)T	This command was first supported on the Cisco 2600, Cisco 3600, and Cisco MC3810 series.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
12.2(11)T	This command was integrated into the Cisco IOS Release 12.2(11)T and implemented on the Cisco VG200.
12.2(11)ZC	This command was integrated in to the Cisco IOS Release 12.2(11)ZC and implemented on the Catalyst 6500 series and Cisco 7600 series CMM.

Examples

The following example shows output for **show rudpv1 failures**:

```
Router# show rudpv1 failures

**** RUDPV1 Failure Stats ****

CreateBufHdrsFailure       0
CreateConnRecsFailure      0
CreateEventQueueFailure    0
OsSpecificInitFailure      0

NotReadyFailures           0
OptionNotSupportedFailures 0
InvalidOptionFailures      0
OptionRequiredFailures     0
GetConnRecFailures         0
InvalidConnFailures        0
EventUnavailFailures       0

GetConnRecFailures         0
FindConnRecFailures        0
EmptyBufferSendFailures    0
```

```
BufferTooLargeFailures     0
ConnNotOpenFailures        0
SendWindowFullFailures     0
GetBufHdrSendFailures      0

SendInProgressFailures     0

GetDataBufFailures         0
GetBufHdrFailures          0

SendFailures               0
SendEackFailures           0
SendAckFailures            0
SendSynFailures            0
SendRstFailures            0
SendTcsFailures            0
SendNullFailures           0

TimerFailures              0
ApplQueueFailures          0
FailedRetransmits          0
IncomingPktsDropped        0
CksumErrors                0
UnknownRudpv1Events        0
InvalidVersion             0
InvalidNegotiation         0
```

The following example shows output for **show rudpv1 parameters**:

```
Router# show rudpv1 parameters

*** RUDPV1 Connection Parameters ***


Next Connection Id:61F72B6C,  Remote conn id 126000

  Conn State             OPEN
  Conn Type              ACTIVE
  Accept Negot params?   Yes
  Receive Window         32
  Send Window            32
  Receive Seg Size       384
  Send Seg Size          384

                     Requested     Negotiated
  Max Auto Reset         5             5
  Max Cum Ack            3             3
  Max Retrans            2             2
  Max OutOfSeq           3             3
  Cum Ack Timeout       100           100
  Retrans Timeout       300           300
  Null Seg Timeout     1000          1000
  Trans State Timeout  2000          2000
  Cksum type            Hdr           Hdr


Next Connection Id:61F72DAC,  Remote conn id 126218

  Conn State             OPEN
  Conn Type              ACTIVE
  Accept Negot params?   Yes
  Receive Window         32
  Send Window            32
  Receive Seg Size       384
```

```
  Send Seg Size          384

                     Requested     Negotiated
  Max Auto Reset         5             5
  Max Cum Ack            3             3
  Max Retrans            2             2
  Max OutOfSeq           3             3
  Cum Ack Timeout       100           100
  Retrans Timeout       300           300
  Null Seg Timeout      1000          1000
  Trans State Timeout   2000          2000
  Cksum type             Hdr           Hdr
```

The following example shows output for **show rudpv1 statistics**:

```
Router# show rudpv1 statistics

*** RUDPV1 Internal Stats ****

Connection ID:61F72B6C,   Current State:OPEN

RcvdInSeq                  647
RcvdOutOfSeq               95

AutoResets                 0
AutoResetsRcvd             0

TotalPacketsSent           1011
TotalPacketsReceived       958
TotalDataBytesSent         17808
TotalDataBytesReceived     17808
TotalDataPacketsSent       742
TotalDataPacketsReceived   742
TotalPacketsRetrans        117
TotalPacketsDiscarded      38

Connection ID:61F72DAC,   Current State:OPEN

RcvdInSeq                  0
RcvdOutOfSeq               0

AutoResets                 0
AutoResetsRcvd             0

TotalPacketsSent           75
TotalPacketsReceived       75
TotalDataBytesSent         0
TotalDataBytesReceived     0
TotalDataPacketsSent       0
TotalDataPacketsReceived   0
TotalPacketsRetrans        0
TotalPacketsDiscarded      0

Cumulative RudpV1 Statistics

NumCurConnections          2

RcvdInSeq                  652
RcvdOutOfSeq               95

AutoResets                 0
AutoResetsRcvd             0

TotalPacketsSent           1102
```

```
TotalPacketsReceived       1047
TotalDataBytesSent         18048
TotalDataBytesReceived     18048
TotalDataPacketsSent       752
TotalDataPacketsReceived   752
TotalPacketsRetrans        122
TotalPacketsDiscarded      38
```

Related Commands

Command	Description
clear rudpv1	Clears the statistics and failure counters.
show rudpv1	Shows RUDP statistics.

Glossary

backhaul—A scheme in which telephony signaling is reliably transported from a gateway to a Media Gateway Controller across a packet-switched network.

fault tolerance—The level of ability within a system to operate properly even if errors occur.

Layer 1—Physical Layer of the OSI Reference Model defined in ITU X.200, responsible for the electric signal being sent and received. This layer can be pictured 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 DS0 timeslot in the T1 is 64 kbps.

Layer 2—Datalink Layer of the OSI Reference Model defined in ITU X.200, responsible for point-to-point delivery of a Protocol Data Unit. Layer 2 protocols have two basic classes: reliable (delivery is guaranteed or an error is reported) and unreliable (delivery can occur without indication to the upper layers).

Layer 3—Network Layer of the OSI Reference Model defined in ITU X.200, responsible for the network routing and delivery of a message. Examples of Layer 3 protocols include X.25 Packet Layer Protocol and the Internet Protocol. Q.931 is not considered a Layer 3 protocol because its concern is not with routing and delivery of a message but with the message body itself.

MG—Media gateway. Terminates facilities (trunks), packetizes the pulse code modulation (PCM) stream into IP/ATM and forwards packets into the IP/ATM network. An MG performs these functions in reverse order on media streams flowing from the packet network to the PSTN.

MGC—Media gateway controller. Provides call control capability to handle signaling traffic from a variety of sources. An MGC also manages connections and resources of its media gateways. Also known as a call agent.

MGC switchover—The rerouting of signaling traffic by the signaling gateway as required (and requested by the MGCs) between related MGCs in the event of failure or unavailability of the currently used MGC. The traffic is rerouted from the primary MGC to the back-up MGC.

MGCP—Media Gateway Control Protocol.

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

PDU—Protocol Data Unit. OSI term for packet.

Q.931—Q Signaling. An inter-PBX signaling protocol for networking PBX supplementary services in a multiple-vendor or single-vendor environment.

RUDP—Cisco Reliable UDP.

session—An RUDP connection between two endpoints. An endpoint is defined by the IP address and the UDP port.

session-group—A logically ordered list of sessions based on priority of the sessions. All sessions in the session-group *must* be configured to connect the same physical machines.

Session-Manager—Manages all sessions in a specific client.

session-set—A collection of session-groups.

SG—Signaling gateway. Transmits and receives PSTN signaling at the edge of an IP/ATM network, and backhauls the signaling to a media gateway controller. The SG function can be coresident with the media gateway function in order to process signaling associated with line or trunk terminations that are controlled by the media gateway.

VSC—Virtual switch controller. The Cisco VSC3000 is an intelligent call agent with universal protocol support. Functioning as a “soft switch,” the Cisco VSC3000 controls the packet telephony network by directing calls across broadband, multi-service packet infrastructures. As a primary component within the Cisco Open Packet Telephony architecture, the Cisco VSC3000 utilizes open and widely recognized industry-standard protocols and interfaces.