

# show controllers voice

To display information about voice-related hardware, use the **show controllers voice** command in privileged EXEC mode.

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(5)XQ	This command was introduced on the Cisco 1750.

**Usage Guidelines** This command displays interface status information that is specific to voice-related hardware, such as the registers of the TDM switch, the host port interface of the digital signal processor (DSP), and the DSP firmware versions. The information displayed is generally useful only for diagnostic tasks performed by technical support.

**Examples** The following is sample output from this command:

```
Router# show controllers voice

EPIC Switch registers:
STDA 0xFF STDB 0xFF SARA 0xAD SARB 0xFF SAXA 0xFF SAXB 0x0 STCR 0x3F
MFAIR 0x3F
STAR 0x65 OMDR 0xE2 VNSR 0x0 PMOD 0x4C PBNR 0xFF POFD 0xF0 POFU 0x18
PCSR 0x1 PICM 0x0 CMD1 0xA0 CMD2 0x70 CBNR 0xFF CTAR 0x2 CBSR 0x20 CSCR
0x0

DSP 0 Host Port Interface:
HPI Control Register 0x202
InterfaceStatus 0x2A MaxMessageSize 0x80
RxRingBufferSize 0x6 TxRingBufferSize 0x9
pInsertRx 0x4 pRemoveRx 0x4 pInsertTx 0x6 pRemoveTx 0x6

Rx Message 0:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000: 0000 4AC7 5F08 91D1 0000 0000 7DF1 69E5 63E1 63E2
0020: 6E7C ED67 DE5D DB5C DC60 EC7E 6BE1 58D3 50CD 4DCE
0040: 50D2 5AE5 7868 DA52 CE4A C746 C647 C94B D25A EAF4
0060: 5DD7 4FCD 4ACA 4ACC 4FD3 5DE8 F769 DC58 D352 D253
0080: D65B E573 6CDF 59D3 4ECF 4FD0

Rx Message 1:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000: 0000 1CDD 3E48 3B74 0000 0000 3437 3D4C F0C8 BBB5
0020: B2B3 B7BF D25B 4138 3331 3339 435F CFBD B6B2 B1B4
```

```

0040:  BBC8 7E48 3B34 3131 363D 4FDE C3B9 B3B1 B3B8 C2DB
0060:  533F 3833 3235 3B48 71CC BDB7 B4B5 B8BF CF67 483D
0080:  3836 383C 455B DAC6 BDB9 B9BB

```

Rx Message 2:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:  0000 4AC8 5F08 9221 0000 0000 54DA 61F5 EF60 DA53
0020:  CF4F CD4E D256 DB63 FCEE 5FDA 55D1 50CF 4FD3 56D8
0040:  5DE1 6E7C EC60 DC59 D655 D456 D85D DF6A F4F4 69E2
0060:  5CDD 5BDC 5BDE 61E9 6DF1 FF76 F16D E96A E566 EA6A
0080:  EB6F F16D EF79 F776 F5F5 73F0

```

Rx Message 3:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:  0000 1CDE 3E48 3BC4 0000 0000 C0CC EC54 453E 3C3C
0020:  3F47 56F3 D1C7 C1BF C0C6 CEE1 6752 4A46 4648 4E59
0040:  6FE4 D6CF CDCE D2DA E57E 675E 5B5B 5E62 6B76 FCF6
0060:  F6FA 7D75 7373 7BF5 EAE1 DCDA DADD E6FE 6559 514D
0080:  4D4E 5563 EFD9 CDC8 C5C6 CAD1

```

Rx Message 4:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:  0000 4AC6 5F08 9181 0000 0000 DD5B DC5E E161 E468
0020:  FAFD 6CE1 5AD3 53D1 53D7 61EC EA59 CF4A C644 C344
0040:  CA4E D86C 60D0 48C2 3EBD 3CBD 3EC0 47CF 5976 DF4F
0060:  C945 C242 C146 C94E D668 73DB 54CE 4DCC 4DCE 53DB
0080:  64F9 ED63 DC59 DA58 DC5D E46C

```

Rx Message 5:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:  0000 1CDC 3E48 3B24 0000 0000 5B5B 5D62 6A76 FCF5
0020:  F5F9 7D78 7374 7CF5 EAE1 DDDA DBDD E7FE 6559 514E
0040:  4D4F 5663 EFD8 CDC8 C6C6 CAD1 E760 4E46 403F 4047
0060:  5173 D5C7 BFBC BCBE C5D4 6D4C 3F3B 3939 3D46 5ADB
0080:  C5BC B7B6 B8BD C8E8 4F3F 3835

```

Tx Message 0:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:  0000 4AC6 5F08 9181 0000 003C DD5B DC5E E161 E468
0020:  FAFD 6CE1 5AD3 53D1 53D7 61EC EA59 CF4A C644 C344
0040:  CA4E D86C 60D0 48C2 3EBD 3CBD 3EC0 47CF 5976 DF4F
0060:  C945 C242 C146 C94E D668 73DB 54CE 4DCC 4DCE 53DB
0080:  64F9 ED63 DC59 DA58 DC5D E46C

```

Tx Message 1:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:  0000 1CDC 3E48 3B24 0000 003C 5B5B 5D62 6A76 FCF5
0020:  F5F9 7D78 7374 7CF5 EAE1 DDDA DBDD E7FE 6559 514E
0040:  4D4F 5663 EFD8 CDC8 C6C6 CAD1 E760 4E46 403F 4047
0060:  5173 D5C7 BFBC BCBE C5D4 6D4C 3F3B 3939 3D46 5ADB
0080:  C5BC B7B6 B8BD C8E8 4F3F 3835

```

Tx Message 2:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:  0000 4AC7 5F08 91D1 0000 003C 7DF1 69E5 63E1 63E2
0020:  6E7C ED67 DE5D DB5C DC60 EC7E 6BE1 58D3 50CD 4DCE
0040:  50D2 5AE5 7868 DA52 CE4A C746 C647 C94B D25A EAF4
0060:  5DD7 4FCD 4ACA 4ACC 4FD3 5DE8 F769 DC58 D352 D253
0080:  D65B E573 6CDF 59D3 4ECF 4FD0

```

Tx Message 3:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:  0000 1CDD 3E48 3B74 0000 003C 3437 3D4C F0C8 BBB5
0020:  B2B3 B7BF D25B 4138 3331 3339 435F CFBD B6B2 B1B4

```

```

0040:  BBC8 7E48 3B34 3131 363D 4FDE C3B9 B3B1 B3B8 C2DB
0060:  533F 3833 3235 3B48 71CC BDB7 B4B5 B8BF CF67 483D
0080:  3836 383C 455B DAC6 BDB9 B9BB

```

## Tx Message 4:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:  0000 4AC8 5F08 9221 0000 003C 54DA 61F5 EF60 DA53
0020:  CF4F CD4E D256 DB63 FCEE 5FDA 55D1 50CF 4FD3 56D8
0040:  5DE1 6E7C EC60 DC59 D655 D456 D85D DF6A F4F4 69E2
0060:  5CDD 5BDC 5BDE 61E9 6DF1 FF76 F16D E96A E566 EA6A
0080:  EB6F F16D EF79 F776 F5F5 73F0

```

## Tx Message 5:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:  0000 1CDE 3E48 3BC4 0000 003C C0CC EC54 453E 3C3C
0020:  3F47 56F3 D1C7 C1BF C0C6 CEE1 6752 4A46 4648 4E59
0040:  6FE4 D6CF CDCE D2DA E57E 675E 5B5B 5E62 6B76 FCF6
0060:  F6FA 7D75 7373 7BF5 EAE1 DCDA DADD E6FE 6559 514D
0080:  4D4E 5563 EFD9 CDC8 C5C6 CAD1

```

## Tx Message 6:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:  0000 1CDA 3E48 3A84 0000 003C E75F 4E46 403F 4147
0020:  5174 D5C7 BFBC BCBE C5D4 6C4C 3F3B 3939 3D46 5BDA
0040:  C5BC B7B6 B8BD C8E9 4F3F 3834 3437 3D4C EEC8 BBB5
0060:  B2B3 B8BF D35A 4138 3331 3339 435F CEBD B6B1 B1B4
0080:  BBC9 7C48 3B34 3131 363D 4FDE

```

## Tx Message 7:

```

packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:  0000 4AC5 5F08 9131 0000 003C 66DE 66EB 67EE FE6E
0020:  F7E7 6B68 E068 EE6A DF5C DF62 EDF1 6FF2 7A78 67DC
0040:  5EDF 62E7 64E6 66E0 7071 EA69 F86E E260 DE5D E665
0060:  EB75 F0FB 6DE9 64E4 69E3 66EA 67E9 6DF9 F177 EC6E
0080:  EB6E F876 F875 7D6E E966 E05D

```

## Tx Message 8:

```

packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:  0000 1CDB 3E48 3AD4 0000 003C C2B9 B3B1 B3B8 C2DC
0020:  523F 3733 3235 3C49 72CB BDB7 B4B5 B8BF CF67 483C
0040:  3836 373C 455C DAC6 BDB9 B9BB C0CC EE54 453E 3C3C
0060:  3F47 56F1 D1C7 C1BF C0C6 CEE1 6651 4A46 4648 4D59
0080:  70E3 D6CF CDCE D2D9 E67E 675E

```

Bootloader 1.8, Appn 3.1

Application firmware 3.1.8, Built by claux on Thu Jun 17 11:00:05 1999

```

VIC Interface Foreign Exchange Station 0/0, DSP instance (0x19543C0)
Singalling channel num 128 Signalling proxy 0x0 Signaling dsp 0x19543C0
tx outstanding 0, max tx outstanding 32
ptr 0x0, length 0x0, max length 0x0
dsp_number 0, Channel ID 1
received 0 packets, 0 bytes, 0 gaint packets
0 drops, 0 no buffers, 0 input errors 0 input overruns
650070 bytes output, 4976 frames output, 0 output errors, 0 output
underrun
0 unaligned frames

```

```

VIC Interface Foreign Exchange Station 0/1, DSP instance (0x1954604)
Singalling channel num 129 Signalling proxy 0x0 Signaling dsp 0x1954604
tx outstanding 0, max tx outstanding 32
ptr 0x0, length 0x0, max length 0x0
dsp_number 0, Channel ID 2
received 0 packets, 0 bytes, 0 gaint packets

```

```
0 drops, 0 no buffers, 0 input errors 0 input overruns
393976 bytes output, 3982 frames output, 0 output errors, 0 output
underrun
0 unaligned frames
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show dial-peer voice</b>	Displays configuration information and call statistics for dial peers.
<b>show interface dspfarm</b>	Displays hardware information including DRAM, SRAM, and the revision-level information on the line card.
<b>show voice dsp</b>	Displays the current status of all DSP voice channels on the Cisco MC3810.
<b>show voice port</b>	Displays configuration information about a specific voice port.

# show crm

To display the carrier call capacities statistics, use the **show crm** command in privileged EXEC mode.

**show crm**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** Privileged EXEC

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

**Usage Guidelines** Both the **show trunk group** command and the **show crm** command display values for the maximum number of calls. These values originate from different configuration procedures:

- In the **show trunk group** command, the Max Calls value originates from the **max-calls** command in the trunk group configuration.
- In the **show crm** command, Max calls indicates the maximum number of available channels after the carrier ID or trunk group label is assigned to an interface using the **trunk-group** (interface) command.

**Examples** The following example illustrates the carrier call capacities statistics:

```
Router# show crm

Carrier:1411
  Max calls:4
  Max Voice (in) :      4      Cur Voice (in) :      0
  Max Voice (out):      4      Cur Voice (out):      0
  Max Data (in)  :      4      Cur Data (in)  :      0
  Max Data (out) :      4      Cur Data (out) :      0

Trunk Group Label: 100
  Max calls:6
  Max Voice (in) :      6      Cur Voice (in) :      0
  Max Voice (out):      6      Cur Voice (out):      0
  Max Data (in)  :      6      Cur Data (in)  :      0
  Max Data (out) :      6      Cur Data (out) :      0
```

Table 48 describes the fields shown in this output, in alphabetical order.

**Table 57** *show crm Field Descriptions*

<b>Field</b>	<b>Description</b>
Carrier	ID of the carrier that handles the calls.
Cur Data (in)	Current number of incoming data calls that are handled by the carrier or trunk group.
Cur Data (out)	Current number of outgoing data calls that are handled by the carrier or trunk group.
Cur Voice (in)	Current number of incoming voice calls that are handled by the carrier or trunk group.
Cur Voice (out)	Current number of outgoing voice calls that are handled by the carrier or trunk group.
Max Calls	Maximum number of calls that are handled by the carrier or trunk group.
Max Data (in)	Maximum number of incoming data calls that are handled by the carrier or trunk group.
Max Data (out)	Maximum number of outgoing data calls that are handled by the carrier or trunk group.
Max Voice (in)	Maximum number of incoming voice calls that are handled by the carrier or trunk group.
Max Voice (out)	Maximum number of outgoing voice calls that are handled by the carrier or trunk group.
Trunk Group Label	Label of the trunk group that handles the calls.

#### Related Commands

<b>Command</b>	<b>Description</b>
<b>carrier-id (dial-peer)</b>	Specifies the carrier associated with VoIP calls.
<b>max-calls</b>	Specifies the maximum number of calls handled by a trunk group.
<b>show trunk group</b>	Displays the configuration parameters for one or more trunk groups.
<b>trunk-group (interface)</b>	Assigns an interface to a trunk group.
<b>trunk-group-label (dial-peer)</b>	Specifies the trunk group associated with VoIP calls.

# show csm

To display the call switching module (CSM) statistics for a particular digital signal processor (DSP) channel or all DSP channels or for a specific modem or DSP channel, use the **show csm** command in privileged EXEC mode.

## Cisco AS5300 Universal Access Server

```
show csm {modem [slot/port | modem-group-number] | voice [slot/dsp/dsp/dsp-channel]}
```

## Cisco AS5800 Universal Access Server

```
show csm voice [shelf/slot/port]
```

Syntax Description		
<b>modem</b>		CSM call statistics for modems.
<b>voice</b>		CSM call statistics for DSP channels.
<i>slot/port</i>	(Optional)	Location (and thereby identity) of a specific modem.
<i>modem-group-number</i>	(Optional)	Location of a particular dial peer. Valid entries are any integers that identify a specific dial peer, from 1 to 32767.
<i>slot/dsp/dsp/dsp-channel</i>	(Optional)	Location of a particular DSP channel.
<i>shelf/slot/port</i>	(Optional)	Location of the voice interface card.

## Defaults

No default behavior or values

## Command Modes

Privileged EXEC

## Command History

Release	Modification
11.3 NA	This command was introduced.
12.0(3)T	Port-specific values for the Cisco AS5300 were added.
12.0(7)T	Port-specific values for the Cisco AS5800 were added.

## Usage Guidelines

This command shows the information related to CSM, which includes the DSP channel, the start time of the call, the end time of the call, and the channel on the controller used by the call.

Use the **show csm modem** command to display the CSM call statistic information for a specific modem, for a group of modems, or for all modems. If a *slot/port* argument is specified, then CSM call statistics are displayed for the specified modem. If the *modem-group-number* argument is specified, the CSM call statistics for all of the modems associated with that modem group are displayed. If no keyword is specified, CSM call statistics for all modems on the Cisco AS5300 universal access server are displayed.

Use the **show csm voice** command to display CSM statistics for a particular DSP channel. If the *slot/dsp/dsp/dsp-channel* or *shelf/slot/port* argument is specified, the CSM call statistics for calls using the identified DSP channel are displayed. If no argument is specified, all CSM call statistics for all DSP channels are displayed.

**Examples**

The following is sample output from this command for the Cisco AS5300 universal access server:

```
Router# show csm voice 2/4/4/0

slot 2, dspm 4, dsp 4, dsp channel 0,
slot 2, port 56, tone, device_status(0x0002): VDEV_STATUS_ACTIVE_CALL.

csm_state(0x0406)=CSM_OC6_CONNECTED, csm_event_proc=0x600E2678, current call thru PRI line
invalid_event_count=0, wdt_timeout_count=0
wdt_timestamp_started is not activated
wait_for_dialing:False, wait_for_bchan:False
pri_chnl=TDM_PRI_STREAM(s0, u0, c22), tdm_chnl=TDM_DSP_STREAM(s2, c27)
dchan_idb_start_index=0, dchan_idb_index=0, call_id=0xA003, bchan_num=22
csm_event=CSM_EVENT_ISDN_CONNECTED, cause=0x0000
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=3
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, stat_busyout=0
oobp_failure=0
call_duration_started=00:06:53, call_duration_ended=00:00:00, total_call_duration=00:00:44
The calling party phone number = 408
The called party phone number = 5271086
total_free_rbs_timeslot = 0, total_busy_rbs_timeslot = 0, total_dynamic_busy_rbs_timeslot
= 0, total_static_busy_rbs_timeslot = 0,
total_sw56_rbs_timeslot = 0, total_sw56_rbs_static_bo_ts = 0,
total_free_isdn_channels = 21, total_busy_isdn_channels = 0, total_auto_busy_isdn_channels
= 0,
min_free_device_threshold = 0
```

The following is sample output from this command for the Cisco AS5800:

```
Router# show csm voice 1/8/19

shelf 1, slot 8, port 19
VDEV_INFO:slot 8, port 19
vdev_status(0x00000401):VDEV_STATUS_ACTIVE_CALL.VDEV_STATUS_HASLOCK.
csm_state(0x00000406)=CSM_OC6_CONNECTED, csm_event_proc=0x60868B8C, current
call thru PRI line
invalid_event_count=0, wdt_timeout_count=0
watchdog timer is not activated
wait_for_bchan:False
pri_chnl=(T1 1/0/0:22), vdev_chnl=(s8, c19)
start_chan_p=0, chan_p=62436D58, call_id=0x800D, bchan_num=22
The calling party phone number =
The called party phone number = 7511
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=1
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, busyout=0, modem_reset=0
call_duration_started=3d16h, call_duration_ended=00:00:00,
total_call_duration=00:00:00
```

[Table 49](#) describes significant fields shown in this output.

**Table 58** *show csm voice Field Descriptions*

Field	Description
slot	Slot where the VFC resides.
shelf/slot/port	The T1 or E1 controller.
dspm/dsp/dsp channel	Which DSP channel is engaged in this call.

**Table 58** show csm voice Field Descriptions (continued)

Field	Description
dsp	DSP through which this call is established.
slot/port	Logical port number for the device. This is equivalent to the DSP channel number. The port number is derived as follows: <ul style="list-style-type: none"> <li>• (max_number_of_dsp_channels per dspm=12) * the dspm # (0-based) +</li> <li>• (max_number_of_dsp_channels per dsp=2) * the dsp # (0-based) + the dsp channel number (0-based).</li> </ul>
tone	Which signaling tone is being used (DTMF, MF, R2). This only applies to CAS calls. Possible values are as follows: <ul style="list-style-type: none"> <li>• mf</li> <li>• dtmf</li> <li>• r2-compelled</li> <li>• r2-semi-compelled</li> <li>• r2-non-compelled</li> </ul>
device_status	Status of the device. Possible values are as follows: <ul style="list-style-type: none"> <li>• VDEV_STATUS_UNLOCKED—Device is unlocked (meaning that it is available for new calls).</li> <li>• VDEV_STATUS_ACTIVE_WDT—Device is allocated for a call and the watchdog timer is set to time the connection response from the central office.</li> <li>• VDEV_STATUS_ACTIVE_CALL—Device is engaged in an active, connected call.</li> <li>• VDEV_STATUS_BUSYOUT_REQ—Device is requested to busyout; does not apply to voice devices.</li> <li>• VDEV_STATUS_BAD—Device is marked as bad and not usable for processing calls.</li> <li>• VDEV_STATUS_BACK2BACK_TEST—Modem is performing back-to-back testing (for modem calls only).</li> <li>• VDEV_STATUS_RESET—Modem needs to be reset (for modem only).</li> <li>• VDEV_STATUS_DOWNLOAD_FILE—Modem is downloading a file (for modem only).</li> <li>• VDEV_STATUS_DOWNLOAD_FAIL—Modem has failed during downloading a file (for modem only).</li> <li>• VDEV_STATUS_SHUTDOWN—Modem is not powered up (for modem only).</li> <li>• VDEV_STATUS_BUSY—Modem is busy (for modem only).</li> <li>• VDEV_STATUS_DOWNLOAD_REQ—Modem is requesting connection (for modem only).</li> </ul>

**Table 58** *show csm voice Field Descriptions (continued)*

Field	Description
csm_state	<p>CSM call state of the current call (PRI line) associated with this device. Possible values are as follows:</p> <ul style="list-style-type: none"> <li>• CSM_IDLE_STATE—Device is idle.</li> <li>• CSM_IC_STATE—A device has been assigned to an incoming call.</li> <li>• CSM_IC1_COLLECT_ADDR_INFO—A device has been selected to perform ANI/DNIS address collection for this call. ANI/DNIS address information collection is in progress. The ANI/DNIS is used to decide whether the call should be processed by a modem or a voice DSP.</li> <li>• CSM_IC2_RINGING—The device assigned to this incoming call has been told to get ready for the call.</li> <li>• CSM_IC3_WAIT_FOR_SWITCH_OVER—A new device is selected to take over this incoming call from the device collecting the ANI/DNIS address information.</li> <li>• CSM_IC4_WAIT_FOR_CARRIER—This call is waiting for the CONNECT message from the carrier.</li> <li>• CSM_IC5_CONNECTED—This incoming call is connected to the central office.</li> <li>• CSM_IC6_DISCONNECTING—This incoming call is waiting for a DISCONNECT message from the VTSP module to complete the disconnect process.</li> <li>• CSM_OC_STATE —An outgoing call is initiated.</li> <li>• CSM_OC1_REQUEST_DIGIT—The device is requesting the first digit for the dial-out number.</li> <li>• CSM_OC2_COLLECT_1ST_DIGIT—The first digit for the dial-out number has been collected.</li> <li>• CSM_OC3_COLLECT_ALL_DIGIT—All the digits for the dial-out number have been collected.</li> <li>• CSM_OC4_DIALING—This call is waiting for a dsx0 (B channel) to be available for dialing out.</li> <li>• CSM_OC5_WAIT_FOR_CARRIER—This (outgoing) call is waiting for the central office to connect.</li> <li>• CSM_OC6_CONNECTED—This (outgoing) call is connected.</li> <li>• CSM_OC7_BUSY_ERROR—A busy tone has been sent to the device (for VoIP call, no busy tone is sent; just a DISCONNECT INDICATION message is sent to the VTSP module), and this call is waiting for a DISCONNECT message from the VTSP module (or ONHOOK message from the modem) to complete the disconnect process.</li> <li>• CSM_OC8_DISCONNECTING—The central office has disconnected this (outgoing) call, and the call is waiting for a DISCONNECT message from the VTSP module to complete the disconnect process.</li> </ul>

**Table 58** show csm voice Field Descriptions (continued)

Field	Description
csm_state: invalid_event_count	Number of invalid events received by the CSM state machine.
wdt_timeout_count	Number of times the watchdog timer is activated for this call.
wdt_timestamp_started	Whether the watchdog timer is activated for this call.
wait_for_dialing	Whether this (outgoing) call is waiting for a free digit collector to become available to dial out the outgoing digits.
wait_for_bchan	Whether this (outgoing) call is waiting for a B channel to send the call out on.
pri_chnl	Which type of TDM stream is used for the PRI connection. For PRI and CAS calls, it is always TDM_PRI_STREAM.
tdm_chnl	Which type of TDM stream is used for the connection to the device used to process this call. In the case of a VoIP call, this is always set to TDM_DSP_STREAM.
dchan_idb_start_index	First index to use when searching for the next IDB of a free D channel.
dchan_idb_index	Index of the currently available IDB of a free D channel.
csm_event	Event just passed to the CSM state machine.
cause	Event cause.
ring_no_answer	Number of times a call failed because there was no response.
ic_failure	Number of failed incoming calls.
ic_complete	Number of successful incoming calls.
dial_failure	Number of times a connection failed because there was no dial tone.
oc_failure	Number of failed outgoing calls.
oc_complete	Number of successful outgoing calls.
oc_busy	Number of outgoing calls whose connection failed because there was a busy signal.
oc_no_dial_tone	Number of outgoing calls whose connection failed because there was no dial tone.
oc_dial_timeout	Number of outgoing calls whose connection failed because the timeout value was exceeded.
call_duration_started	Start of this call.
call_duration_ended	End of this call.
total_call_duration	Duration of this call.
The calling party phone number	Calling party number as given to CSM by ISDN.
The called party phone number	Called party number as given to CSM by ISDN.
total_free_rbs_time slot	Total number of free RBS (CAS) time slots available for the whole system.
total_busy_rbs_time slot	Total number of RBS (CAS) time slots that have been busied-out. This includes both dynamically and statically busied out RBS time slots.

**Table 58** *show csm voice Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
total_dynamic_busy_rbs_time slot	Total number of RBS (CAS) time slots that have been dynamically busied out.
total_static_busy_rbs_time slot	Total number of RBS (CAS) time slots that have been statically busied out (that is, they are busied out using the CLI command).
total_free_isdn_channels	Total number of free ISDN channels.
total_busy_isdn_channels	Total number of busy ISDN channels.
total_auto_busy_isdn_channels	Total number of ISDN channels that are automatically busied out.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show call active voice</b>	Displays the contents of the active call table.
<b>show call history voice</b>	Displays the contents of the call history table.
<b>show num-exp</b>	Displays how number expansions are configured.
<b>show voice port</b>	Displays configuration information about a specific voice port.

# show debug condition

To display the debugging filters that have been enabled for VoiceXML applications, use the **show debug condition** command in privileged EXEC mode.

## show debug condition

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

### Usage Guidelines

This command displays the debugging filter conditions that have been set for VoiceXML applications by using the **debug condition application voice** command.

### Examples

The following is sample output from this command:

```
Router# show debug condition

Condition 1: application voice vmail (1 flags triggered)
           Flags: vmail
Condition 2: application voice myappl (1 flags triggered)
           Flags: myappl
```

[Table 50](#) describes the fields shown in this output.

**Table 59** *show debug condition Field Descriptions*

Field	Description
Condition <i>n</i>	Sequential number identifying the filter condition that was set for the specified command.
Flags	Name of the voice application for which the condition was set.

### Related Commands

Command	Description
<b>debug condition application voice</b>	Filters out debugging messages for all VoiceXML applications except the specified application.
<b>debug http client</b>	Displays debugging messages for the HTTP client.
<b>debug vxml</b>	Displays debugging messages for VoiceXML features.

# show dial-peer video

To display configuration information for video dial peers, use the **show dial-peer video** command in privileged EXEC mode.

**show dial-peer video** [*number*] [**summary**]

Syntax Description	
<i>number</i>	(Optional) A specific video dial peer. Output displays information about that dial peer.
<b>summary</b>	(Optional) Output displays a one-line summary of each video dial peer.

**Defaults** If both the *name* argument and **summary** keyword are omitted, command output displays detailed information about all video dial peers.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(5)XK	This command was introduced on the Cisco MC3810.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

**Usage Guidelines** Use this command to display the configuration for all video dial peers configured for a router. To show configuration information for only one specific dial peer, use the *number* argument to identify the dial peer.

**Examples** On a Cisco MC3810, the following sample output displays detailed information about all configured video dial peers:

```
Router# show dial-peer video

Video Dial-Peer 1
  type = videocodec, destination-pattern = 111
  port signal = 1/0, port media = Serial1
  nsap = 47.0091810000000050E201B101.00107B09C6F2.C8
Video Dial-Peer 2
  type = videoatm, destination-pattern = 222
  session-target = ATM0 svc nsap 47.0091810000000050E201B101.00E01E92ADC2.C8
Video Dial-Peer 3
  type = videoatm, destination-pattern = 333
  session-target = ATM0 pvc 70/70
```

# show dial-peer voice

To display information for voice dial peers, use the **show dial-peer voice** command in EXEC mode.

**show dial-peer voice** [*number* | **summary**]

Syntax Description		
<i>number</i>	(Optional) A specific voice dial peer. Output displays detailed information about that dial peer.	
<b>summary</b>	(Optional) Output displays a short summary of each voice dial peer.	

**Defaults** If both the *name* argument and **summary** keyword are omitted, output displays detailed information about all voice dial peers.

**Command Modes** EXEC

Command History	Release	Modification
	11.3(1)T	This command was introduced.
	11.3(1)MA	The <b>summary</b> keyword was added for Cisco MC3810.
	12.0(3)XG	This command was implemented for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
	12.0(4)T	This command was implemented for VoFR on the Cisco 7200 series.
	12.1(3)T	This command was implemented for Modem Passthrough over VoIP on the Cisco AS5300.
	12.2(2)XB	This command was modified to support VoiceXML applications.
	12.2(4)T	This command was implemented on the Cisco 1750.
	12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
	12.2(2)XN	Support for enhanced MGCP voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2 and implemented on the and Cisco IAD2420.

**Usage Guidelines** Use this command to display the configuration for all VoIP and plain old telephone service (POTS) dial peers configured for a router. To show configuration information for only one specific dial peer, use the *number* argument to identify the dial peer. To show summary information for all dial peers, use the **summary** keyword.

**Examples**

The following is sample output from the **show dial-peer voice** command for a POTS dial peer:

```
Router> show dial-peer voice 100

VoiceEncapPeer100
  information type = voice,
  description = '',
  tag = 100, destination-pattern = '',
  answer-address = '', preference=0,
  numbering Type = 'unknown'
  group = 100, Admin state is up, Operation state is up,
  incoming called-number = '555...', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
  huntstop = disabled,
  in bound application associated: 'vxml_inb_app'
  out bound application associated: ''
  dnis-map =
  permission :both
  incoming COR list:maximum capability
  outgoing COR list:minimum requirement
  type = pots, prefix = '',
  forward-digits default
  session-target = '', voice-port = '',
  direct-inward-dial = disabled,
  digit_strip = enabled,
  register E.164 number with GK = TRUE

  Connect Time = 0, Charged Units = 0,
  Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
  Accepted Calls = 0, Refused Calls = 0,
  Last Disconnect Cause is "",
  Last Disconnect Text is "",
  Last Setup Time = 0.
```

The following is sample output from this command for a VoIP dial peer:

```
Router> show dial-peer voice 101

VoiceOverIpPeer101
  information type = voice,
  description = '',
  tag = 101, destination-pattern = '5551212',
  answer-address = '', preference=0,
  numbering Type = 'unknown'
  group = 101, Admin state is up, Operation state is up,
  incoming called-number = '', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
  modem passthrough = system,
  huntstop = disabled,
  in bound application associated: 'DEFAULT'
  out bound application associated: 'vapp1'
  dnis-map =
  permission :both
  incoming COR list:maximum capability
  outgoing COR list:minimum requirement
  type = voip, session-target = 'ipv4:10.10.1.1',
  technology prefix:
  settle-call = disabled
  ip media DSCP = default, ip signaling DSCP = default, UDP checksum = di,
  session-protocol = cisco, session-transport = system, req-qos = best-ef
  acc-qos = best-effort,
  RTP dynamic payload type values: NTE = 101
  Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
  CAS=123, ClearChan=125, PCM switch over u-law=126,A-law=127
```

```

fax rate = voice,    payload size = 20 bytes
fax protocol = system
fax NSF = 0xAD0051 (default)
codec = g729r8,    payload size = 20 bytes,
Expect factor = 0, Icpif = 20,
Playout Mode is set to default,
Initial 60 ms, Max 300 ms
Playout-delay Minimum mode is set to default, value 40 ms
Expect factor = 0,
Max Redirects = 1, Icpif = 20, signaling-type = ext-signal,
CLID Restrict = disabled
VAD = enabled, Poor QOV Trap = disabled,
voice class perm tag = ``
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.

```

Table 51 describes fields shown in this output, in alphabetical order.

**Table 60** show dial-peer voice Field Descriptions

Field	Description
Accepted Calls	Number of calls accepted from this peer since system startup.
acc-qos	Lowest acceptable quality of service configured for calls for this peer.
Admin state	Administrative state of this peer.
answer-address	Answer address configured for this dial peer.
Charged Units	Total number of charging units that have applied to this peer since system startup, in hundredths of a second.
codec	Default voice codec rate of speech for this peer.
Connect Time	Accumulated connect time to the peer since system startup for both incoming and outgoing calls, in hundredths of a second.
dest-pat	Destination pattern (telephone number) for this peer.
dnis-map	The name of the dialed-number identification service (DNIS) map that is configured in the dial peer, if any.
DTMF Relay	Indicates whether or not dual-tone multifrequency (DTMF) relay has been enabled, by using the <b>dtmf-relay</b> command, for this dial peer.
Expect factor	User-requested expectation factor of voice quality for calls through this peer.
Failed Calls	Number of failed call attempts to this peer since system startup.
fax-rate	Fax transmission rate configured for this peer.
group	Group number associated with this peer.
huntstop	Indicates whether dial-peer hunting has been turned on, by using the <b>huntstop</b> command, for this dial peer.
Icpif	Configured calculated planning impairment factor (ICPIF) value for calls sent by a dial peer.

**Table 60** show dial-peer voice Field Descriptions (continued)

Field	Description
in bound application associated	Interactive voice response (IVR) application that is configured to handle inbound calls to this dial peer.
incall-number	Full E.164 telephone number to be used to identify the dial peer.
incoming called-number	Indicates the incoming called number if it has been set by using the <b>incoming-called number</b> command.
information type	Information type for this call; for example, voice or fax.
Last Disconnect Cause	Encoded network cause associated with the last call. This value is updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the system uptime when the last call to this peer was started.
Modem passthrough	Modem pass-through signaling method is named signaling event (NSE).
Operation state	Operational state of this peer.
out bound application associated	The voice application that is configured to handle outbound calls from this dial peer. Outbound calls are handed off to the named application.
Payload type	NSE payload type.
Permission	Configured permission level for this peer.
Poor QOV Trap	Whether poor quality of voice trap messages has been enabled or disabled.
Redundancy	Packet redundancy (RFC 2198) for modem traffic.
Refused Calls	Number of calls from this peer refused since system startup.
req-qos	Configured requested quality of service for calls for this dial peer.
session-target	Session target of this peer.
sess-proto	Session protocol to be used for Internet calls between local and remote routers through the IP backbone.
Successful Calls	Number of completed calls to this peer.
tag	Unique dial peer ID number.
VAD	Whether voice activation detection (VAD) is enabled for this dial peer.

The following is sample output from this command:

```
Router> show dial-peer voice summary

dial-peer hunt 0

      TAG TYPE  ADMIN OPER PREFIX  DEST-PATTERN  PASS
      3  mmoup  up   down          0
     100 pots  up   up            0
     101 voip  up   up            5551212      0  syst ipv4:10.10.1.1
     102 voip  up   up            5551234      0  syst ipv4:10.10.1.1
```

```

99 voip up down 0 syst
33 mmoip up down 0

```

Table 52 describes the fields shown in this output, in alphabetical order.

**Table 61** show dial-peer voice summary Field Descriptions

Field	Description
dial-peer hunt	Hunt group selection order that is defined for the dial peer by using the <b>dial-peer hunt</b> command.
TAG	Unique identifier assigned to the dial peer when it was created.
TYPE	Type of dial peer: POTS, VoIP, VoFR, VoATM, or MMoIP.
ADMIN	Whether the administrative state is up or down.
OPER	Whether the operational state is up or down.
PREFIX	Prefix that is configured in the dial peer by using the <b>prefix</b> command.
DEST-PATTERN	Destination pattern that is configured in the dial peer by using the <b>destination-pattern</b> command.
PREF	Hunt group preference that is configured in the dial peer by using the <b>preference</b> command.
PASS THRU	Modem pass-through method that is configured in the dial peer by using the <b>modem passthrough</b> command.
SESS-TARGET	Destination that is configured in the dial peer by using the <b>session target</b> command.
PORT	Router voice port that is configured for the dial peer. Valid only for POTS dial peers.

#### Related Commands

Command	Description
<b>show call active voice</b>	Displays the VoIP active call table.
<b>show call history voice</b>	Displays the VoIP call history table.
<b>show dialplan incall number</b>	Displays which POTS dial peer is matched for a specific calling number or voice port.
<b>show dialplan number</b>	Displays which dial peer is reached when a specific telephone number is dialed.
<b>show num-exp</b>	Displays how the number expansions are configured in VoIP.
<b>show voice port</b>	Displays configuration information about a specific voice port.

# show dialplan dialpeer

To display the outbound dial peers that are matched to an incoming dial peer based on the class of restriction (COR) criteria and the dialed number, use the **show dialplan dialpeer** command in privileged EXEC mode.

**show dialplan dialpeer** *incoming-dialpeer-tag* **number** *number* [**timeout**]

Syntax Description	
<i>incoming-dialpeer-tag</i>	The dial peer COR identifier used to determine the matching outbound dial peer.
<i>number</i>	The dialed number used in conjunction with the COR identifier to determine the matching outbound dial peer.
<b>timeout</b>	(Optional) Allows matching for variable-length destination patterns.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on Cisco AS5800 access servers.
	12.2(11)T	This command was implemented on the Cisco 1751 and Cisco 3700 series routers and on Cisco AS5300 access servers.

**Usage Guidelines** Use this command as a troubleshooting tool to determine which outbound dial peer is matched for an incoming call, based on the COR criteria and dialed number specified in the command line. Use the **timeout** keyword to enable matching variable-length destination patterns associated with dial peers. This can increase your chances of finding a match for the dial peer number you specify.



**Note**

For actual voice calls coming into the router, the incoming corlist of a specified inbound dial peer and the outgoing called number will be used to match the outbound dial peer.

**Examples** The following sample output shows an incoming call with a dialed number of 19001111 and meeting the COR criteria as part of dial peer 300 with incoming COR-list has been matched to an outbound dial peer with IP address 1.8.50.7:

```
Router# show dialplan dialpeer 300 number 1900111
VoiceOverIpPeer900
  information type = voice,
  description = '',
  tag = 900, destination-pattern = `1900',
  answer-address = '', preference=0,
  numbering Type = `unknown'
  group = 900, Admin state is up, Operation state is up,
  incoming called-number = '', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
```

```

modem passthrough = system,
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
outgoing COR list:to900
type = voip, session-target = `ipv4:1.8.50.7',
technology prefix:
settle-call = disabled
...
Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Matched: 19001111 Digits: 4
Target: ipv4:1.8.50.7

```

Table 62 describes the significant fields shown in the display.

**Table 62** show dialplan command Field Descriptions

Field	Description
Macro Exp.	Expected destination pattern for this dial peer.
VoiceEncapPeer	Dial peer associated with the calling number entered.
VoiceOverIpPeer	Dial peer associated with the calling number entered.
peer type	Type of this dial peer (voice or data).
information type	Information type for this dial peer (voice or data).
description	Any additional information for this dial peer entered using the <b>description</b> dial peer command.
tag	Unique number identifying the dial peer.
destination-pattern	Destination pattern (telephone number) configured for this dial peer.
answer-address	Answer address (calling number) configured for this dial peer.
preference	Hunt group preference order set for this dial peer.
CLID restriction	Indicates the Caller ID restriction (if any) configured for this dial peer.
CLID Network Number	Indicates the originating network of the Caller ID source.
CLID Second Number sent	Indicates the digits in the second number (if any) forwarded for this dial peer.
source carrier-id	VoIP or POTS source carrier identifier.
source trunk-group-label	VoIP or POTS source trunk group identifier.
numbering Type	Identifies the numbering scheme employed for this dial peer.
group	Dial peer group in which this dial peer is a member.
Admin state	Administrative state of this dial peer.

**Table 62** show dialplan command Field Descriptions (continued)

Field	Description
Operation state	Operational state of this dial peer.
incoming called-number	Called number (DNIS) configured for this dial peer.
connections/maximum	Number of actual and maximum allowable connections associated with this dial peer.
DTMF Relay	Whether the <b>dtmf-relay</b> command is enabled or disabled for this dial peer.
URI classes: Incoming (Request)	URI voice class used for matching dial peer to Request-URI in an incoming SIP Invite message.
URI classes: Incoming (To)	URI voice class used for matching dial peer to the To header in an incoming SIP Invite message.
URI classes: Incoming (From)	URI voice class used for matching dial peer to the From header in an incoming SIP Invite message.
URI classes: Destination	URI voice class used to match the dial peer to the destination URI for an outgoing call.
modem transport	Transport method configured for modem calls. The default is system, which means that the value configured globally is used.
huntstop	Whether the <b>huntstop</b> command is enabled or disabled for this dial peer.
in bound application associated	IVR application that is associated with this dial peer when this dial peer is used for an inbound call leg.
out bound application associated	IVR application that is associated with this dial peer when this dial peer is used for an outbound call leg.
dnis-map	Name of the dialed-number identification service (DNIS) map that is configured in the dial peer with the <b>dnis-map</b> command.
permission	Configured permission level for this dial peer.
incoming COR list	Class of restriction (COR) criteria associated when matching an incoming dial peer.
outgoing COR list	COR criteria used to determine the appropriate outbound dial peer.
Translation profile (Incoming)	Incoming translation criteria applied to this dial peer.
Translation profile (Outgoing)	Translation criteria applied to this dial peer when matching an outbound dial peer.
incoming call blocking	Indicates whether or not incoming call blocking has been applied for this dial peer.
translation-profile	The predefined translation profile associated with this dial peer.
disconnect-cause	Encoded network cause associated with the last call.
voice-port	Voice port through which calls come into this dial peer.
type	Type of dial peer (POTS or VoIP).
prefix	Prefix number that is added to the front of the dial string before it is forwarded to the telephony device.

**Table 62** show dialplan command Field Descriptions (continued)

Field	Description
forward-digits	Which digits are forwarded to the telephony interface as configured using the <b>forward-digits</b> command.
session-target	Configured session target (IP address or host name) for this dial peer.
direct-inward-dial	Whether the <b>direct-inward-dial</b> command is enabled or disabled for this dial peer.
digit_strip	Whether digit stripping is enabled or disabled in the dial peer. Enabled is the default.
register E.164 number with GK	Indicates whether or not the dial peer has been configured to register its full E.164-format number with the local gatekeeper.
fax rate	The transmission speed configured for fax calls. The default is system, which means that the value configured globally is used.
payload size	The size (in bytes) for a fax transmission payload.
session-protocol	Session protocol to be used for Internet calls between local and remote router via the IP backbone.
req-qos	Configured requested quality of service for calls for this dial peer.
acc-qos	Lowest acceptable quality of service configured for calls for this dial peer.
codec	Voice codec configured for this dial peer. Default is G.729 (8 kbps).
Expect factor	User-requested expectation factor of voice quality for calls through this dial peer.
Icpif	Configured calculated planning impairment factor (ICPIF) value for calls sent by this dial peer.
VAD	Indicates whether or not voice activation detection (VAD) is enabled for this dial peer.
voice class sip url	URL format (SIP or TEL) used for SIP calls to this dial peer, as configured with the <b>voice-class sip url</b> command. The default is system, which means that the value configured globally with the <b>url</b> command in voice service VoIP SIP mode is used.
voice class sip rel1xx	Indicates whether or not reliable provisional responses are supported, as configured with the <b>voice-class sip rel1xx</b> command. The default is system, which means that the value configured globally with the <b>rel1xx</b> command in voice service VoIP SIP mode is used.
voice class perm tag	Voice class for a trunk that is assigned to this dial peer with the <b>voice-class permanent</b> command.
Connect Time	Unit of measure indicating the call connection time associated with this dial peer.
Charged Units	Number of call units charged to this dial peer.
Successful Calls	Number of completed calls to this dial peer since system startup.
Failed Calls	Number of uncompleted (failed) calls to this dial peer since system startup.

**Table 62** *show dialplan command Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Incomplete Calls	Number of incomplete calls to this dial peer since system startup.
Accepted Calls	Number of calls from this dial peer accepted since system startup.
Refused Calls	Number of calls from this dial peer refused since system startup.
Last Disconnect Cause	Encoded network cause associated with the last call. This value is updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the System Up Time when the last call to this peer was started.
Matched	Destination pattern matched for this dial peer.
Digits	Number of digits in this destination pattern matched for this dial peer.
Target	Matched session target (IP address or host name) for this dial peer.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show dialplan in-carrier</b>	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
<b>show dialplan in-trunk-group-label</b>	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.
<b>show dialplan incall</b>	Displays which POTS dial peer is matched for a specific calling number or voice port.
<b>show dialplan number</b>	Displays which dial peer is matched for a particular telephone number.

# show dialplan in-carrier

To display which incoming VoIP or POTS dial peer is matched for a specific source carrier or voice port, use the **show dialplan in-carrier** command in privileged EXEC mode.

```
show dialplan in-carrier carrier-id [voip | pots]
```

## Syntax Description

<i>carrier-id</i>	VoIP or POTS source carrier identifier.
<b>voip</b>	(Optional) Allows you to limit the search criteria to only VoIP dial peers.
<b>pots</b>	(Optional) Allows you to limit the search criteria to only POTS dial peers.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(13)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers.

## Usage Guidelines

Use this command as a troubleshooting tool to determine which VoIP or POTS dial peer is matched for an incoming call, based on the carrier identifier specified in the command line. Use the **voip** or **pots** keywords to further limit the scope of possible matches for the dial peer specified in the **show dialplan** command line.

## Examples

The following sample output shows a VoIP or POTS dial peer being matched to another POTS dial peer based on its carrier identifier, "aaa":

```
Router# show dialplan in-carrier aaa pots

  Inbound pots dialpeer Matching based on source carrier-id

VoiceEncapPeer7777
  information type = voice,
  description = '',
  tag = 7777, destination-pattern = '',
  answer-address = '', preference=0,
  CLID Restriction = None
  CLID Network Number = ''
  CLID Second Number sent
  source carrier-id = 'aaa',      target carrier-id = '',
  source trunk-group-label = '', target trunk-group-label = '',
  numbering Type = 'unknown'
  group = 7777, Admin state is up, Operation state is up,
  incoming called-number = '', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
  huntstop = disabled,
  in bound application associated:'DEFAULT'
  out bound application associated:''
  dnis-map =
  permission :both
```

```

incoming COR list:maximum capability
outgoing COR list:minimum requirement
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = ''
disconnect-cause = 'no-service'
voice-port = ''
  type = pots, prefix = '',
  forward-digits default
  session-target = '', up,
  direct-inward-dial = disabled,
  digit_strip = enabled,
  register E.164 number with GK = TRUE
  fax rate = system,  payload size = 20 bytes

Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Matched:  Digits:0
Target:

```



**Note**

[Table 62](#) describes the significant fields shown in the display.

**Related Commands**

Command	Description
<b>show dialplan dialpeer</b>	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
<b>show dialplan in-trunk-group-label</b>	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.
<b>show dialplan incall</b>	Displays which POTS dial peer is matched for a specific calling number or voice port.
<b>show dialplan number</b>	Displays which dial peer is matched for a particular telephone number.

# show dialplan in-trunk-group-label

To display which incoming VoIP or POTS dial peer is matched for a specific trunk group label, use the **show dialplan in-trunk-group-label** command in privileged EXEC mode.

```
show dialplan in-trunk-group-label trunk-group-label [pots | voip]
```

Syntax Description	
<i>trunk-group-label</i>	VoIP or POTS source trunk group identifier.
<b>voip</b>	(Optional) Allows you to limit the search criteria to only VoIP dial peers.
<b>pots</b>	(Optional) Allows you to limit the search criteria to only POTS dial peers.

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers.

**Usage Guidelines**

Use this command to determine which VoIP or POTS dial peer is matched for an incoming call, based on the identifier of the source trunk group. The router attempts to match these items in the order listed. Use the **voip** or **pots** keywords to further limit the scope of possible matches for the dial peer specified in the **show dialplan** command line.

**Examples**

The following sample output shows an inbound VoIP or POTS dial peer being matched to an outbound POTS dial peer based on the trunk group label “NYtrunk”:

```
Router# show dialplan in-trunk-group-label NYtrunk pots

  Inbound pots dialpeer Matching based on source trunk-group-label

VoiceEncapPeer2003
  information type = voice,
  description = '',
  tag = 2003, destination-pattern = '',
  answer-address = '', preference=0,
  CLID Restriction = None
  CLID Network Number = ''
  CLID Second Number sent
  source carrier-id = '', target carrier-id = '',
  source trunk-group-label = 'NYtrunk', target trunk-group-label = '',
  numbering Type = 'unknown'
  group = 2003, Admin state is up, Operation state is up,
  incoming called-number = '', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
  huntstop = disabled,
  in bound application associated:'debit-card'
  out bound application associated:''
  dnis-map =
  permission :both
```

```

incoming COR list:maximum capability
outgoing COR list:minimum requirement
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = ''
disconnect-cause = 'no-service'
voice-port = ''
  type = pots, prefix = '',
  forward-digits default
  session-target = '', up,
  direct-inward-dial = disabled,
  digit_strip = enabled,
  register E.164 number with GK = TRUE
  fax rate = system,  payload size = 20 bytes

Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Matched:  Digits:0
Target:

```



**Note**

[Table 62](#) describes the significant fields shown in the display.

**Related Commands**

Command	Description
<b>show dialplan dialpeer</b>	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
<b>show dialplan in-carrier</b>	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
<b>show dialplan incall</b>	Displays which POTS dial peer is matched for a specific calling number or voice port.
<b>show dialplan number</b>	Displays which dial peer is matched for a particular telephone number.

# show dialplan incall

To display which incoming POTS dial peer is matched for a specific calling number or voice port, use the **show dialplan incall number** command in privileged EXEC mode.

**show dialplan incall** *voice-port* **number** *calling-number* [**timeout**]

Syntax Description		
<i>voice-port</i>		Voice port location. The syntax of this argument is platform-specific. For information on the syntax for a particular platform, see the <b>voice-port</b> command.
<i>calling-number</i>		E.164 Calling number or ANI of the incoming voice call.
<b>timeout</b>		(Optional) Allows matching for variable-length destination patterns.

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series.
	12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3725, and Cisco 3745 and the <b>timeout</b> keyword was added.

**Usage Guidelines** Use this command as a troubleshooting tool to determine which POTS dial peer is matched for an incoming call, for the selected calling number and voice port. The router attempts to match these items in the order listed:

1. Calling number with answer-address configured in dial peer
2. Calling number with destination-pattern configured in dial peer
3. Voice port with voice port configured in dial peer

The router first attempts to match a dial peer based on the calling number (ANI). If the router is unable to match a dial peer based on the calling number, it matches the call to a POTS dial peer based on the selected voice interface. If more than one dial peer uses the same voice port, the router selects the first matching dial peer. Use the **timeout** keyword to enable matching variable-length destination patterns associated with dial peers. This can increase your chances of finding a match for the dial peer number you specify.



**Note**

For actual voice calls coming into the router, the router attempts to match the called number (the dialed number identification service [DNIS] number) with the incoming called-number configured in a dial peer. The router, however, does not consider the called number when using the **show dialplan incall number** command.

**Examples** The following sample output shows that an incoming call from interface 1/0/0:D with a calling number of 12345 is matched to POTS dial peer 10:

```

Router# show dialplan incall 1/0/0:D number 12345

Macro Exp.: 12345

VoiceEncapPeer10
  information type = voice,
  tag = 10, destination-pattern = `123..',
  answer-address = `', preference=0,
  numbering Type = `unknown'
  group = 10, Admin state is up, Operation state is up,
  incoming called-number = `', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
  huntstop = disabled,
  in bound application associated: DEFAULT
  out bound application associated:
  permission :both
  incoming COR list:maximum capability
  outgoing COR list:minimum requirement
  type = pots, prefix = `',
  forward-digits default
  session-target = `', voice-port = `1/0/0:D',
  direct-inward-dial = disabled,
  digit_strip = enabled,

  register E.164 number with GK = TRUE
  Connect Time = 0, Charged Units = 0,

  register E.164 number with GK = TRUE
  Connect Time = 0, Charged Units = 0,
  Successful Calls = 0, Failed Calls = 0,
  Accepted Calls = 0, Refused Calls = 0,
  Last Disconnect Cause is "",
  Last Disconnect Text is "",
  Last Setup Time = 0.
Matched: 12345  Digits: 3
Target:

```

The following sample output shows that, if no dial peer has a destination pattern or answer address that matches the calling number of 888, the incoming call is matched to POTS dial peer 99, because the call comes in on voice port 1/0/1:D, which is the voice port configured for this dial peer:

```

Router# show dialplan incall 1/0/1:D number 888

Macro Exp.: 888

VoiceEncapPeer99
  information type = voice,
  tag = 99, destination-pattern = `99...',
  answer-address = `', preference=1,
  numbering Type = `national'
  group = 99, Admin state is up, Operation state is up,
  incoming called-number = `', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
  huntstop = disabled,
  in bound application associated: DEFAULT
  out bound application associated:
  permission :both
  incoming COR list:maximum capability
  outgoing COR list:minimum requirement
  type = pots, prefix = `5',
  forward-digits 4
  session-target = `', voice-port = `1/0/1:D',
  direct-inward-dial = enabled,
  digit_strip = enabled,

```

```

register E.164 number with GK = TRUE
    Connect Time = 0, Charged Units = 0,
    Successful Calls = 0, Failed Calls = 0,
    Accepted Calls = 0, Refused Calls = 0,
    Last Disconnect Cause is "",
    Last Disconnect Text is "",
    Last Setup Time = 0.
Matched:    Digits: 0
Target:

```

**Note**

[Table 62](#) describes the significant fields shown in the display.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show dialplan dialpeer</b>	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
<b>show dialplan in-carrier</b>	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
<b>show dialplan in-trunk-group-label</b>	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.
<b>show dialplan number</b>	Displays which dial peer is matched for a particular telephone number.

# show dialplan number

To display which outgoing dial peer is reached when a particular telephone number is dialed, use the **show dialplan number** command in privileged EXEC mode.

```
show dialplan number dial-string [carrier identifier] [fax | huntstop | voice] [timeout]
```

Syntax Description		
	<i>dial-string</i>	Particular destination pattern (E.164 telephone number).
	<b>carrier</b>	(Optional) Indicates that you wish to base your search for applicable dial peers on the source carrier identifier.
	<i>identifier</i>	(Optional) Source carrier identifier to accompany the <b>carrier</b> keyword.
	<b>fax</b>	(Optional) Fax information type.
	<b>huntstop</b>	(Optional) Terminates further dial-peer hunting upon encountering the first dial-string match.
	<b>timeout</b>	(Optional) Allows matching for variable-length destination patterns.
	<b>voice</b>	(Optional) Voice information type.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.3(1)T	This command was introduced on the Cisco 3600 series.
	12.2(1)	The <b>huntstop</b> keyword was added.
	12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3725, and Cisco 3745 and the <b>timeout</b> keyword was added.
	12.2(11)T	The <b>carrier</b> , <b>fax</b> , and <b>voice</b> keywords were added.

**Usage Guidelines** Use this command to test whether the dial plan configuration is valid and working as expected. Use the **timeout** keyword to enable matching variable-length destination patterns associated with dial peers. This can increase your chances of finding a match for the dial peer number you specify.

**Examples** The following is sample output from this command using a destination pattern of 1001:

```
Router# show dialplan number 1001

Macro Exp.: 1001

VoiceEncapPeer1003
  information type = voice,
  tag = 1003, destination-pattern = `1001',
  answer-address = `', preference=0,
  numbering Type = `unknown'
  group = 1003, Admin state is up, Operation state is up,
  incoming called-number = `', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
  huntstop = enabled,
```

```

    type = pots, prefix = `',
    forward-digits default
    session-target = `', voice-port = `1/1',
    direct-inward-dial = disabled,
    Connect Time = 0, Charged Units = 0,
    Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
    Accepted Calls = 0, Refused Calls = 0,
    Last Disconnect Cause is "",
    Last Disconnect Text is "",
    Last Setup Time = 0.
Matched: 1001  Digits: 4
Target:

VoiceEncapPeer1004
    information type = voice,
    tag = 1004, destination-pattern = `1001',
    answer-address = `', preference=0,
    numbering Type = `unknown'
    group = 1004, Admin state is up, Operation state is up,
...
Matched: 1001  Digits: 4
Target:

VoiceEncapPeer1002
    information type = voice,
    tag = 1002, destination-pattern = `1001',
    answer-address = `', preference=0,
    numbering Type = `unknown'
    group = 1002, Admin state is up, Operation state is up,
...
Matched: 1001  Digits: 4
Target:

VoiceEncapPeer1001
    information type = voice,
    tag = 1001, destination-pattern = `1001',
    answer-address = `', preference=0,
    numbering Type = `unknown'
    group = 1001, Admin state is up, Operation state is up,
...
Matched: 1001  Digits: 4
Target:

```

The following is sample output from this command using a destination pattern of 1001 and the **huntstop** keyword:

```
Router# show dialplan number 1001 huntstop
```

```

Macro Exp.: 1001

VoiceEncapPeer1003
    information type = voice,
    tag = 1003, destination-pattern = `1001',
    answer-address = `', preference=0,
    numbering Type = `unknown'
    group = 1003, Admin state is up, Operation state is up,
    incoming called-number = `', connections/maximum = 0/unlimited,
    DTMF Relay = disabled,
    huntstop = enabled,
    type = pots, prefix = `',
    forward-digits default
    session-target = `', voice-port = `1/1',
    direct-inward-dial = disabled,
    Connect Time = 0, Charged Units = 0,

```

```

Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Matched: 1001 Digits: 4
Target:
    
```



**Note**

[Table 62](#) describes the significant fields shown in the display.

**Related Commands**

Command	Description
<b>show dialplan dialpeer</b>	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
<b>show dialplan in-carrier</b>	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
<b>show dialplan in-trunk-group-label</b>	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.
<b>show dialplan incall</b>	Displays which POTS dial peer is matched for a specific calling number or voice port.

# show dspfarm

To display digital-signal-processor (DSP) farm-service information such as operational status and DSP resource allocation for transcoding and conferencing, use the **show dspfarm** command in privileged EXEC mode.

```
show dspfarm [all | dsp {active | all | idle} | sessions]
```

Syntax Description		
	<b>all</b>	(Optional) All DSP-farm global information.
	<b>dsp</b>	(Optional) DSP-farm DSP information.
	<b>active</b>	(Optional) Information about active DSPs.
	<b>all</b>	(Optional) Information about all DSP-farm DSPs.
	<b>idle</b>	(Optional) Information about the idle DSPs.
	<b>sessions</b>	(Optional) Information about DSP-farm sessions and connections.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(5)YH	This command was introduced on the Cisco VG200.
	12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

**Usage Guidelines** The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMS) to provide DSP resources.

**Examples** The following is sample output from this command:

```
Router# show dspfarm

DSPFARM Configuration Information:
Admin State: UP, Oper Status: ACTIVE - Cause code: NONE
Transcoding Sessions: 4, Conferencing Sessions: 0
RTP Timeout: 600

Router# show dspfarm all

DSPFARM Configuration Information:
Admin State: UP, Oper Status: ACTIVE - Cause code: NONE
Transcoding Sessions: 4, Conferencing Sessions: 2
RTP Timeout: 1200
Connection average duration: 3600, Connection check interval 600
Codec G729 VAD: ENABLED

Total number of active session(s) 0, and connection(s) 0
```

SLOT	DSP	CHNL	STATUS	USE	TYPE	SESS-ID	CONN-ID	PKTS-RXED	PKTS-TXED
1	3	1	UP	FREE	conf	-	-	-	-
1	3	2	UP	FREE	conf	-	-	-	-
1	3	3	UP	FREE	conf	-	-	-	-
1	3	4	UP	FREE	conf	-	-	-	-
1	3	5	UP	FREE	conf	-	-	-	-
1	3	6	UP	FREE	conf	-	-	-	-
1	4	1	UP	FREE	conf	-	-	-	-
1	4	2	UP	FREE	conf	-	-	-	-
1	4	3	UP	FREE	conf	-	-	-	-
1	4	4	UP	FREE	conf	-	-	-	-
1	4	5	UP	FREE	conf	-	-	-	-
1	4	6	UP	FREE	conf	-	-	-	-
1	5	1	UP	FREE	xcode	-	-	-	-
1	5	2	UP	FREE	xcode	-	-	-	-
1	5	3	UP	FREE	xcode	-	-	-	-
1	5	4	UP	FREE	xcode	-	-	-	-
1	5	5	UP	FREE	xcode	-	-	-	-
1	5	6	UP	FREE	xcode	-	-	-	-
1	5	7	UP	FREE	xcode	-	-	-	-
1	5	8	UP	FREE	xcode	-	-	-	-

Total number of DSPFARM DSP channel(s) 20

Router# **show dspfarm dsp all**

DSPFARM Configuration Information:

Admin State: UP, Oper Status: ACTIVE - Cause code: NONE

Transcoding Sessions: 4, Conferencing Sessions: 2

RTP Timeout: 1200

Connection average duration: 3600, Connection check interval 600

Codec G729 VAD: ENABLED

Total number of active session(s) 0, and connection(s) 0

SLOT	DSP	CHNL	STATUS	USE	TYPE	SESS-ID	CONN-ID	PKTS-RXED	PKTS-TXED
1	3	1	UP	FREE	conf	-	-	-	-
1	3	2	UP	FREE	conf	-	-	-	-
1	3	3	UP	FREE	conf	-	-	-	-
1	3	4	UP	FREE	conf	-	-	-	-
1	3	5	UP	FREE	conf	-	-	-	-
1	3	6	UP	FREE	conf	-	-	-	-
1	4	1	UP	FREE	conf	-	-	-	-
1	4	2	UP	FREE	conf	-	-	-	-
1	4	3	UP	FREE	conf	-	-	-	-
1	4	4	UP	FREE	conf	-	-	-	-
1	4	5	UP	FREE	conf	-	-	-	-
1	4	6	UP	FREE	conf	-	-	-	-
1	5	1	UP	FREE	xcode	-	-	-	-
1	5	2	UP	FREE	xcode	-	-	-	-
1	5	3	UP	FREE	xcode	-	-	-	-
1	5	4	UP	FREE	xcode	-	-	-	-
1	5	5	UP	FREE	xcode	-	-	-	-
1	5	6	UP	FREE	xcode	-	-	-	-
1	5	7	UP	FREE	xcode	-	-	-	-
1	5	8	UP	FREE	xcode	-	-	-	-

Total number of DSPFARM DSP channel(s) 20

```
Router# show dspfarm sessions
```

```
sess_id  conn_id  stype  mode      codec  pkt  ripaddr      rport  sport
4         145      xcode  sendrecv  g711a  20   10.10.10.19  19460  21284
4         161      xcode  sendrecv  g729   10   10.10.10.28  19414  20382
5         177      xcode  sendrecv  g711u  20   10.10.10.17  18290  21170
5         193      xcode  sendrecv  g729b  10   10.10.10.18  19150  18968
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>dspfarm (DSP farm)</b>	Enables DSP-farm service.

---

# show frame-relay vofr

To display information about the FRF.11 subchannels being used on Voice over Frame Relay (VoFR) data link connection identifiers (DLCIs), use the **show frame-relay vofr** command in privileged EXEC mode.

```
show frame-relay vofr [interface [dlci [cid]]]
```

## Syntax Description

<i>interface</i>	(Optional) Specific interface type and number for which you wish to display FRF.11 subchannel information.
<i>dlci</i>	(Optional) Specific data link connection identifier for which you wish to display FRF.11 subchannel information.
<i>cid</i>	(Optional) Specific subchannel for which you wish to display information.

## Defaults

If this command is entered without a specified interface, FRF.11 subchannel information is displayed for all VoFR interfaces and DLCIs configured on the router.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.0(4)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.

## Usage Guidelines

This command is currently not supported on the Cisco MC3810 for PVCs configured with the **vofr cisco** command or the **frame-relay interface-dlci voice-encap** command.

## Examples

The following is sample output from this command when an interface is not specified:

```
Router# show frame-relay vofr

interface      vofr-type  dlci  cid  cid-type
Serial0/0.1    VoFR       16    4    data
Serial0/0.1    VoFR       16    5    call-control
Serial0/0.1    VoFR       16    10   voice
Serial0/1.1    VoFR cisco  17    4    data
```

The following is sample output from this command when an interface is specified:

```
Router# show frame-relay vofr serial0

interface      vofr-type  dlci  cid  cid-type
Serial0        VoFR       16    4    data
Serial0        VoFR       16    5    call-control
Serial0        VoFR       16    10   voice
```

The following is sample output from this command when an interface and a DLCI are specified:

```
Router# show frame-relay vofr serial10 16

VoFR Configuration for interface Serial0

dlci vofr-type  cid cid-type          input-pkts  output-pkts  dropped-pkts
16   VoFR        4   data              0           0            0
16   VoFR        5   call-control     85982       86099        0
16   VoFR        10  voice            2172293     6370815      0
```

The following is sample output from this command when an interface, a DLCI, and a CID are specified:

```
Router# show frame-relay vofr serial10 16 10

VoFR Configuration for interface Serial0 dlci 16

   vofr-type VoFR    cid 10      cid-type voice
   input-pkts 2172293  output-pkts 6370815  dropped-pkts 0
```

Table 57 describes significant fields shown in this output.

**Table 63** show frame-relay vofr Field Descriptions

Field	Description
interface	Number of the interface that has been selected for observation of FRF.11 subchannels.
vofr-type	Type of VoFR DLCI being observed.
cid	Portion of the specified DLCI that is carrying the designated traffic type. A DLCI can be subdivided into 255 subchannels.
cid-type	Type of traffic carried on this subchannel.
input-pkts	Number of packets received by this subchannel.
output-pkts	Number of packets sent on this subchannel.
dropped-pkts	Total number of packets discarded by this subchannel.

#### Related Commands

Command	Description
<b>show call active voice</b>	Displays the contents of the active call table.
<b>show call history voice</b>	Displays the contents of the call history table.
<b>show dial-peer voice</b>	Displays configuration information and call statistics for dial peers.
<b>show frame-relay fragment</b>	Displays Frame Relay fragmentation details.
<b>show frame-relay pvc</b>	Displays statistics about PVCs for Frame Relay interfaces.
<b>show voice-port</b>	Displays configuration information about a specific voice port.

# show gatekeeper calls

To display the status of each ongoing call of which a gatekeeper is aware, use the **show gatekeeper calls** command in privileged EXEC mode.

## show gatekeeper calls

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
	12.0(5)T	The output for this command was changed.
	12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
	12.2(4)T	Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
	12.2(2)XB1	This command was implemented on the Cisco AS5850.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400 and Cisco AS5850 in this release.

**Usage Guidelines** Use this command to show all active calls currently being handled by a particular Multimedia Conference Manager (MCM) gatekeeper. If you force a disconnect for either a particular call or all calls associated with a particular MCM gatekeeper by using the **clear h323 gatekeeper call** command, the system does not display information about those calls.

**Examples** The following is sample output from this command:

```
Router# show gatekeeper calls

Total number of active calls = 1.
                        GATEKEEPER CALL INFO
                        =====
LocalCallID           Age (secs)   BW
12-3339                94          768 (Kbps)
  Endpt(s):Alias      E.164Addr   CallSignalAddr  Port  RASignalAddr  Port
  src EP:epA          10.0.0.0    1720            10.0.0.0  1700
  dst EP:epB@zoneB.com
  src PX:pxA          10.0.0.0    1720            10.0.0.00  24999
  dst PX:pxB          255.255.255.0  1720            255.255.255.0  24999
```

Table 58 describes significant fields shown in this output.

**Table 64** *show gatekeeper calls Field Descriptions*

Field	Description
LocalCallID	Identification number of the call.
Age(secs)	Age of the call, in seconds.
BW(Kbps)	Bandwidth in use, in kilobytes per second.
Ends	Role of each endpoint (terminal, gateway, or proxy) in the call (originator, target, or proxy) and the call signaling and Registration, Admission, and Status (RAS) protocol address.
Alias	H.323-Identification (ID) or Email-ID of the endpoint.
E.164Addr	E.164 address of the endpoint.
CallSignalAddr	Call-signaling IP address of the endpoint.
Port	Call-signaling port number of the endpoint.
RASSignalAddr	RAS IP address of the endpoint.
Port	RAS port number of the endpoint.

#### Related Commands

Command	Description
<b>clear h323 gatekeeper call</b>	Forces the disconnection of a specific call or of all calls active on a particular gatekeeper.

# show gatekeeper circuits

To display the circuit information on a gatekeeper, use the **show gatekeeper circuits** command in privileged EXEC mode.

**show gatekeeper circuits** [**begin** | **exclude** | **include**] *expression*

Syntax Description	Parameter	Description
	<b>begin</b>	(Optional) Displays all circuits, beginning with the line containing the expression.
	<b>exclude</b>	(Optional) Displays all circuits, excluding those containing the expression.
	<b>include</b>	(Optional) Displays all circuits, including those containing the expression.
	<i>expression</i>	(Optional) Word or phrase used to determine what lines are displayed.

**Defaults** Shows all circuit information.

**Command Modes** Privileged EXEC

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

**Usage Guidelines** Use this command to display current configuration information about the circuits that are registered with the gatekeeper.

**Examples** The following command displays the circuit information for the gatekeeper:

```
Router# show gatekeeper circuits

Circuit      Endpoint    Max Calls Avail Calls Resources      Zone
-----
CarrierA     Total Endpoints: 2
              3640-gw1   25         25         Available
              5400-gw1   23         19         Unavailable
CarrierB     Total Zones: 1
                                                    MsPacmanGK
```

[Table 59](#) describes the fields shown in this output.

**Table 65** *show gatekeeper circuits Field Descriptions*

Field	Description
Circuit	Name of the each circuit connected to the gatekeeper.
Endpoint	Name of each H.323 endpoint.
Max Calls	Maximum number of calls that circuit can handle.

**Table 65** *show gatekeeper circuits Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Avail Calls	Number of new calls that the circuit can handle at the current time.
Resources	Whether the circuit's resources have exceeded the defined threshold limits. The <b>endpoint resource-threshold</b> command defines these thresholds.
Zone	Zone that supports the endpoint. The <b>zone circuit-id</b> command assigns a zone to an endpoint.
Total Endpoints	Total number of endpoints supported by the circuit.
Total Zones	Total number of zones supported by the circuit.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>endpoint resource-threshold</b>	Sets a gateway's capacity thresholds in the gatekeeper.
<b>zone circuit-id</b>	Assigns a remote zone to a carrier.

# show gatekeeper cluster

To display all the configured clusters and to provide validation of the configuration, use the **show gatekeeper cluster** command in privileged EXEC mode.

**show gatekeeper cluster**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.2(2)XB1	This command was implemented on the Cisco AS5850.

**Examples** The following is sample output from this command:

```
Router# show gatekeeper cluster

                CONFIGURED CLUSTERS
                =====
Cluster Name    Type      Local Zone  Elements  IP
-----
Cluster A      Local    AGK1        AGK2      192.168.200.254 1719
                AGK3      192.168.200.223 1719
Cluster B      Remote   BGK1        BGK1      192.168.200.257 1719
                BGK2      192.168.200.258 1719
                BGK3      192.168.200.259 1719
```

Related Commands	Command	Description
	<b>show gatekeeper endpoints</b>	Displays the status of all registered endpoints for a gatekeeper.
	<b>show gatekeeper performance statistics</b>	Displays information about the number of calls accepted and rejected and finds the number of endpoints sent to other gatekeepers.
	<b>show gatekeeper zone cluster</b>	Displays the dynamic status of all local clusters.

# show gatekeeper endpoint circuits

To display the information of all registered endpoints and carriers or trunk groups for a gatekeeper, use the **show gatekeeper endpoint circuits** command in privileged EXEC mode.

```
show gatekeeper endpoint circuits [{begin | exclude | include} expression]
```

## Syntax Description

<b>  begin</b>	(Optional) Displays all circuits, beginning with the line that contains <i>expression</i> .
<b>  exclude</b>	(Optional) Displays all circuits, excluding those that contain <i>expression</i> .
<b>  include</b>	(Optional) Displays all circuits, including those that contain <i>expression</i> .
<i>expression</i>	(Optional) Word or phrase used to determine what lines are displayed.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.
12.2(11)T	The display format was modified to show the E.164 ID, carrier and trunk group data, and total number of active calls.

## Usage Guidelines

Use this command to display current configuration information about the endpoints and carriers registered with the gatekeeper. Note that you must type the pipe (|) before any of the optional keywords.

## Examples

The following command displays the circuit information for the gatekeeper:

```
Router# show gatekeeper endpoint circuits

                        GATEKEEPER ENDPOINT REGISTRATION
                        =====
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name          Type  Flags
-----
172.18.195.120  1720  172.18.195.120  51059  LavenderGK        VOIP-GW
      E164-ID: 4081234
      H323-ID: 3640-gw1
      Carrier: CarrierA, Max Calls: 25, Available: 25
172.18.197.143  1720  172.18.197.143  57071  LavenderGK        VOIP-GW
      H323-ID: 5400-gw1
      Carrier: CarrierB, Max Calls: 23, Available: 19
      Carrier: CarrierA, Max Calls: 25, Available: 25
Total number of active registrations = 2
```

Table 66 describes the fields shown in this output.

**Table 66** show gatekeeper endpoint circuits Fields

Field	Description
CallSignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with an alias, a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	RAS IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper ID) that this endpoint registered in.
Type	Endpoint type (for example, terminal, gateway, or MCU).
Flags	S—Endpoint is statically entered from the <b>alias</b> command rather than being dynamically registered through RAS messages. O—Endpoint, which is a gateway, has sent notification that it is nearly out of resources.
E164-ID	E.164 ID of the endpoint.
H323-ID	H.323 ID of the endpoint.
Carrier	Carrier associated with the endpoint.
Max Calls	Maximum number of calls the circuit can handle.
Available	Number of new calls the circuit can handle currently.

**Related Commands**

Command	Description
<b>endpoint circuit-id h323id</b>	Assigns a circuit to a non-Cisco endpoint.
<b>endpoint resource-threshold</b>	Sets a gateway's capacity thresholds in the gatekeeper.
<b>zone circuit-id</b>	Assigns a circuit to a remote zone.

# show gatekeeper endpoints

To display the status of all registered endpoints for a gatekeeper, use the **show gatekeeper endpoints** command in privileged EXEC mode.

**show gatekeeper endpoints** [**alternates**]

<b>Syntax Description</b>	<b>alternates</b>	(Optional) Displays information about alternate endpoints. All information normally included with this command is also displayed.
---------------------------	-------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3(2)NA	This command was introduced.
	12.0(5)T	The display format was modified for H.323 Version 2.
	12.1(5)XM	The <b>alternates</b> keyword was added.
	12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
	12.2(2)XB1	This command was implemented on the Cisco AS5850.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. The registration and call capacity values were added to the output display.
	12.3(1)	This command was modified to reflect concurrent calls for the endpoints.

## Examples

The following is sample output from this command:

```
Router# show gatekeeper endpoints

CallsignalAddr  Port  RASSignalAddr  Port  Zone Name  Type  F
-----
172.21.127.8    1720  172.21.127.8   24999  sj-gk      MCU   --
      H323-ID:joe@cisco.com
      Voice Capacity Max.=23  Avail.=23
      Total number of active registrations = 1
172.21.13.88   1720  172.21.13.88   1719   sj-gk      VOIP-GW  0   H323-ID:1a-gw
```

Table 67 describes significant fields shown in this output.

**Table 67** show gatekeeper endpoints Field Descriptions

Field	Description
CallSignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with an alias (or aliases), a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	Registration, Admission, and Status (RAS) protocol IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper identification [ID]) to which this endpoint is registered.
Type	Endpoint type (for example, terminal, gateway, or multipoint control unit [MCU]).
F	S—Endpoint is statically entered from the <b>alias</b> command rather than being dynamically registered through RAS messages. O—Endpoint, which is a gateway, has sent notification that it is nearly out of resources.
Voice Capacity Max.	Maximum number of channels available on the endpoint.
Avail.	Current number of channels available on the endpoint.
Total number of active registrations	Total number of endpoints registered with the gatekeeper.

In the following example, the **show gatekeeper endpoints** output has been modified to reflect concurrent calls for the endpoint. If an endpoint is not reporting capacity and the **endpoint max-calls h323id** command is not configured, “Voice Capacity Max.” and “Avail.” will not be shown. “Current.= 2” indicates that the current active calls for the endpoint are 2.

```
Router# show gatekeeper endpoints
!
                        GATEKEEPER ENDPOINT REGISTRATION
                        =====
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name        Type  Flags
-----
172.18.200.27  1720  172.18.200.27  49918  GK-1              VOIP-GW
      H323-ID:GW1
      Voice Capacity Max.=  Avail.=  Current.= 2
```

If an endpoint is reporting capacity but the **endpoint max-calls h323id** command is not configured, “Voice Capacity Max.” and “Avail.” will show reported call capacity of the endpoint as follows:

```
Router# show gatekeeper endpoints
!
                        GATEKEEPER ENDPOINT REGISTRATION
                        =====
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name        Type  Flags
-----
172.18.200.29  1720  172.18.200.29  53152  GK-2              VOIP-GW
      H323-ID:GW2
      Voice Capacity Max.= 23  Avail.= 22  Current.= 1
```

If an endpoint is reporting capacity but the **endpoint max-calls h323id** command is not configured, “Voice Capacity Max.” will show the maximum calls configured and “Avail.” will show the available calls of the endpoint. In this example, “Voice Capacity Max.= 10” is showing that the maximum calls configured for the endpoint are 10. “Avail.= 2” shows that currently available calls for the endpoint are 2. “Current.= 8” shows that current active calls for the endpoint are 8.

```
Router# show gatekeeper endpoints
!
                                GATEKEEPER ENDPOINT REGISTRATION
                                =====
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name          Type      Flags
-----
172.18.200.27   1720  172.18.200.27  49918  GK-1               VOIP-GW
H323-ID:GW1
Voice Capacity Max.= 10  Avail.= 2  Current.= 8
```

Table 67 describes significant fields in the output examples.

**Table 68** *show gatekeeper endpoints Field Descriptions*

Field	Description
CallSignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with an alias (or aliases), a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	Registration, Admission, and Status (RAS) protocol IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper ID) to which this endpoint is registered.
Type	The endpoint type (for example, terminal, gateway, or multipoint control unit [MCU]).
Flags	S—Endpoint is statically entered from the <b>alias</b> command rather than being dynamically registered through RAS messages. O—Endpoint, which is a gateway, has sent notification that it is nearly out of resources.

#### Related Commands

Command	Description
<b>endpoint resource-threshold</b>	Sets a gateway’s capacity thresholds in the gatekeeper.
<b>show gatekeeper endpoint circuits</b>	Displays endpoint and carrier or trunk group call capacities.
<b>show gatekeeper gw-type-prefix</b>	Displays the gateway technology prefix table.
<b>show gatekeeper zone status</b>	Displays the status of zones related to a gatekeeper.
<b>show gateway</b>	Displays the current gateway status.

# show gatekeeper gw-type-prefix

To display the gateway technology prefix table, use the **show gatekeeper gw-type-prefix** command in privileged EXEC mode.

## show gatekeeper gw-type-prefix

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(5)T	The display format was modified for H.323 Version 2.
	12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
	12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
	12.2(2)XB1	This command was implemented on the Cisco AS5850.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

**Examples** The following is sample output from this command for a gatekeeper that controls two local zones, sj-gk and la-gk:

```
Router# show gatekeeper gw-type-prefix

GATEWAY TYPE PREFIX TABLE
=====
Prefix:12#*      (Default gateway-technology)
  Zone sj-gk master gateway list:
    10.0.0.0:1720 sj-gw1
    10.0.0.0:1720 sj-gw2 (out-of-resources)
    10.0.0.0:1720 sj-gw3
  Zone sj-gk prefix 408..... priority gateway list(s):
  Priority 10:
    10.0.0.0:1720 sj-gw1
  Priority 5:
    10.0.0.0:1720 sj-gw2 (out-of-resources)
    10.0.0.0:1720 sj-gw3
Prefix:7#*      (Hopoff zone la-gk)
  Statically-configured gateways (not necessarily currently registered):
    10.0.0.0:1720
    10.0.0.0:1720
  Zone la-gk master gateway list:
    10.0.0.0:1720 la-gw1
    10.0.0.0:1720 la-gw2
```

Table 69 describes significant fields shown in this output.

**Table 69** *show gatekeeper gw-type-prefix Field Descriptions*

Field	Description
Prefix	Technology prefix defined with the <b>gw-type-prefix</b> command.
Zone sj-gk master gateway list	List of all the gateways registered to zone sj-gk with the technology prefix under which they are listed. (This display shows that gateways sj-gw1, sj-gw2, and sj-gw3 have registered in zone sj-gk with the technology prefix 12#.)
Zone sj-gk prefix 408..... priority gateway list(s)	List of prioritized gateways to handle calls to area code 408.
Priority 10	Highest priority level. Gateways listed following “Priority 10” are given the highest priority when selecting a gateway to service calls to the specified area code. (In this display, gateway sj-gw1 is given the highest priority to handle calls to the 408 area code.)
Priority 5	Any gateway that does not have a priority level assigned to it defaults to priority 5.
(out-of-resources)	Indication that the displayed gateway has sent a “low-in-resources” notification.
(Hopoff zone la-gk)	Any call that specifies this technology prefix should be directed to hop off in the la-gk zone, no matter what the area code of the called number is. (In this display, calls that specify technology prefix 7# are always routed to zone la-gk, regardless of the actual zone prefix in the destination address.)
Zone la-gk master gateway list	List of all the gateways registered to la-gk with the technology prefix under which they are listed. (This display shows that gateways la-gw1 and la-gw2 have registered in zone la-gk with the technology prefix 7#. No priority lists are displayed here because none were defined for zone la-gk.)
(Default gateway-technology)	If no gateway-type prefix is specified in a called number, then gateways that register with 12# are the default type to be used for the call.
Statically-configured gateways	List of all IP addresses and port numbers of gateways that are incapable of supplying technology-prefix information when they register. This display shows that, when gateways 1.1.1.1:1720 and 2.2.2.2:1720 register, they are considered to be of type 7#.

#### Related Commands

Command	Description
<b>show gatekeeper calls</b>	Displays the status of each ongoing call of which a gatekeeper is aware.
<b>show gatekeeper endpoints</b>	Displays the status of all registered endpoints for a gatekeeper.
<b>show gateway</b>	Displays the current gateway status.

# show gatekeeper performance statistics

To display information about the number of calls accepted and rejected and to find the number of endpoints sent to other gatekeepers, use the **show gatekeeper performance statistics** command in privileged EXEC mode.

**show gatekeeper performance statistics** [**zone** [**name** *zone-name*]] [**cumulative**]

## Syntax Description

<b>zone</b>	(Optional) Zone statistics for the gatekeeper.
<b>name</b>	(Optional) Zone name or gatekeeper name.
<i>zone-name</i>	Local zone name.
<b>cumulative</b>	(Optional) Total statistics collected by the gatekeeper since the last reload. These values are not reset by the <b>clear h323 gatekeeper statistics</b> command.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T1	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(15)T	The <b>zone</b> , <b>name</b> , and <b>cumulative</b> keywords were added and <i>zone-name</i> argument was added.

## Usage Guidelines

Use this command to display the number of calls accepted, the number of calls rejected because of overload, and the number of endpoints sent to other gatekeepers.

When you enter this command, statistical data that relates to the router is displayed. You can identify the number of call initiation events using the following:

- Automatic repeat request (ARQ)
- Admission confirmation (ACF)
- Admission rejection (ARJ)

You can identify endpoint contact events that have been requested and either confirmed or rejected on the router using the following:

- Location request (LRQ)
- Location confirm (LCF)
- Location reject (LRJ)

The counts associated with overload and the number of endpoints sent to alternate gatekeepers that are associated with overload conditions are also displayed. Only when the router experiences an overload condition do these counters reveal a value other than zero. The real endpoint count simply displays the number of endpoints registered on this router platform. The time stamp displays the start time when the counters started capturing the data. When you want to request a new start period, enter the **clear h323 gatekeeper statistics** command. The counters are reset and the time stamp is updated with the new time.

You can identify endpoint contact events that have been requested and either confirmed or rejected on the router using the following:

- Location confirm (LCF)
- Location rejection (LRJ)
- Location request (LRQ)

You can identify zone-level registration statistics using the following:

- Registration confirmation (RCF)
- Registration rejection (RRJ)
- Registration request (RRQ)

You can identify zone-level unregistration statistics using the following:

- Unregistration confirmation (UCF)
- Unregistration rejection (URJ)
- Unregistration request (URQ)

## Examples

The following is sample output from this command:

```
Router# show gatekeeper performance statistics

Performance statistics captured since:00:14:02 UTC Mon Mar 1 1993

RAS inbound message counters:
  Originating ARQ:4      Terminating ARQ:1      LRQ:7
RAS outbound message counters:
  ACF:5 ARJ:0 LCF:7 LRJ:0
  ARJ due to overload:0
  LRJ due to overload:0

Load balancing events:0
Real endpoints:2
```

The following is sample BASIC output from the **show gatekeeper performance stats** command:

```
Router# show gatekeeper performance stats

-----Gatekeeper Performance Statistics-----

Performance statistics captured since: 00:17:00 UTC Mon Mar 1 1993

Gatekeeper level Admission Statistics:
  ARQs received: 1
  ARQs received from originating endpoints: 0
  ACFs sent: 1
  ACFs sent to the originating endpoint: 0
  ARJs sent: 0
  ARJs sent to the originating endpoint: 0
  ARJs sent due to overload: 0
  Number of concurrent calls: 0
```

```

Number of concurrent originating calls: 0

Gatekeeper level Location Statistics:
  LRQs received: 1
  LRQs sent: 0
  LCFs received: 0
  LCFs sent: 1
  LRJs received: 0
  LRJs sent: 0
  LRJs sent due to overload: 0

Gatekeeper level Registration Statistics:
  RRJ due to overload: 0
  Total Registered Endpoints: 1

Gatekeeper level Disengage Statistics:
  DRQs received: 1
  DRQs sent: 0
  DCFs received: 0
  DCFs sent: 1
  DRJs received: 0
  DRJs sent: 0
!
Load balancing events: 0

```

The following CUMULATIVE sample output is the same as for BASIC output; the difference is that the BASIC counters are cleared by the **clear h323 gatekeeper statistics** command and CUMULATIVE counters are not.

```

Router# show gatekeeper performance stats zone name voip3-2600-2

Performance statistics for zone voip3-2600-2

-----Zone Level Performance Statistics-----

Performance statistics captured since: 00:17:00 UTC Mon Mar 1 1993

Zone level Admission Statistics:
  ARQs received: 1
  ARQs received from originating endpoints: 0
  ACFs sent: 1
  ACFs sent to the originating endpoint: 0
  ARJs sent: 0
  ARJs sent to the originating endpoint: 0
  Number of concurrent total calls: 0
  Number of concurrent originating calls: 0

Zone level Location Statistics:
  LRQs received: 1
  LRQs sent: 0
  LCFs received: 0
  LCFs sent: 1
  LRJs received: 0
  LRJs sent: 0

Zone level Registration Statistics:
  Full RRQs received: 1
  Light RRQs received: 574
  RCFs sent: 576
  RRJs sent: 0
  Total Registered Endpoints: 1

Zone level UnRegistration Statistics:
  URQs received: 0

```

```

URQs sent: 0
UCFs received: 0
UCFs sent: 0
URJs received: 0
URJs sent: 0
URQs sent due to timeout: 0

```

Zone level Disengage Statistics:

```

DRQs received: 1
DRQs sent: 0
DCFs received: 0
DCFs sent: 1
DRJs received: 0
DRJs sent: 0

```

Table 70 shows significant fields shown in the displays. Most of the fields are self-explanatory and are not listed in the table.

**Table 70** *show gatekeeper performance statistics* Field Descriptions

Field	Description
Full RRQs received	A full registration request (RRQ) contains all registration information that is used to establish or change a registration.
Light RRQs received	A light RRQ contains abbreviated registration information that is used to maintain an existing registration.

#### Related Commands

Command	Description
<b>clear h323 gatekeeper statistics</b>	Clears statistics about gatekeeper performance.

*ft\_gms.fm kfulton 2/4/03*

# show gatekeeper servers

To display a list of currently registered and statically configured triggers on a gatekeeper router, use the **show gatekeeper servers** command in EXEC mode.

**show gatekeeper servers** [*gkid*]

<b>Syntax Description</b>	<i>gkid</i> (Optional) Local gatekeeper name to which this trigger applies.
---------------------------	---

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(1)T	This command was introduced on the Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200, and Cisco MC3810.
	12.2(2)XB	The output of this command was modified to show additional server statistics, including the following: gatekeeper server timeout value; Gatekeeper Transaction Message Protocol (GKTMP) version installed; number of Registration Request (RRQ), Registration Response (RRQ), Response Confirmation (RCF), and Response Reject (RRJ) messages received; timeouts encountered; average response time; and if the server is usable.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
	12.2(11)T	This command was implemented on the Cisco 3700 series.
	12.2(15)T12	The command was modified to show additional server statistics.
	12.3(8)T	The command was modified to show additional server statistics.
	12.3(9)	The command was modified to show additional server statistics.

**Usage Guidelines** Use this command to show all server triggers (whether dynamically registered from the external servers or statically configured from the command-line interface) on this gatekeeper. If the gatekeeper ID is specified, only triggers applied to the specified gatekeeper zone appear. If the gatekeeper ID is not specified, server triggers for all local zones on this gatekeeper appear.

**Examples** The following is sample output from this command:

```
Router# show gatekeeper servers

GATEKEEPER SERVERS STATUS
=====

Gatekeeper Server listening port: 8250
Gatekeeper Server timeout value: 30 (100ms)
GateKeeper GKTMP version: 4.1

Gatekeeper-ID: Gatekeeper1
-----
RRQ Priority: 5
```

```

Server-ID: Server43
Server IP address: 209.165.200.254:40118
Server type: dynamically registered
Connection Status: active
Trigger Information:
Trigger unconditionally
Server Statistics:
REQUEST RRQ Sent=0
RESPONSE RRQ Received = 0
RESPONSE RCF Received = 0
RESPONSE RRJ Received = 0
Average response time(ms)=0
Server Usable=TRUE

```

Timeout Statistics:

```

Server-ID: Server43
Server IP address: 209.165.200.254:40118
Server type: dynamically registered
Connection Status: active
Timeout Encountered=0

```

Table 71 describes significant fields shown in this output.

**Table 71** show gatekeeper servers Field Descriptions

Field	Description
GateKeeper GKTMP version	Version of Gatekeeper Transaction Message Protocol installed.
RRQ Priority	Registration priority.
Server-ID	Server ID name.
Server IP address	Server IP address.
Server type	Type of server.
Connection Status	Whether the connection is active or inactive.
Trigger Information	Which Registration, Admission, and Status (RAS) messages the Cisco IOS gatekeeper forwards to the external application.
REQUEST RRQ	Registration requests received.
RESPONSE RRQ	Registration responses received.
RESPONSE RCF	Response confirmations received.
RESPONSE RRJ	Response reject messages received.

**Related Commands**

Command	Description
<b>debug gatekeeper server</b>	Traces all the message exchanges between the Cisco IOS gatekeeper and the external applications.
<b>endpoint circuit-id h323id</b>	Tracks call capacity information on the gatekeeper.
<b>server registration-port</b>	Configures a listening port on the gatekeeper for server registration.
<b>server trigger arq</b>	Configures static triggers on the gatekeeper.

# show gatekeeper status

To display overall gatekeeper status, including authorization and authentication status and zone status, use the **show gatekeeper status** command in EXEC mode.

## show gatekeeper status

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
	12.1(5)XM	This command was modified to show information about load balancing and vendor-specific attributes.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.2(2)XB	This command was modified to show information about server flow control.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

**Examples** The following is sample output from this command:

```
Router# show gatekeeper status

Gatekeeper State: UP
  Load Balancing:  DISABLED
  Flow Control:    ENABLED
  Zone Name:       snet-3660-3
  Accounting:      DISABLED
  Endpoint Throttling:  DISABLED
  Security:        DISABLED
  Maximum Remote Bandwidth:          unlimited
  Current Remote Bandwidth:          0 kbps
  Current Remote Bandwidth (w/ Alt GKs): 0 kbps
```

Table 72 describes significant fields shown in this output.

**Table 72** *show gatekeeper status Field Descriptions*

Field	Description
Gatekeeper State	Gatekeeper state has the following values: <ul style="list-style-type: none"> <li>• UP is operational.</li> <li>• DOWN is administratively shut down.</li> <li>• INACTIVE is administratively enabled; that is, the <b>no shutdown</b> command has been issued, but no local zones have been configured.</li> <li>• HSRP STANDBY indicates that the gatekeeper is on hot standby and will take over when the currently active gatekeeper fails.</li> </ul>
Load Balancing	Whether load balancing is enabled.
Flow Control	Whether server flow control is enabled.
Zone Name	Zone name to which the gatekeeper belongs.
Accounting	Whether authorization and accounting features are enabled.
Endpoint Throttling	Whether endpoint throttling is enabled.
Security	Whether security features are enabled.
Bandwidth	Maximum remote bandwidth, current remote bandwidth, and current remote bandwidth with alternate gatekeepers.

#### Related Commands

Command	Description
<b>show gatekeeper servers</b>	Displays statistics about the gatekeeper.

# show gatekeeper status cluster

To display information about each element of a local cluster, such as the amount of memory used, the number of active calls, and the number of endpoints registered on the element, use the **show gatekeeper status cluster** command in privileged EXEC mode.

**show gatekeeper status cluster**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(5)XM1	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.2(2)XB1	This command was implemented on the Cisco AS5850.

**Examples** The following command displays information about elements of a local cluster, two of whose components are RoseGK and LavenderGK:

```
Router# show gatekeeper status cluster

                CLUSTER INFORMATION
                =====
Hostname      %Mem  %CPU  Active  Endpoint  Last
-----      -
RoseGK        72    0     1     Local Host
LavenderGK    30    1     0         4         14s
```

Related Commands	Command	Description
	<b>show gatekeeper endpoints</b>	Displays the status of all registered endpoints for a gatekeeper.
	<b>show gatekeeper performance statistics</b>	Displays information about the number of calls accepted and rejected, and finds the number of endpoints sent to other gatekeepers.
	<b>show gatekeeper zone cluster</b>	Displays the dynamic status of all local clusters.

# show gatekeeper zone cluster

To display the dynamic status of all local clusters, use the **show gatekeeper zone cluster** command in privileged EXEC mode.

## show gatekeeper zone cluster

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(5)XM1	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.2(2)XB1	This command was implemented on the Cisco AS5850.

**Examples** The following command displays information about the current bandwidth values and about when the last announcement message from the alternate gatekeeper was received. In the following example, PRI represents the priority value assigned to an alternate gatekeeper. This field ranges from 0 to 127, with 127 representing the lowest priority.

Router# **show gatekeeper zone cluster**

```

LOCAL CLUSTER INFORMATION, 6t
=====
LOCAL GK NAME   ALT GK NAME   PRI  TOT BW  INT BW  REM BW  LAST ANNOUNCE  ALT GK STATUS
-----
ParisGK         GenevaGK      120  0       0       0       7s             CONNECTED
NiceGK          ZurichGK     100  0       0       0       7s             CONNECTED

```

Related Commands	Command	Description
	<b>timer cluster-element announce</b>	Defines the time interval between successive announcement messages exchanged between elements of a local cluster.
	<b>zone cluster local</b>	Defines a local grouping of gatekeepers.
	<b>zone remote</b>	Statically specifies a remote zone if DNS is unavailable or undesirable.

# show gatekeeper zone prefix

To display the zone prefix table, use the **show gatekeeper zone prefix** command in privileged EXEC mode.

**show gatekeeper zone prefix [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays the dynamic zone prefixes registered by each gateway.
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3(2)NA	This command was introduced.
12.2(15)T	The <b>all</b> keyword was added.	

**Usage Guidelines** If the **all** keyword is not specified, the **show gatekeeper zone prefix** command displays the static zone prefixes only. Use the **include** filter with the **all** keyword to display the prefixes associated with a particular gateway. For example, the **show gatekeeper zone prefix all | include GW1** command displays the dynamic prefixes associated with gateway GW1.

**Examples** The following command displays the zone prefix table for the gatekeeper:

```
Router# show gatekeeper zone prefix
```

```

ZONE PREFIX TABLE
=====
GK-NAME          E164-PREFIX
-----          -
gk2              408*
gk2              5551001*
gk2              5551002*
gk2              5553020*
gk2              5553020*
gk1              555...
gk2              719*
gk2              919*
    
```

The following command displays the zone prefix table, including the dynamic zone prefixes, for the gatekeeper:

```
Router# show gatekeeper zone prefix all
```

```

ZONE PREFIX TABLE
=====
GK-NAME          E164-PREFIX          Dynamic GW-priority
-----          -
gk2              408*
gk2              5551001*            GW1 /5
gk2              5551002*            GW1 /5 GW2 /10
    
```

```

gk2          5553020*          GW1 /8
gk2          5553020*
gk1          555...
gk2          719*
gk2          919*            GW2 /5

```

Table 73 describes significant fields shown in this output.

**Table 73** show gatekeeper zone prefix Field Descriptions

Field	Description
GK-NAME	Gatekeeper name.
E164-PREFIX	E.164 prefix and a dot that acts as a wildcard for matching each remaining number in the telephone number.
Dynamic GW-priority	Gateway that serves this E164 prefix.  Gateway priority. A 0 value prevents the gatekeeper from using the gateway for that prefix. Value 10 places the highest priority on the gateway. The default priority value for a dynamic gateway is 5.

# show gatekeeper zone status

To display the status of zones related to a gatekeeper, use the **show gatekeeper zone status** command in privileged EXEC mode.

## show gatekeeper zone status

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(5)T	The display format was modified for H.323 Version 2.
	12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
	12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
	12.2(2)XB1	This command was implemented on the Cisco AS5850.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

**Examples** The following is sample output from this command:

```
Router# show gatekeeper zone status

                        GATEKEEPER ZONES
                        =====
GK name      Domain Name  RAS Address  PORT  FLAGS  MAX-BW  CUR-BW
-----      -
sj.xyz.com   xyz.com      10.0.0.0     1719  LS          (kbps)  (kbps)
-----      -
SUBNET ATTRIBUTES :
  All Other Subnets : (Enabled)
PROXY USAGE CONFIGURATION :
  inbound Calls from germany.xyz.com :
    to terminals in local zone sj.xyz.com :use proxy
    to gateways in local zone sj.xyz.com :do not use proxy
  Outbound Calls to germany.xyz.com
    from terminals in local zone germany.xyz.com :use proxy
    from gateways in local zone germany.xyz.com :do not use proxy
  Inbound Calls from all other zones :
    to terminals in local zone sj.xyz.com :use proxy
    to gateways in local zone sj.xyz.com :do not use proxy
  Outbound Calls to all other zones :
    from terminals in local zone sj.xyz.com :do not use proxy
    from gateways in local zone sj.xyz.com :do not use proxy
tokyo.xyz.co xyz.com      10.0.0.0     1719  RS          0
milan.xyz.co xyz.com      10.0.0.0     1719  RS          0
```

Table 74 describes significant fields shown in this output.

**Table 74** *show gatekeeper zone status Field Descriptions*

Field	Description
GK name	Gatekeeper name (also known as the zone name), which is truncated after 12 characters in the display.
Domain Name	Domain with which the gatekeeper is associated.
RAS Address	Registration, Admission, and Status (RAS) protocol address of the gatekeeper.
FLAGS	Displays the following information: <ul style="list-style-type: none"> <li>• S = static (CLI-configured, not DNS-discovered)</li> <li>• L = local</li> <li>• R = remote</li> </ul>
MAX-BW	Maximum bandwidth for the zone, in kbps.
CUR-BW	Current bandwidth in use, in kbps.
SUBNET ATTRIBUTES	List of subnets controlled by the local gatekeeper.
PROXY USAGE CONFIGURATION	Inbound and outbound proxy policies as configured for the local gatekeeper (or zone).

#### Related Commands

Command	Description
<b>show gatekeeper calls</b>	Displays the status of each ongoing call of which a gatekeeper is aware.
<b>show gatekeeper endpoints</b>	Displays the status of registered endpoints for a gatekeeper.
<b>show gateway</b>	Displays the current gateway status.

# show gateway

To display the current status of the gateway, use the **show gateway** command in privileged EXEC mode.

**show gateway**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.3(6)NA2	This command was introduced.
	12.0(5)T	The display format was modified for H.323 Version 2.
	12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
	12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
	12.2(2)XB1	This command was implemented on the Cisco AS5850.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

## Examples

The following sample output shows the report that appears when the gateway is not registered with a gatekeeper:

```
Router# show gateway

Gateway gateway1 is not registered to any gatekeeper
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Enabled but NOT Active
H323 resource threshold values:
    DSP: Low threshold 60, High threshold 70
    DS0: Low threshold 60, High threshold 70
```

This following sample output indicates that an E.164 address has been assigned to the gateway:

```
Router# show gateway

Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
E.164 Number 5551212
H323-ID gateway1
```

The following sample output shows the report that appears when the gateway is registered with a gatekeeper and H.323 resource threshold reporting is enabled with the **resource threshold** command:

```
Router# show gateway

Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Enabled and Active
```

```
H323 resource threshold values:
  DSP: Low threshold 60, High threshold 70
  DSO: Low threshold 60, High threshold 70
```

The following sample output shows the report that appears when the gateway is registered with a gatekeeper and H.323 resource threshold reporting is disabled with the **no resource threshold** command:

```
Router# show gateway

Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Disabled
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>resource threshold</b>	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.

---

# show h323 gateway

To display statistics for H.323 gateway messages that have been sent and received and to display the reasons for which H.323 calls have been disconnected, use the **show h323 gateway** command in privileged EXEC mode.

**show h323 gateway** [**cause-code stats** | **h225** | **ras**]

## Syntax Description

<b>cause-code stats</b>	(Optional) Output displays the disconnect cause codes that the H.323 subsystem has received. A disconnect can originate either from the far-end gateway or from the opposite call leg on the local gateway.
<b>h225</b>	(Optional) Output lists cumulative counts of the number of H.225 messages that have been sent and received since the counters were last cleared.
<b>ras</b>	(Optional) Output lists the counters for Registration, Admission, and Status (RAS) messages that have been sent to and received from the gatekeeper since the counters were last cleared.

## Defaults

To display statistics for all the options, use this command without any of the optional keywords.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(4)T	This command was introduced on Cisco H.323 platforms except for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

## Examples

In the following example from a Cisco 3640 router, this command is used without keywords to display the statistics for all the options. See [Table 75](#), [Table 76](#), and [Table 77](#) for descriptions of the fields.

```
Router# show h323 gateway

H.323 STATISTICS AT 01:45:55

H.225 REQUESTS      SENT      RECEIVED   FAILED
Setup               0         5477       0
Setup confirm       5424      0          0
Alert               2734      0          0
Progress            2701      0          0
Call proceeding     5477      0          0
Notify              0         0          0
Info                0         0          0
User Info           0         0          0
Facility            2732      0          0
Release             5198      5313       241
Reject              0         0          0
Passthrough         0         0          0

H225 establish timeout 0
RAS failed           0
```

```

H245 failed          0

RAS MESSAGE          REQUESTS SENT    CONFIRMS RCVD    REJECTS RCVD
GK Discovery         grq 0             gcf 0            grj 0
Registration         rrq 130          rcf 130          rrj 0
Admission            arq 5477         acf 5477         arj 0
Bandwidth           brq 0            bcf 0            brj 0
Disengage            drq 5439         dcf 5439         drj 0
Unregister           urq 0            ucf 0            urj 0
Resource Avail       rai 0            rac 0
Req In Progress     rip 0

RAS MESSAGE          REQUESTS RCVD    CONFIRMS SENT    REJECTS SENT
GK Discovery         grq 0            gcf 0            grj 0
Registration         rrq 0            rcf 0            rrj 0
Admission            arq 0            acf 0            arj 0
Bandwidth           brq 0            bcf 0            brj 0
Disengage            drq 0            dcf 0            drj 0
Unregister           urq 0            ucf 0            urj 0
Resource Avail       rai 0            rac 0
Req In Progress     rip 0

DISC CAUSE CODE      FROM OTHER PEER    FROM H323 PEER
16 normal call clearing 66                5325
31 normal, unspecified 1                  0
34 no circuit         31                0
41 temporary failure  3                  0
44 no requested circuit 13                0

```

In the following example from a Cisco 3640 router, this command is used with the **cause-code stats** keyword to display the disconnect cause codes that the H.323 subsystem has received. A disconnect can originate either from the far-end gateway or from the opposite call leg on the local gateway. Only the nonzero cause-code counts are displayed.

```

Router# show h323 gateway cause-code stats

CAUSE CODE STATISTICS AT 01:40:25

DISC CAUSE CODE      FROM OTHER PEER    FROM H323 PEER
16 normal call clearing 66                4976
31 normal, unspecified 1                  0
34 no circuit         31                0
41 temporary failure  3                  0
44 no requested circuit 13                0

```

[Table 75](#) describes significant fields shown in this output

**Table 75** show h323 gateway cause-code stats Field Descriptions

Field	Description
<b>Column Headings:</b>	
DISC CAUSE CODE	Decimal value of the cause code, followed by the textual description.
FROM OTHER PEER	Number of disconnects that have been received from the opposite call leg for each cause code (for example, from a PRI T1 POTS peer or a Foreign exchange station [FXS] POTS peer).
FROM H323 PEER	Number of disconnects that have been received from the far-end gateway for each cause code.

**Fields listed under the headings are self-explanatory.**

In the following example from a Cisco 3640 router, this command is used with the **h225** keyword to display the cumulative counts of the number of H.225 messages that were sent and received since the counters were last cleared.

Each row shows the sent, received, and failed counts for one type of H.225 request. If the counters have not been cleared, total counts are shown for the router since it was last reloaded.

```
Router# show h323 gateway h225

H.225 STATISTICS AT 00:44:57

H.225 REQUESTS      SENT      RECEIVED   FAILED
Setup               1654      0          0
Setup confirm       0         1654      0
Alert               0         828       0
Progress            0         826       0
Call proceeding     0         1654      0
Notify              0         0          0
Info                0         0          0
User Info           0         0          0
Facility            0         828       0
Release             1613      9          1
Reject              0         0          0
Passthrough         0         0          0

H225 establish timeout 0
RAS failed           1
H245 failed         0
```

Table 76 describes significant fields shown in this output.

**Table 76** show h323 gateway h225 Field Descriptions

Field	Description
<b>Column Headings:</b>	
H.225 REQUESTS	Types of H.225 messages.
SENT	Number of H.225 messages sent by the gateway.
RECEIVED	Number of H.225 messages received from a remote gateway or endpoint.
FAILED	Number of H.225 messages that could not be sent. A failure could occur if, for example, the H.323 subsystem tried to send an H.225 release request but the TCP socket had already been closed.
<b>Fields:</b>	
Setup	Number of setup messages that were sent, that were received, or that could not be sent. This message is sent by a calling H.323 entity to indicate its desire to set up a connection to the called entity.
Setup confirm	Number of setup confirm messages that were sent, that were received, or that could not be sent. This message may be sent by an H.323 entity to acknowledge receipt of a setup message.
Alert	Number of alert messages that were sent, that were received, or that could not be sent. This message may be sent by the called user to indicate that called user alerting has been initiated. (In everyday terms, the “phone is ringing.”)

**Table 76** show h323 gateway h225 Field Descriptions (continued)

Field	Description
Progress	Number of progress messages that were sent, that were received, or that could not be sent. This message may be sent by an H.323 entity to indicate the progress of a call.
Call proceeding	Number of call proceeding messages that were sent, that were received, or that could not be sent. This message may be sent by the called user to indicate that requested call establishment has been initiated and that no more call establishment information is accepted.
Notify	Number of notify messages that were sent, that were received, or that could not be sent.
Info	Number of information messages that were sent, that were received, or that could not be sent.
User Info	Number of user information messages that were sent, that were received, or that could not be sent. This message may be used to provide additional information for call establishment (for example, overlap signaling), to provide miscellaneous call-related information, or to deliver proprietary features.
Facility	Number of facility messages that were sent, that were received, or that could not be sent. This message is used to provide information on where a call should be directed or for an endpoint to indicate that the incoming call must go through a gatekeeper.
Release	Number of release complete messages that were sent, that were received, or that could not be sent. This message is sent by a gateway to indicate the release of the call if the reliable call signaling channel is open.
Reject	Number of reject messages that were sent, that were received, or that could not be sent.
Passthrough	Number of pass-through messages that were sent, that were received, or that could not be sent.
H225 establish timeout	Number of times the H.323 subsystem was unable to establish an H.225 connection to a remote gateway for a call.
RAS failed	Number of times an Admission Reject (ARJ) or Disengage Reject (DRJ) message is received from the gatekeeper. This counter should equal the arj + drj received counters shown in the <b>show h323 gateway ras</b> command output.
H245 failed	Number of times the H.323 subsystem was unable to create an H.245 tunnel for a call or was unable to send an H.245 message.

In the following example from a Cisco 3640 router, this command is used with the **ras** keyword to display the counters for Registration, Admission, and Status (RAS) messages that were sent to the gatekeeper and received from the gatekeeper. With the exception of the Resource Avail and Req In Progress messages, each RAS message has three variations: a request message, a confirm message, and a reject message. For example, for the Admission message type, there is an Admission Request (arq) message, an Admission Confirm (acf) message, and an Admission Reject (arj) message. The gateway sends the arq message, and the gatekeeper responds with either an acf or an arj message, depending on whether the gatekeeper confirms or rejects the admission request.

Each of the two tables that follow lists the same message types, with each row showing a different message type. The first table shows the requests sent, the confirms received, and the rejects received. The second table shows the requests received, the confirms sent, and the rejects sent. Some rows in the second table would apply only to the gatekeeper (for example, a gateway would never receive a Registration Request (rrq) message, send a Registration Confirmation (rcf) message, or send a Registration Rejection (rrj) message).

Router# **show h323 gateway ras**

RAS STATISTIC AT 01:10:01

```

RAS MESSAGE      REQUESTS SENT    CONFIRMS RCVD   REJECTS RCVD
GK Discovery     grq 3           gcf 1           grj 0
Registration     rrq 73          rcf 73          rrj 0
Admission       arq 3216        acf 3215        arj 1
Bandwidth       brq 0           bcf 0           brj 0
Disengage       drq 3174        dcf 3174        drj 0
Unregister       urq 0           ucf 0           urj 0
Resource Avail  rai 0           rac 0
Req In Progress rip 0
    
```

```

RAS MESSAGE      REQUESTS RCVD    CONFIRMS SENT   REJECTS SENT
GK Discovery     grq 0           gcf 0           grj 0
Registration     rrq 0           rcf 0           rrj 0
Admission       arq 0           acf 0           arj 0
Bandwidth       brq 0           bcf 0           brj 0
Disengage       drq 0           dcf 0           drj 0
Unregister       urq 0           ucf 0           urj 0
Resource Avail  rai 0           rac 0
Req In Progress rip 0
    
```

Table 77 describes significant fields shown in this output.

**Table 77 show h323 gateway ras Field Descriptions**

Field	Description
<b>Column Headings for the First Table:</b>	
RAS MESSAGE	Type RAS message.
REQUESTS SENT	Number of RAS request messages sent by the gateway to a gatekeeper.
CONFIRMS RCVD	Number of RAS confirmation messages received from a gatekeeper.
REJECTS RCVD	Number of RAS reject messages received from a gatekeeper.
<b>Column Headings for the Second Table:</b>	
RAS MESSAGE	Type of RAS message.
REQUESTS RCVD	Number of RAS request messages received from a gatekeeper.
CONFIRMS SENT	Number of RAS confirmation messages sent by the gateway.
REJECTS SENT	Number of RAS reject messages sent by the gateway.
<b>Fields:</b>	
GK Discovery	Gatekeeper Request (GRQ) message requests that any gatekeeper receiving it respond with a Gatekeeper Confirmation (GCF) message granting it permission to register. The Gateway Reject (GRJ) message is a rejection of this request, indicating that the requesting endpoint should seek another gatekeeper.

**Table 77** show h323 gateway ras Field Descriptions

Field	Description
Registration	Registration Request (RRQ) message is a request from a terminal to a gatekeeper to register. If the gatekeeper responds with a Registration Confirmation (RCF) message, the terminal uses the responding gatekeeper for future calls. If the gatekeeper responds with a Registration Reject (RRJ) message, the terminal must seek another gatekeeper with which to register.
Admission	Admission Request (ARQ) message requests that an endpoint be allowed access to the packet-based network by the gatekeeper, which either grants the request with an Admission Confirmation (ACF) message or denies it with an Admission Reject (ARJ) message.
Bandwidth	Bandwidth Request (BRQ) message requests that an endpoint be granted a changed packet-based network bandwidth allocation by the gatekeeper, which either grants the request with a Bandwidth Confirmation (BCF) message or denies it with a Bandwidth Reject (BRJ) message.
Disengage	If sent from an endpoint to a gatekeeper, the Disengage Request (DRQ) message informs the gatekeeper that an endpoint is being dropped. If sent from a gatekeeper to an endpoint, the DRQ message forces a call to be dropped; such a request is not refused. The DRQ message is not sent directly between endpoints.
Unregister	UnRegistration Request (URQ) message requests that the association between a terminal and a gatekeeper be broken. Note that the URQ request is bidirectional; that is, a gatekeeper can request a terminal to consider itself unregistered, and a terminal can inform a gatekeeper that it is revoking a previous registration.
Resource Avail	Resource Availability Indication (RAI) message is a notification from a gateway to a gatekeeper of its current call capacity for each H-series protocol and data rate for that protocol. The gatekeeper responds with a Resource Availability Confirmation (RAC) message upon receiving an RAI message to acknowledge its reception.
Req In Progress	Request In Progress (RIP) message can be used by a gateway or gatekeeper when a response to a message cannot be generated within a typical retry timeout period. The RIP message specifies the time period after which a response should have been generated.

# show h323 gateway prefixes

To display the status of the destination pattern database and the status of the individual destination patterns, use the **show h323 gateway prefixes** command in privileged EXEC mode.

## show h323 gateway prefixes

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(15)T	This command was introduced.

**Usage Guidelines** Use the **show h323 gateway prefixes** command to display the destination patterns from the active plain old telephone service (POTS) dial peers, the current state of the destination pattern (whether they have been sent to or acknowledged by the gatekeeper), and whether advertisement of dynamic prefixes is enabled on the gateway.

**Examples** The following command displays the status of the gateway’s destination pattern database:

```
Router# show h323 gateway prefixes

GK Supports Additive RRQ           : True
GW Additive RRQ Support Enabled    : True
Pattern Database Status            : Active

Destination                          Active
Pattern                               Status      Dial-Peers
=====
1110509*                             ADD ACKNOWLEDGED      2
1110511*                             ADD ACKNOWLEDGED      2
23*                                   ADD ACKNOWLEDGED      2
```

[Table 78](#) describes the significant fields shown in the display.

**Table 78** show h323 gateway prefixes Field Descriptions

Field	Description
Pattern Database Status	Status of the gateway's destination pattern database: active or inactive.
Status	<p>Status of the destination pattern. The status can be one of the following values:</p> <p><b>ADD PENDING</b>—The gateway has a prefix that is waiting to be sent to the gatekeeper. Prefixes are sent only at the lightweight registration request (RRQ) RAS message schedule, which is every 30 seconds.</p> <p><b>ADD SENT</b>—The gateway sent the prefix to the gatekeeper and is waiting for it to be acknowledged by a registration confirm (RCF) RAS message.</p> <p><b>ADD ACKNOWLEDGED</b>—The gateway received an RCF message indicating that the gatekeeper accepted the prefix. This is the normal status when dynamic zone prefix registration is working properly.</p> <p><b>ADD REJECTED</b>—The gatekeeper did not accept the prefix and sent a registration reject (RRJ) RAS message. One reason for rejection could be that the gatekeeper already has this prefix registered for a different zone, either by static zone prefix configuration, or because another gateway in a different zone dynamically registered this prefix first.</p> <p><b>DELETE PENDING</b>—The prefix has gone out of service, for example, because the dial peer shut down, and the gateway is waiting to send an unregistration request (URQ) RAS message to the gatekeeper to remove it. URQ messages are sent at the lightweight RRQ schedule, which is every 30 seconds.</p> <p><b>DELETE SENT</b>—The gateway sent a URQ message to remove the prefix to the gatekeeper. There is no DELETE ACKNOWLEDGED status. If the prefix is subsequently brought back in service, the status goes back to ADD PENDING.</p>

# show http client cache

To display information about the entries contained in the HTTP client cache, use the **show http client cache** command in EXEC mode.

**show http client cache [brief]**

<b>Syntax Description</b>	<b>brief</b> (Optional) Displays summary information about the HTTP client cache.
---------------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

**Usage Guidelines** For more information on HTTP caching, refer to the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1*, June 1999, IETF.

**Examples** The following is sample output from this command:

```
Router# show http client cache

HTTP Client cached information
=====
Maximum memory pool allowed for HTTP Client caching = 100000 K-bytes
Maximum file size allowed for caching = 10 K-bytes
Total memory used up for Cache = 18837 Bytes
Message response timeout = 10 secs
Total cached entries      = 5
Total non-cached entries = 0

                Cached entries
                =====
Cached table entry 167, number of cached entries = 2
Request URL           Ref  FreshTime  Age      Size
-----
abc.com/vxml/menu.vxml 0    20         703     319
abc.com/vxml/opr.vxml  0   647424    646     2772
Cached table entry 171, number of cached entries = 1
Request URL           Ref  FreshTime  Age      Size
-----
onlineshop.com/catalog/advance.vxml 0   69077     1297649 3453
Cached table entry 172, number of cached entries = 1
Request URL           Ref  FreshTime  Age      Size
-----
theater.com/vxml/menu_main.vxml 0   86400     1297661 8734
```

```

Cached table entry 176, number of cached entries = 1
Request URL                               Ref  FreshTime  Age      Size
-----
popcorn.com/menu/selection.vxml          1    20         7        3559

```

Table 79 describes the fields shown in this output.

**Table 79** show http client cache Field Descriptions

Field	Description
Maximum memory pool allowed for HTTP Client caching	Maximum amount of memory available for the HTTP client to store cached entries in kilobytes. This value is configured by using the <b>http client cache memory</b> command.
Maximum file size allowed for caching	Maximum size of a file that can be cached, in kilobytes. If a file exceeds this limit, it cannot be cached. This value is configured by using the <b>http client cache memory</b> command.
Total memory used up for Cache	Total amount of memory that is currently being used to store cached entries in kilobytes.
Total cached entries	Total number of cached entries.
Total non-cached entries	Total number of temporary, one-time used HTTP entries that are not currently cached.
Cached table entry	Index marker of the cached table entry. Each cached table entry can contain multiple URLs that were requested and cached.
number of cached entries	Number of URL entries in the cached table entry.
Request URL	URL of the cached entry.
Ref	Whether the cached entry is still in use by the application. 0 means the entry has been freed; 1 or more means that the entry is still being used by that number of applications.
FreshTime	Lifetime of a cached entry, in seconds. When an entry is the same age or older than the refresh time, the entry expires. When a request is made to a cached entry that has expired, the HTTP client sends the server a conditional request for an update.  This value is configured on the HTTP server or by using the <b>http client cache refresh</b> command on the gateway.
Age	Time for which the entry has been in the cache, in seconds.
Size	Size of the cached entry, in kilobytes.

#### Related Commands

Command	Description
<b>http client cache memory</b>	Configures the HTTP client cache.
<b>http client cache refresh</b>	Configures the HTTP client cache refresh time.
<b>http client response timeout</b>	Configures the HTTP client server response timeout.
<b>show http client connection</b>	Displays current HTTP client connection information.

# show http client connection

To display the current configuration values for HTTP client connections to HTTP servers, use the **show http client connection** command in EXEC mode.

**show http client connection**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

**Usage Guidelines** In this command, the values for the following commands are shown:

- **http client connection idle timeout** as “connection idle timeout”
- **http client connection persistent** as “persistent connection”
- **http client connection timeout** as “initial socket connection timeout”



**Note**

For more information on HTTP caching, refer to the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1*, June 1999, IETF.

**Examples** The following is sample output from this command:

```
Router# show http client connection

HTTP Client Connections:
=====
Persistent connection      = enabled
Initial socket connection timeout = 10 secs
Connection idle timeout   = 60 secs
Total HTTP server connections = 0
```

Table 80 describes the fields shown in this output.

**Table 80** *show http client connection Field Descriptions*

Field	Description
Persistent connection	Whether HTTP keepalive connections have been enabled by using the <b>http client connection persistent</b> command.
Initial socket connection timeout	Number of seconds for which the HTTP client waits for a server to establish a connection before giving up. This value is set by using the <b>http client connection timeout</b> command.
Connection idle timeout	Number of seconds for which the HTTP client waits before terminating an idle connection. This value is set by using the <b>http client connection idle timeout</b> command.
Total HTTP server connections	Total number of current connections to an HTTP server.

#### Related Commands

Command	Description
<b>http client cache memory</b>	Configures the HTTP client cache.
<b>http client connection idle timeout</b>	Sets the number of seconds for which the HTTP client waits before terminating an idle connection.
<b>http client connection persistent</b>	Enables HTTP persistent connections so that multiple files can be loaded using the same connection.
<b>http client connection timeout</b>	Sets the number of seconds for which the HTTP client waits for a server to establish a connection before giving up.
<b>http client response timeout</b>	Configures the HTTP client server response.

# show http client history

To display a list of the last 20 requests made by the HTTP client to the server, use the **show http client history** command in EXEC mode.

**show http client history**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

**Usage Guidelines** For more information on HTTP caching, refer to the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1*, June 1999, IETF.

**Examples** The following is sample output from this command, showing the most recent GET and POST requests from the HTTP client to the server:

```
Router# show http client history

POST http://banks.com/servlets/account
GET http://banks.com/GetDigit.vxml
GET http://banks.com/form.vxml
GET http://onlineshop.com/menu.vxml
POST http://onlineshop.com/servlets/order
GET http://weather.com/servlets/weather?city=SanFrancisco&state=CA
```

Related Commands	Command	Description
	<b>http client cache memory</b>	Configures the HTTP client cache.
	<b>http client response timeout</b>	Configures the HTTP client server response.
	<b>show http client connection</b>	Displays current HTTP client connection information.

# show interface dspfarm

To display digital signal processor (DSP) information on the two-port T1/E1 high-density port adapter for the Cisco 7200 series, use the **show interface dspfarm** command in privileged EXEC mode.

**show interface dspfarm** [*slot/port*] **dsp** [*number*] [**long** | **short**]

Syntax Description	
<i>slot</i>	(Optional) Slot location of the port adapter.
<i>/port</i>	(Optional) Port number on the port adapter.
<b>dsp</b>	DSP information.
<i>number</i>	(Optional) Number of DSP sets to show. Range is from 1 to 30.
<b>long</b>	(Optional) Detailed DSP information.
<b>short</b>	(Optional) Brief DSP information.

**Defaults** No default behavior or values

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(5)XE	This command was introduced on the Cisco 7200 series.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

**Usage Guidelines** You can display the local time-division multiplexing (TDM) cross-connect map by using the **show interface dspfarm <x/y | x/y/z> dsp tdm** command.

**Examples** The following is sample output from this command for port adapter slot 0 of chassis slot 3 on a Cisco 7200 series router:

```
Router# show interface dspfarm 3/0

DSPfarm3/0 is up, line protocol is up
Hardware is VXC-2T1/E1
MTU 256 bytes, BW 12000 Kbit, DLY 0 usec,
  reliability 255/255, txload 4/255, rxload 1/255
Encapsulation VOICE, loopback not set
C549 DSP Firmware Version:MajorRelease.MinorRelease (BuildNumber)
  DSP Boot Loader:255.255 (255)
  DSP Application:4.0 (3)
  Medium Complexity Application:3.2 (5)
  High Complexity Application:3.2 (5)
Total DSPs 30, DSP0-DSP29, Jukebox DSP id 30
Down DSPs:none
Total sig channels 120 used 24, total voice channels 120 used 0
  0 active calls, 0 max active calls, 0 total calls
  30887 rx packets, 0 rx drops, 30921 tx packets, 0 tx frags
```

```

0 curr_dsp_tx_queued, 29 max_dsp_tx_queued
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy:fifo
Output queue 0/0, 0 drops; input queue 0/75, 0 drops
5 minute input rate 13000 bits/sec, 94 packets/sec
5 minute output rate 193000 bits/sec, 94 packets/sec
 30887 packets input, 616516 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
30921 packets output, 7868892 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 output buffer failures, 0 output buffers swapped out

```

Table 81 describes significant fields shown in this output.

**Table 81** show interface dspfarm Field Descriptions

Field	Description
DSPfarm3/0 is up	DSPfarm interface is operating. The interface state can be up, down, or administratively down.
Line protocol is	Whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Version number of the hardware.
MTU	256 bytes.
BW	12000 kilobits.
DLY	Delay of the interface, in microseconds.
Reliability	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability, calculated as an expedient average over 5 minutes).
Txload	Number of packets sent.
Rxload	Number of packets received.
Encapsulation	Encapsulation method assigned to the interface.
Loopback	Loopback conditions.
C549 DSP Firmware Version	Version of DSP firmware installed.
DSP Boot Loader	DSP boot loader version.
DSP Application	DSP application code version.
Medium Complexity Application	DSP Medium Complexity Application code version.
High Complexity Application	DSP High Complexity Application code version.
Total DSPs	Total DSPs that are equipped in the PA.
DSP0-DSP	DSP number range.
Jukebox DSP id	Jukebox DSP number.
Down DSPs	DSPs not in service.
Total sig channels...used...	Total number of signal channels used.
Total voice channels...used...	Total number of voice channels used.
Active calls	Number of active calls.

**Table 81** show interface dspfarm Field Descriptions (continued)

Field	Description
Max active calls	Maximum number of active calls.
Total calls	Total number of calls.
Rx packets	Number of received (rx) packets.
Rx drops	Number of rx packets dropped at PA.
Tx packets	Number of transmit (tx) packets.
Tx frags	Number of tx packets that were fragmented.
Curr_dsp_tx_queued	Number of tx packets that are being queued at host DSP queues.
Max_dsp_tx_queued	The max total tx packets that were queued at host DSP queues.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched and not when packets are fast switched.
Output	Number of hours, minutes, and seconds since the last packet was successfully sent by the interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched and not when packets are fast switched.
Output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks (**) are printed.
Last clearing of “show interface” counters	Number of times the “show interface” counters were cleared.
queueing strategy	First-in, first-out queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue	Number of packets in output queue.
Drops	Number of packets dropped because of a full queue.
Input queue	Number of packets in input queue.
Minute input rate	Average number of bits and packets received per minute in the past 5 minutes.
Bits/sec	Average number of bits sent per second.
Packets/sec	Average number of packets sent per second.
Packets input	Total number of error-free packets received by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.
No buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no-input-buffer events.

**Table 81** *show interface dspfarm Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
Runts	Number of packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Number of packets that are discarded because they exceed the maximum packet size for the medium. For instance, any Ethernet packet that is greater than 1518 bytes is considered a giant.
Throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
Input errors	Number of packet input errors.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station sending bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
Frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
Overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the ability of the receiver to handle the data.
Ignore	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
Abort	Illegal sequence of one bits on the interface.
Packets output	Total number of messages sent by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
Underruns	Number of times that the far end transmitter has been running faster than the near-end router's receiver can handle.
Output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this value might not balance with the sum of the enumerated output errors; some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.

**Table 81** *show interface dspfarm Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Collisions	Number of messages re-sent because of an Ethernet collision. Collisions are usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
Interface resets	Number of times an interface has been completely reset. Resetting can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurs, or when an interface is looped back or shut down.
Output buffer failures	Number of failed buffers.
Output buffers swapped out	Number of buffers swapped out.

# show ip sctp association list

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

## show ip sctp association list

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

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

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

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

```
Router# show ip sctp association list

*** SCTP Association List ****

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

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

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

Table 82 describes significant fields shown in this output.

**Table 82** *show ip sctp association list Field Descriptions*

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

#### Related Commands

Command	Description
<b>clear ip sctp statistics</b>	Clears statistics counts for SCTP.
<b>debug ip sctp api</b>	Reports SCTP diagnostic information and messages.
<b>show ip sctp association parameters</b>	Shows the parameters configured for the association defined by the association identifier.
<b>show ip sctp association statistics</b>	Shows the current statistics for the association defined by the association identifier.
<b>show ip sctp errors</b>	Shows error counts logged by SCTP.
<b>show ip sctp instances</b>	Shows the currently defined SCTP instances.
<b>show ip sctp statistics</b>	Shows the overall statistics counts for SCTP.
<b>show iua as</b>	Shows information about the current condition of an application server.
<b>show iua asp</b>	Shows information about the current condition of an application server process.

# show ip sctp association parameters

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

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

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

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)MB	This command was introduced as part of the <b>show ip sctp</b> command.
	12.2(2)T	This command was introduced as the <b>show ip sctp association parameters</b> command.
	12.2(4)T	This command was integrated into Cisco IOS release 12.2(4)T.
	12.2(8)T	Three new output fields were added to this command: Outstanding bytes, per destination address; Round trip time (RTT), per destination address; and Smoothed round trip time (SRTT), per destination address.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 and Cisco AS5850.
	12.2(15)T	This command was implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

**Usage Guidelines** The **show ip sctp association parameters** command provides information to determine the stability of SCTP associations, dynamically calculated statistics about destinations, values to assess network congestion. This command also displays parameter values for the specified association.

This command requires an association identifier. Association identifiers can be obtained from the output of the **show ip sctp association list** command.

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

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

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

**Examples**

The following sample output shows the IP SCTP association parameters for association 0:

```
Router# show ip sctp association parameters 0

** Sctp Association Parameters **

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

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

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

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

Local vertag: 9A245CD4 Remote vertag: 2A08D122
Num inbound streams: 10 outbound streams: 10
Max assoc retrans: 5 Max init retrans: 8
CumSack timeout: 200 ms Bundle timeout: 100 ms
Min RTO: 1000 ms Max RTO: 60000 ms
LocalRwnd: 18000 Low: 13455 RemoteRwnd: 15252 Low: 13161
Congest levels: 0 current level: 0 high mark: 325
```

[Table 83](#) describes significant fields shown in this output.

**Table 83** *show ip sctp association parameters Field Descriptions*

Field	Description
AssocID	SCTP association identifier.
Context	Internal upper-layer handle.
InstanceID	SCTP association instance identifier.
Assoc state	SCTP association state, which can be ESTABLISHED, CLOSED, COOKIE-WAIT, and COOKIE-ECHOED.
Uptime	Duration of time for which the association has been active.
Local port	Port number for the local SCTP endpoint.
Local addresses	IP addresses for the local SCTP endpoint.
Remote port	Port number for the remote SCTP endpoint.
Primary dest addr	Primary destination address.
Effective primary dest addr	Current primary destination address.
Heartbeats	Status of heartbeats.
Timeout	Heartbeat timeout.

**Table 83** show ip sctp association parameters Field Descriptions (continued)

Field	Description
RTO/RTT/SRTT	Retransmission timeout, round trip time, and smoothed round trip time, calculated from network feedback.
TOS	IP precedence setting.
MTU	Maximum transmission unit size, in bytes, that a particular interface can handle.
cwnd	Congestion window value calculated from network feedback. The amount of data that can be outstanding in the network for that particular destination.
ssthresh	Slow-start threshold value calculated from network feedback.
outstand	Number of outstanding bytes.
Num retrans	Current number of times that data has been retransmitted to that address.
Max retrans	Maximum number of times that data has been retransmitted to that address.
Num times failed	Number of times that the address has been marked as failed.
Local vertag, Remote vertag	Verification tags (vertags). Tags are chosen during association initialization and do not change.
Num inbound streams, Num outbound streams	Maximum inbound and outbound streams. This number does not change.
Max assoc retrans	Maximum association retransmit limit. Number of times that any particular chunk may be retransmitted before a declaration that the association failed, which indicates that the chunk could not be delivered on any address.
Max init retrans	Maximum initial retransmit limit. Number of times that the chunks for initialization may be retransmitted before declaring that the attempt to establish the association failed.
CumSack timeout	Cumulative selective acknowledge (SACK) timeout. The maximum time that a SACK may be delayed while attempting to bundle together with data chunks.
Bundle timeout	Maximum time that data chunks may be delayed while attempting to bundle with other data chunks.
Min RTO, Max RTO	Minimum and maximum retransmit timeout values allowed for the association.
LocalRwnd, RemoteRwnd	Local and remote receive windows.
Congest levels: current level, high mark	Current congestion level and highest number of packets queued.

**Related Commands**

Command	Description
<b>clear ip sctp statistics</b>	Clears statistics counts for SCTP.
<b>debug ip sctp api</b>	Reports SCTP diagnostic information and messages.
<b>show ip sctp association list</b>	Shows a list of all current SCTP associations.
<b>show ip sctp association statistics</b>	Shows the current statistics for the association defined by the association identifier.

<b>Command</b>	<b>Description</b>
<b>show ip sctp errors</b>	Shows error counts logged by Sctp.
<b>show ip sctp instances</b>	Shows all currently defined Sctp instances.
<b>show ip sctp statistics</b>	Shows overall statistics counts for Sctp.
<b>show iua as</b>	Shows information about the current condition of an application server.
<b>show iua asp</b>	Shows information about the current condition of an application server process.

# show ip sctp association statistics

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

**show ip sctp association statistics** *assoc-id*

<b>Syntax Description</b>	<i>assoc-id</i>	Association identifier, which can be obtained from the output of the <b>show ip sctp association list</b> command.
---------------------------	-----------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)MB	This command was introduced as part of the <b>show ip sctp</b> command.
	12.2(2)T	This command was introduced as the <b>show ip sctp association statistics</b> command.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(8)T	Two new output fields were added to this command: Number of unordered data chunks sent and Number of unordered data chunks received. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
	12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

<b>Usage Guidelines</b>	This command shows only the information that has become available since the last time a <b>clear ip sctp statistics</b> command was executed.
-------------------------	---

**Examples** The following sample output shows the statistics accumulated for SCTP association 0:

```
Router# show ip sctp association statistics 0

** SCTP Association Statistics **

AssocID/InstanceID: 0/1
Current State: ESTABLISHED
Control Chunks
  Sent: 623874  Rcvd: 660227
Data Chunks Sent
  Total: 14235644  Retransmitted: 60487
  Ordered: 6369678  Unordered: 6371263
  Avg bundled: 18  Total Bytes: 640603980
Data Chunks Rcvd
  Total: 14496585  Discarded: 1755575
  Ordered: 6369741  Unordered: 6371269
  Avg bundled: 18  Total Bytes: 652346325
  Out of Seq TSN: 3069353
ULP Dgrams
```

Sent: 12740941 Ready: 12740961 Rcvd: 12740941

Table 84 describes significant fields shown in this output.

**Table 84** *show ip sctp association statistics Field Descriptions*

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

#### Related Commands

Command	Description
<b>clear ip sctp statistics</b>	Clears statistics counts for SCTP.
<b>debug ip sctp api</b>	Reports SCTP diagnostic information and messages.
<b>show ip sctp association list</b>	Shows a list of all current SCTP associations.
<b>show ip sctp association parameters</b>	Shows the parameters configured for the association defined by the association identifier.
<b>show ip sctp errors</b>	Shows error counts logged by SCTP.
<b>show ip sctp instances</b>	Shows all currently defined SCTP instances.
<b>show ip sctp statistics</b>	Shows overall statistics counts for SCTP.
<b>show iua as</b>	Shows information about the current condition of an application server.
<b>show iua asp</b>	Shows information about the current condition of an application server process.

# show ip sctp errors

To display the error counts logged by the Stream Control Transmission Protocol (SCTP), use the **show ip sctp errors** command in privileged EXEC mode.

## show ip sctp errors

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

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

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

**Examples** The following sample output shows a session with no errors:

```
Router# show ip sctp errors

*** Sctp Error Statistics ****

No Sctp errors logged.
```

The following sample output shows a session that has SCTP errors:

```
Router# show ip sctp errors

** Sctp Error Statistics **

Invalid verification tag:      5
Communication Lost:           64
Destination Address Failed:   3
Unknown INIT params rcvd:    16
Invalid cookie signature:     5
Expired cookie:               1
Peer restarted:               1
No Listening instance:         2
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear ip sctp statistics</b>	Clears statistics counts for SCTP.
<b>debug ip sctp api</b>	Reports SCTP diagnostic information and messages.
<b>show ip sctp association list</b>	Shows a list of all current SCTP associations.
<b>show ip sctp association parameters</b>	Shows the parameters configured for the association defined by the association ID.
<b>show ip sctp association statistics</b>	Shows the current statistics for the association defined by the association ID.
<b>show ip sctp instances</b>	Shows the currently defined SCTP instances.
<b>show ip sctp statistics</b>	Shows overall statistics counts for SCTP.
<b>show iua as</b>	Shows information about the current condition of an AS.
<b>show iua asp</b>	Shows information about the current condition of an ASP.

# show ip sctp instances

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

## show ip sctp instances

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

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

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

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

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

```
Router# show ip sctp instances

*** SCTP Instances ***

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

```

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

```

```

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

```

```

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

```

### Related Commands

Command	Description
<b>clear ip sctp statistics</b>	Clears statistics counts for Sctp.
<b>debug ip sctp api</b>	Reports Sctp diagnostic information and messages.
<b>show ip sctp association list</b>	Shows a list of all current Sctp associations.
<b>show ip sctp association parameters</b>	Shows the parameters configured for the association defined by the association identifier.
<b>show ip sctp association statistics</b>	Shows the current statistics for the association defined by the association identifier.
<b>show ip sctp errors</b>	Shows error counts logged by Sctp.
<b>show ip sctp statistics</b>	Shows the overall statistics counts for Sctp.
<b>show iua as</b>	Shows information about the current condition of an AS.
<b>show iua asp</b>	Shows information about the current condition of an ASP.

# show ip sctp statistics

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

## show ip sctp statistics

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

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

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

**Examples** The following sample output shows IP SCTP statistics:

```
Router# show ip sctp statistics

*** SCTP Overall Statistics ***

Total Chunks Sent:          2097
Total Chunks Rcvd:         2766

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

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear ip sctp statistics</b>	Clears statistics counts for SCTP.
<b>debug ip sctp api</b>	Reports SCTP diagnostic information and messages.
<b>show ip sctp association list</b>	Shows a list of all current SCTP associations.
<b>show ip sctp association parameters</b>	Shows the parameters configured and calculated for the association defined by the association identifier.
<b>show ip sctp association statistics</b>	Shows the current statistics for the association defined by the association identifier.
<b>show ip sctp errors</b>	Shows error counts logged by SCTP.
<b>show ip sctp instances</b>	Shows all currently defined SCTP instances.
<b>show iua as</b>	Shows information about the current condition of an AS.
<b>show iua asp</b>	Shows information about the current condition of an ASP.

## show iua as

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

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

### Syntax Description

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

### Command Modes

Privileged EXEC

### Command History

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

### Usage Guidelines

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

### Examples

The following sample output from this command shows that the current state of the AS (as1) is active and that there are four PRI interfaces configured to use this AS:

```
Router# show iua as all

Name of AS :as1
  Total num of ASPs configured :2
    asp1
    asp2
  Current state : ACTIVE
  Active ASP :asp1
  Number of ASPs up :1
  Fail-Over time : 4000 milliseconds
  Local address list : 10.1.2.345 10.2.3.456
  Local port:2139
  Interface IDs registered with this AS
    Interface ID
    0 (Dchannel0)
    3 (Dchannel3)
    2 (Dchannel2)
    1 (Dchannel1)
```

Table 85 shows important fields in the output.

**Table 85** *show iua as all Field Descriptions*

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

#### Related Commands

Command	Description
<b>clear ip sctp statistics</b>	Clears statistics counts for Sctp.
<b>show ip sctp association list</b>	Shows a list of all current Sctp associations.
<b>show ip sctp association parameters</b>	Shows the parameters configured for the association defined by the association ID.
<b>show ip sctp association statistics</b>	Shows the current statistics for the association defined by the association ID.
<b>show ip sctp errors</b>	Shows error counts logged by Sctp.
<b>show ip sctp instances</b>	Shows the currently defined Sctp instances.
<b>show ip sctp statistics</b>	Shows the overall statistics counts for Sctp.
<b>show isdn</b>	Shows information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels.
<b>show iua asp</b>	Shows information about the current condition of an ASP.

# show iua asp

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

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

## Syntax Description

<b>all</b>	Displays information about all configured ASPs.
<b>name <i>asp-name</i></b>	Name of a particular ASP. Displays information about just that ASP.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

## Usage Guidelines

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

## Examples

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

```
Router# show iua asp all

Name of ASP :asp1
Current State of ASP:ASP-Active
Current state of underlying SCTP Association IUA_ASSOC_ESTAB , assoc id 0
SCTP Association information :
    Local Receive window :9000
    Remote Receive window :9000
    Primary Dest address requested by IUA 10.11.2.33
    Effective Primary Dest address 10.11.2.33
Remote address list :10.22.3.44
Remote Port :9900
Statistics :
    Invalid SCTP signals Total :0 Since last 0
    SCTP Send failures :0
```

[Table 86](#) describes significant fields shown in this output.

**Table 86** show iua asp all Field Descriptions

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

**Related Commands**

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

# show mgcp

To display values for Media Gateway Control Protocol (MGCP) parameters, use the **show mgcp** command in privileged EXEC mode.

**show mgcp** [**connection** | **endpoint** | **statistics**]

Syntax Description	connection	(Optional) Displays the active MGCP-controlled connections.
	<b>endpoint</b>	(Optional) Displays the MGCP-controlled endpoints.
	<b>statistics</b>	(Optional) Displays MGCP statistics regarding received and transmitted network messages.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced on the Cisco AS5300.
	12.1(3)T	This command output was updated to display additional gateway and platform information.
	12.1(5)XM	Output was updated to display additional gateway and platform information.
	12.2(2)T	This command was implemented on the Cisco 7200 series.
	12.2(2)XA	The <b>profile</b> keyword was added to the <b>show mgcp</b> command.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(2)XB	Output for the <b>show mgcp</b> command was enhanced to display the status of MGCP system resource check (SRC) call admission control (CAC) and Service Assurance Agent (SA Agent) CAC. (Refer to the Cisco IOS Release 12.2(2)XB online document <i>MGCP VoIP Call Admission Control</i> .)  In addition, the <b>nas dump slot port channel</b> and <b>nas info</b> keywords and arguments were added to the <b>show mgcp</b> command. Because the number of keywords increased, the command-reference page for the <b>show mgcp</b> command was separated into the following command-reference pages: <ul style="list-style-type: none"> <li>• <b>show mgcp</b></li> <li>• <b>show mgcp connection</b></li> <li>• <b>show mgcp endpoint</b></li> <li>• <b>show mgcp nas</b></li> <li>• <b>show mgcp profile</b></li> <li>• <b>show mgcp statistics</b></li> </ul>
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
	12.2(2)XN	Support for enhanced MGCP voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.

Release	Modification
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 2.0. It was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5850, and Cisco IAD2420 series. The MGCP SGCP RSIP field was enhanced to show the status of the <b>mgcp sgcp disconnected notify</b> command.
12.2(13)T	This command was supported with MGCP in Cisco IOS Release 12.2(13)T.
12.2(15)T	This command was implemented on the Cisco 1751 and Cisco 1760.

## Usage Guidelines

This command provides administrative high-level information about the values configured for MGCP parameters on the router. For more specific types of information, see the **show mgcp connection**, **show mgcp endpoint**, **show mgcp nas**, **show mgcp profile**, and **show mgcp statistics** commands.

## Examples

The following is sample output from this command:

```
Router# show mgcp

MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 172.18.195.147 2300 Initial protocol service is SGCP 1.5
MGCP block-newcalls DISABLED
MGCP send SGCP RSIP:forced/restart/graceful DISABLED, disconnected ENABLED
MGCP quarantine mode discard/step
MGCP quarantine of persistent events is ENABLED
MGCP dtmf-relay for VoIP disabled for all codec types
MGCP dtmf-relay voaal2 codec all
MGCP voip modem passthrough mode: NSE, codec: g711ulaw, redundancy: DISABLED,
MGCP voaal2 modem passthrough mode: NSE, codec: g711ulaw
MGCP TSE payload: 100
MGCP T.38 Named Signalling Event (NSE) response timer: 200
MGCP Network (IP/AAL2) Continuity Test timer: 3000
MGCP 'RTP stream loss' timer: 2
MGCP request timeout 500
MGCP maximum exponential request timeout 4000
MGCP gateway port: 2427, MGCP maximum waiting delay 3000
MGCP restart delay 0, MGCP vad DISABLED
MGCP rtrcac DISABLED
MGCP system resource check DISABLED
MGCP xpc-codec: DISABLED, MGCP persistent hookflash: DISABLED
MGCP persistent offhook: ENABLED, MGCP persistent onhook: DISABLED
MGCP piggyback msg DISABLED, MGCP endpoint offset DISABLED
MGCP simple-sdp DISABLED
MGCP undotted-notation DISABLED
MGCP codec type g711ulaw, MGCP packetization period 20
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lwm 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP IP ToS low delay disabled, MGCP IP ToS high throughput disabled
MGCP IP ToS high reliability disabled, MGCP IP ToS low cost disabled
MGCP IP RTP precedence 5, MGCP signaling precedence: 3
MGCP default package: line-package
MGCP supported packages: gm-package dtmf-package trunk-package line-package
                        hs-package atm-package ms-package dt-package res-package
                        mt-package
```

Table 87 describes significant fields shown in this output.

**Table 87** *show mgcp Field Descriptions*

Field	Description
MGCP Admin State...Oper State	Administrative and operational state of the MGCP daemon. The administrative state controls starting and stopping the application using the <b>mgcp</b> and <b>mgcp block-newcalls</b> commands. The operational state controls normal MGCP operations.
MGCP call-agent	Address of the call agent specified in the <b>mgcp call-agent</b> or <b>call-agent</b> command and protocol initiated for this session.
MGCP block-newcalls	State of the <b>mgcp block-newcalls</b> command.
MGCP send SGCP RSIP, disconnected	Setting for the <b>mgcp sgcp restart notify</b> and the <b>mgcp sgcp disconnected notify</b> commands (enabled or disabled).
MGCP quarantine mode	How the quarantine buffer is to handle Simple Gateway Control Protocol (SGCP) events.
MGCP quarantine of persistent events is	Whether SGCP persistent events are handled by the quarantine buffer.
MGCP dtmf-relay	Setting for the <b>mgcp dtmf-relay</b> command.
MGCP voip modem passthrough	Settings for mode, codec, and redundancy from the <b>mgcp modem passthrough mode</b> , <b>mgcp modem passthrough codec</b> , and <b>mgcp modem passthrough voip redundancy</b> commands.
MGCP voaal2 modem passthrough	Settings for mode, codec, and redundancy from the <b>mgcp modem passthrough mode</b> and <b>mgcp modem passthrough codec</b> commands.
MGCP TSE payload	Setting for the <b>mgcp tse payload</b> command.
MGCP Network (IP/AAL2) Continuity Test timer	Setting for the <b>net-cont-test</b> keyword in the <b>mgcp timer</b> command.
MGCP 'RTP stream loss' timer	Setting for the <b>receive-rtcp</b> keyword in the <b>mgcp timer</b> command.
MGCP request timeout	Setting for the <b>mgcp request timeout</b> command.
MGCP maximum exponential request timeout	Setting for the <b>mgcp request timeout max</b> command.
MGCP gateway port	User Datagram Protocol (UDP) port specification for the gateway.
MGCP maximum waiting delay	Setting for the <b>mgcp max-waiting-delay</b> command.
MGCP restart delay	Setting for the <b>mgcp restart-delay</b> command.
MGCP vad	Setting for the <b>mgcp vad</b> command.
MGCP rtrcac	Whether MGCP SA Agent CAC has been enabled with the <b>mgcp rtrcac</b> command.
MGCP system resource check	Whether MGCP SRC CAC has been enabled with the <b>mgcp src-cac</b> command.
MGCP xpc-codec	Whether the <b>mgcp sdp xpc-codec</b> command has been configured to generate the X-pc codec field for Session Description Protocol (SDP) codec negotiation in Network-based Call Signaling (NCS) and Trunking Gateway Control Protocol (TGCP).

**Table 87** show mgcp Field Descriptions (continued)

Field	Description
MGCP persistent hookflash	Whether the <b>mgcp persistent hookflash</b> command has been configured to send persistent hookflash events to the call agent.
MGCP persistent offhook	Whether the <b>mgcp persistent offhook</b> command has been configured to send persistent offhook events to the call agent.
MGCP persistent onhook	Whether the <b>mgcp persistent onhook</b> command has been configured to send persistent onhook events to the call agent.
MGCP piggyback msg	Whether the <b>mgcp piggyback message</b> command has been configured to enable piggyback messaging.
MGCP endpoint offset	Whether the <b>mgcp endpoint offset</b> command has been configured to enable incrementing of the local portion of an endpoint name for NCS. The local portion contains the analog or digital voice port identifier.
MGCP simple-sdp	Whether the <b>mgcp sdp simple</b> command has been configured to enable simple mode SDP operation.
MGCP undotted notation	Whether the <b>mgcp sdp notation undotted</b> command has been configured to enable undotted SDP notation for the codec string.
MGCP codec type	Setting for the <b>mgcp codec</b> command.
MGCP packetization period	The <b>packetization period</b> parameter setting for the <b>mgcp codec</b> command.
MGCP JB threshold lwm	Jitter-buffer minimum-threshold parameter setting for the <b>mgcp quality-threshold</b> command.
MGCP JB threshold hwm	Jitter-buffer maximum-threshold parameter setting for the <b>mgcp quality-threshold</b> command.
MGCP LAT threshold lwm	Latency minimum-threshold parameter setting for the <b>mgcp quality-threshold</b> command.
MGCP LAT threshold hwm	Latency maximum-threshold parameter setting for the <b>mgcp quality-threshold</b> command.
MGCP PL threshold lwm	Packet-loss minimum-threshold parameter setting for the <b>mgcp quality-threshold</b> command.
MGCP PL threshold hwm	Packet-loss maximum-threshold parameter setting for the <b>mgcp quality-threshold</b> command.
MGCP CL threshold lwm	Cell-loss minimum-threshold parameter setting for the <b>mgcp quality-threshold</b> command.
MGCP CL threshold hwm	Cell-loss maximum-threshold parameter setting for the <b>mgcp quality-threshold</b> command.
MGCP playout mode is	Jitter-buffer packet type and size.
MGCP IP ToS low delay	The <b>low-delay</b> parameter setting for the <b>mgcp ip-tos</b> command.
MGCP IP ToS high throughput	The <b>high-throughput</b> parameter setting for the <b>mgcp ip-tos</b> command.
MGCP IP ToS high reliability	The <b>high-reliability</b> parameter setting for the <b>mgcp ip-tos</b> command.
MGCP IP ToS low cost	The <b>low-cost</b> parameter setting for the <b>mgcp ip-tos</b> command.

Table 87 show mgcp Field Descriptions (continued)

Field	Description
MGCP IP RTP precedence	The <b>rtp precedence</b> parameter setting for the <b>mgcp ip-tos</b> command.
MGCP signaling precedence	The <b>signaling precedence</b> parameter setting for the <b>mgcp ip-tos</b> command.
MGCP default package	Package configured as the default package with the <b>mgcp default-package</b> command.
MGCP supported packages	Packages configured with the <b>mgcp package-capability</b> command to be supported on this gateway in this session.
MGCP T.38 Fax	Settings for the <b>mgcp fax t.38</b> command. The following values are displayed: <ul style="list-style-type: none"> <li>• MGCP T.38 fax: enabled or disabled.</li> <li>• Error correction mode (ECM): enabled or disabled.</li> <li>• Non-standard facilities (NSF) override: enabled or disabled. If enabled, the override code is displayed.</li> <li>• MGCP T.38 fax low-speed redundancy: the factor set on the gateway for redundancy.</li> <li>• MGCP T.38 fax high-speed redundancy: the factor set on the gateway for redundancy.</li> </ul>

## Related Commands

Command	Description
<b>debug mgcp</b>	Enables debug traces for MGCP errors, events, media, packets, and parser.
<b>mgcp</b>	Allocates resources for the MGCP and starts the daemon.
<b>security password-group</b>	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
<b>show mgcp connection</b>	Displays information for active MGCP-controlled connections.
<b>show mgcp endpoint</b>	Displays information for MGCP-controlled endpoints.
<b>show mgcp nas</b>	Displays MGCP NAS information for data ports.
<b>show mgcp profile</b>	Displays values for MGCP profile-related parameters.
<b>show mgcp statistics</b>	Displays MGCP statistics regarding received and transmitted network messages.



