

show gateway through show modem relay statistics

- show gateway, on page 2
- show h323 calls preserved, on page 4
- show h323 gateway, on page 6
- show h323 gateway prefixes, on page 12
- show http client cache, on page 14
- show http client cache, on page 18
- show http client cookie, on page 21
- show http client history, on page 22
- show http client secure status, on page 23
- show http client statistics, on page 25
- show interface dspfarm, on page 28
- show interfaces cable-modem, on page 33
- show ip address trusted check, on page 37
- show iua as, on page 38
- show iua asp, on page 41
- show media-proxy sessions, on page 43
- show media resource status, on page 47
- show mediacard, on page 48
- show mgcp, on page 51
- show mgcp connection, on page 60
- show mgcp endpoint, on page 64
- show mgcp nas, on page 67
- show mgcp profile, on page 71
- show mgcp srtp, on page 75
- show mgcp statistics, on page 78
- show modem relay statistics, on page 82

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
DS0: 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
```

Field descriptions should be self-explanatory.

Related Commands

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

show h323 calls preserved

To display data about active H.323 VoIP preserved calls, use the **show h323 calls preserved** command in user EXEC or privileged EXEC mode.

show h323 calls preserved

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The **show h323 calls preserved** command displays data per preserved call. Only active calls are displayed; preserved call history is not.

If translation rules are configured, the value displayed in the "Calling Number" field may have been translated by a gateway. Gateways handle called number values as the numbers to which calls are routed.

The "CallID" field displays the shorter form of the 16-octet, globally-unique connection ID that is allocated for each call leg. The show call active voice brief command also displays a shorter form of the CallID value (part of the third octet and the fourth octet). The longer form of the CallID value is output by the **show call active voice** command.

The CallID value can be used to refer to a call leg associated with the CallID when issuing other voice commands on the gateway, such as the **show voice call status** command and the **clear call voice** command.

An output value of -1 displayed in the "H225 FD" or "H245 FD" field denotes that the call was preserved due to an error detected on the H.225.0 connection. The actual H.225.0 socket file descriptor used for this call can be found from the syslog message that was output when this call was preserved.

To obtain more information about a call, you can also use the **show call active voice** command. Calls can be cleared with the **clear call voice causecode** command.

Examples

The following is sample output from the **show h323 calls preserved** command where one active call is preserved:

```
Router# show h323 calls preserved
CallID = 11EC , Calling Number = , Called Number = 3210000 ,
RemoteSignallingIPAddress=9.13.0.26 , RemoteSignallingPort=49760 ,
RemoteMediaIPAddress=9.13.0.11 , RemoteMediaPort=17910 , Preserved Duration = 262 , Total
Duration = 562 , H225 FD = -1 , H245 FD = -1
```

The table below provides an alphabetical listing of the fields displayed in the output of the **show h323 calls preserved** command and a description of each field.

Table 1: show h323 calls preserved Field Descriptions

Field	Description
Called Number	The phone number entered by the caller.
CallID	The shortened name for connection ID displayed in the **show call active voice brief** command.
H225 FD	The file descriptor number of the H.225.0 TCP socket.
H245 FD	The file descriptor number of the H.245 TCP socket.
Preserved Duration	The time in seconds that the call has been preserved.
RemoteMediaIPAddress	The remote media IP address.
RemoteMediaPort	The remote media IP address.
RemoteSignallingIPAddress	The remote signaling IP address.
RemoteSignallingPort	The remote signaling port.
Total Duration	The time in seconds of the phone call.

Related Commands

Command	Description
call preserve	Enables the preservation of H.323 VoIP calls.
clear call voice	Clears one or more voice calls detected as inactive because there is no RTP or RTCP activity.
show call active voice	Displays call information for voice calls in progress.
show voice call	Displays the call status for voice ports on the Cisco router.

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

cause -code stats	(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.
h225	(Optional) Output lists cumulative counts of the number of H.225 messages that have been sent and received since the counters were last cleared.
ras	(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.

Command Default

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 the tables below 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
```

The table below describes significant fields shown in this output

Table 2: show h323 gateway cause-code stats Field Descriptions

Field	Description
Column Headings:	
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
```

The table below describes significant fields shown in this output.

Table 3: show h323 gateway h225 Field Descriptions

Field	Description
Column Headings:	Types of H.225 messages.
H.225 REQUESTS	
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.
Fields:	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	
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.")

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 show h323 gateway ras 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
```

The table below describes significant fields shown in this output.

Table 4: show h323 gateway ras Field Descriptions

Field	Description
Column Headings for the First Table:	
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.
Column Headings for the Second Table:	
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.

Field	Description
Fields:	
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.
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.

Related Commands

Command	Description
show h323 gateway prefixes	Displays the status of the destination-pattern database and the status of the individual destination patterns.

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.

Command Default

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
```

The table below describes the significant fields shown in the display.

Table 5: show h323 gateway prefixes Field Descriptions

Field	Description
Pattern Database Status	Status of the gateway's destination-pattern database: active or inactive.

Field	Description
Status	Status of the destination pattern. The status can be one of the following values: ADD PENDING--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. ADD SENT--The gateway sent the prefix to the gatekeeper and is waiting for it to be acknowledged by a registration confirm (RCF) RAS message. ADD ACKNOWLEDGED--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. ADD REJECTED--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. DELETE PENDING--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. DELETE SENT--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.

Related Commands

Command	Description
show h323 gateway	Displays statistics for H.323 gateway messages that have been sent and received and the reasons for which H.l323 calls have been disconnected.

show http client cache

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

show http client cache [**brief**]

Syntax Description

brief	(Optional) Displays summary information about the HTTP client cache.

Command Modes

User EXEC (>)
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.
12.4(15)T	The command output was modified to display files cached with URLs of HTTP and HTTPS format in separate tables. The command output was modified to mask out values of the URL attributes when caching of query data returned from the HTTP server is enabled.
12.4(15)XY	A pound sign (#) was added next to the Age field in the command output to indicate entries marked stale manually.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T

Usage Guidelines

For more information on HTTP caching, see 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
```

In the following example, the **set http client cache stale** command was used to set all the entries in the HTTP client cache to stale. Stale entries are indicated by a pound sign (#) next to the Age field.

```
Router# show http client cache
HTTP Client cached information
==============================
Maximum memory pool allowed for HTTP Client caching = 20000 K-bytes
Maximum file size allowed for caching = 1000 K-bytes
Total memory used up for Cache = 37758 Bytes
Message response timeout = 10 secs
Total cached entries = 7
Total non-cached entries = 0
           Cached entries
           ==============
entry 142, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
0     30         53233       # 486      63D8FCC4
url: http://goa/TEST1.vxml
entry 145, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     4001998    53218       # 151      0
url: http://win2003/TEST2.vxml
entry 157, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     30         28          # 185      0
url: http://goa/TEST3.vxml
entry 164, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     2231127    53233       # 1183     0
url: http://goa/audio/en_welcome.au
entry 166, 2 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     2231127    53233       # 4916     0
url: http://goa/audio/en_one.au
1     2231127    53229       # 4500     0
url: http://goa/audio/en_three.au
entry 169, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     2231127    53229       # 7224     0
url: http://goa/audio/en_two.au
```

The table below describes the fields shown in this output.

Table 6: 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 **http client cache memory** 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 **http client cache memory** 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 **http client cache refresh** command on the gateway.
Age	Time for which the entry has been in the cache, in seconds. • Pound sign (#) indicates entries marked stale manually. • Asterisk (*) indicates entries that have become stale without manual intervention.
Size	Size of the cached entry, in bytes.

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client cache refresh	Configures the HTTP client cache refresh time.

Command	Description
http client response timeout	Configures the HTTP client server response timeout.
set http client cache stale	Sets the status of all entries in the HTTP client cache to stale.
show http client connection	Displays current HTTP client connection information.

show http client cache

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

show http client cache [**brief**]

Syntax Description

brief	(Optional) Displays summary information about the HTTP client cache.

Command Modes

User EXEC (>)
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.
12.4(15)T	The command output was modified to display files cached with URLs of HTTP and HTTPS format in separate tables. The command output was modified to mask out values of the URL attributes when caching of query data returned from the HTTP server is enabled.

Usage Guidelines

For more information on HTTP caching, see 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 = 10000 K-bytes (default)
Maximum file size allowed for caching = 50 K-bytes (default)
Total memory used up for Cache = 4271 Bytes
Message response timeout = 10 secs
Total cached entries = 2
Total non-cached entries = 0
Cached entries
           ==============
entry 135, 2 entries
Ref   FreshTime   Age          Size        context
---   ---------   ---          ----        -------
0     121393      557          1419        0
url: http://10.1.200.21/vxml/menu_main.vxml
1     121447      13           2119        0
url: https://10.1.200.21/catalog/advance.vxml
```

The following is sample output from this command when caching of query data returned from the HTTP server is enabled using the http client cache query command. Note that values of the URL attributes are masked out with asterisks (*) to protect caller privacy.

```
Router# show http client cache
HTTP Client cached information
==============================
Maximum memory pool allowed for HTTP Client caching = 10000 K-bytes (default)
Maximum file size allowed for caching = 50 K-bytes (default)
Total memory used up for Cache = 5382 Bytes
Message response timeout = 10 secs
Total cached entries = 4
Total non-cached entries = 0
Cached entries
==============
entry 135, 2 entries
Ref FreshTime Age Size context
--- --------- --- ---- -------
0 121393 577 1419 0
url: http://10.1.200.21/vxml/menu_main.vxml
1 121447 13 2119 0
url: https://10.1.200.21/catalog/advance.vxml
entry 170, 2 entries
Ref FreshTime Age Size context
--- --------- --- ---- -------
0 86400 709 478 67117ABC
url: https://www.somebankurl.com/scripts/login.php?user=*******&password=***
0 86400 528 478 686324C4
url: https://www.somebankurl.com/scripts/login.php?user=********&password=*****
```

The table below describes the fields shown in this output.

Table 7: 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 **http client cache memory**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 **http client cache memory**command.
Total memory used up for Cache	Total amount of memory that is currently being used to store cached entries in kilobytes. **Note** In some cases, large files may be cached by two processes. This number is the part of the files cached by the HTTP client process only, so this number may be smaller than the actual size of the files.
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.

Field	Description
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 **http client cache refresh**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. **Note** In some cases, large files may be cached by two processes. This number is the part of the file cached by the HTTP client process only, so this number may be smaller than the actual size of the file.

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client cache query	Enables caching of query data returned from the HTTP server.
http client cache refresh	Configures the HTTP client cache refresh time.
http client response timeout	Configures the HTTP client server response timeout.
show http client connection	Displays current HTTP client connection information.

show http client cookie

To display cookies that are stored by the HTTP client, use the **show http client cookie** command in privileged EXEC mode.

show http client cookie [**id** *call-id*]

Syntax Description

id *call-id*	(Optional) Displays cookies for the specified call only.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the *call-id* argument to display cookies for a specific call; otherwise, this command displays cookies for all calls. Cookies are stored only for the duration of a call. When a call terminates, all associated cookies are deleted. If you use the *call-id* argument and the call is not active, cookies are not displayed and an error message indicates that the call is not active.

Use the **show call active voice brief** command to display the *call-id* for an active call.

Examples

The following is sample output from the **show http client cookie** command:

```
Router# show http client cookie id 144567
HTTP Client Cookies
===================
TestCookieY==password Path=/ Domain=.cisco.com
TestCookieX==username Path=/ Domain=.cisco.com
```

The output lists the name, path, and domain of the cookie. Field descriptions should be self-explanatory.

Related Commands

Command	Description
debug http client cookie	Displays debugging traces related to HTTP cookies.
http client cache memory	Configures the memory limits for the HTTP client cache.
http client cache refresh	Configures the refresh time for the HTTP client cache.
http client cookie	Enables the HTTP client to send and receive and cookies.
show call active voice brief	Displays a call information summary for active calls.
show http client cache	Displays current HTTP client cache information.

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 user EXEC or privileged EXEC mode.

show http client history

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
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, see 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://example.com/servlets/account
   GET http://example.com/GetDigit.vxml
   GET http://example.com/form.vxml
   GET http://sample.com/menu.vxml
   POST http://sample.com/servlets/order
   GET http://sample.com/servlets/weather?city=SanFrancisco&state=CA
```

Output shows only requests. There are no field headings.

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client response timeout	Configures the HTTP client server response.
show http client connection	Displays current HTTP client connection information.

show http client secure status

To display the trustpoint and cipher suites that are configured in the HTTP client, use the **show http client secure status** command in user EXEC or privileged EXEC mode.

show http client secure status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE 17.14.1a	This command was modified to display the following TLS v1.3 ciphers: • tls13-aes128-gcm-sha256 • tls13-aes256-gcm-sha384 • tls13-chacha20-poly1305-sha256

Usage Guidelines

This command displays the trustpoint and cipher suites configured in the HTTP client by the **http client secure-trustpoint** and **http client secure-ciphersuite** commands.

Examples

The following sample output displays the configured five cipher suites:

```
Device# show http client secure status

HTTP Client Secure Ciphersuite: rc4-128-md5 rc4-128-sha 3des-cbc-sha des-cbc-sha null-md5
HTTP Client Secure Trustpoint: myca
```

The following sample output displays the configured TLS v1.3 cipher suites:

```
Device# show http client secure status

HTTP Client Secure Ciphersuite: tls13-aes128-gcm-sha256 tls13-aes256-gcm-sha384
tls13-chacha20-poly1305-sha256
HTTP Client Secure Trustpoint: test
```

The following sample output displays the configured default TLS cipher suites:

```
Device# show http client secure status

HTTP Client Secure Ciphersuite: aes-128-cbc-sha rsa-aes-cbc-sha2 dhe-rsa-aes-cbc-sha2
ecdhe-rsa-aes-gcm-sha2
ecdhe-rsa-aes-cbc-sha2 ecdhe-ecdsa-aes-gcm-sha2 tls13-aes128-gcm-sha256
tls13-aes256-gcm-sha384 tls13-chacha20-poly1305-sha256
HTTP Client Secure Trustpoint: ciscoctg-DC1-1A-CA-1
```

The table below describes the significant fields shown in the display.

Table 8: show http client secure status Field Descriptions

Field	Description
HTTP Client Secure Ciphersuite	Cipher suites. • 3des-cbc-sha: Encryption tls_rsa_with_3des_ede_cbc_sha (TLS1.0) ciphersuite • aes-128-cbc-sha: Encryption tls_rsa_with_aes_128_cbc_sha (TLS1.2 & below) ciphersuite • des-cbc-sha: Encryption tls_rsa_with_des_cbc_sha (TLS1.0) ciphersuite • dhe-rsa-aes-cbc-sha2: Encryption tls_rsa_with_cbc_sha2 (TLS1.2) ciphersuite • ecdhe-ecdsa-aes-gcm-sha2: Encryption tls_rsa_with_ecdhe-ecdsa-aes-gcm-sha2 (TLS1.2) ciphersuite • ecdhe-rsa-aes-cbc-sha2: Encryption tls_rsa_with_aes-cbd-sha2 (TLS1.2) ciphersuite • ecdhe-rsa-aes-gcm-sha2: Encryption tls_rsa_with_aes-gcm-sha2 (TLS1.2) ciphersuite • null-md5: Encryption tls_rsa_with_null_md5 (TLS1.0) ciphersuite • rc4-128-md5: Encryption tls_rsa_with_rc4_128_md5 (TLS1.0) ciphersuite • rc4-128-sha; Encryption tls_rsa_with_rc4_128_sha (TLS1.0) ciphersuite • rsa-aes-cbc-sha2: Encryption tls_rsa_with_aes_cbc_sha2 (TLS1.2) ciphersuite • tls13-aes128-gcm-sha256: Encryption tls13_aes128_gcm_sha256 (TLS1.3) ciphersuite • tls13-aes256-gcm-sha384: Encryption tls13_aes256_gcm_sha384 (TLS1.3) ciphersuite • tls13-chacha20-poly1305-sha256: Encryption tls13_chacha20_poly1305_sha256 (TLS1.3) ciphersuite
HTTP Client Secure Trustpoint	Trustpoint name.

Related Commands

Command	Description
http client secure-trustpoint	Declares the trustpoint that the HTTP client will use.
http client secure-ciphersuite	Sets the secure encryption cipher suite for the HTTP client.

show http client statistics

To display information about the communication between the HTTP server and the client, use the **show http client statistics** command in user EXEC or privileged EXEC mode.

show http client statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the data displayed by this command to determine whether the network topology between the HTTP server and client is properly designed and configured. To reset to zero all the counters that collect the information this command displays, use the **clear http client statistics** command.

Examples

The following sample output from this command shows statistics about the communication between the HTTP server and client:

```
Router# show http client statistics
    HTTP Client Statistics:
    =======================
Elapsed time: 759962960 msec
Load Count:
  total load count = 6899220
  total byte count = 26028731394
  largest file size = 624742 bytes
  smallest file size = 374 bytes
Server Response Time to Connect:
  longest response to connect = 10484 msec
  shortest response to connect = 24 msec
Server Response Time to Load:
  longest response to load = 11936 msec
  shortest response to load = 20 msec
File Load Time from Server:
  longest load time = 13124 msec
  shortest load time = 56 msec
Server Connection Count:
  max connections = 23
  established connections = 6901185
Load Rate:
  1 hour : 123300000 bytes
  1 min  : 2055000 bytes
  1 sec  : 34250 bytes
  1 msec : 34.25 bytes
Individual Counts:
  app_requests = 8538451                app_callbacks = 8538451
  200_OK_rsp = 8512959                  other_rsp = 0
  total_errors = 25492                  client_timeouts = 25470
```

```
client_errs = 0                          connect_errs/_timeouts = 7
msg_decode_errs = 0                      msg_encode_errs = 0
msg_xmit_errs = 15                       write_Q_full = 0
socket_rcv_errs = 0                      supported_method_errs = 0
retries = 4645                           late_responses = 0
out_of_memory = 0                        mem_reallocs = 1206
msg_malloced = 0                         event_malloced = 45
cache_freed_by_ager = 1565
```

The table below describes the significant fields shown in the display.

Table 9: show http client statistics Field Descriptions

Field	Description
Elapsed time	Time elapsed since the first HTTP request, in milliseconds (ms).
total load count	Number of API events.
total byte count	Total bytes downloaded from the server by API requests.
largest file size smallest file size	Size of largest and smallest files downloaded from the server, in bytes.
longest response to connect shortest response to connect	Longest and shortest time taken by the server to establish a network connection requested by the client, in ms.
longest response to load shortest response to load	Longest and shortest time taken by the server to fulfill a download request from the client, in ms.
longest load time shortest load time	Longest and shortest time taken by the server to complete downloading the entire file, in ms.
max connections	Maximum concurrent connections.
established connections	Number of currently active and previously established connections.
Load Rate	Downloading rate in bytes/hour, bytes/minute, bytes/second, and bytes/ms.
app_requests	Number of GET and POST requests.
app_callbacks	Number of callbacks to the application.
200_OK_rsp	Number of server messages with response code 200 OK or 304 Not Modified.
other_rsp	Number of server messages with a response code other than 200 and 304.
total_errors	Number of errors encountered by the client.
client_timeouts	Number of timeouts the client has experienced, for example, response timeouts.
client_errs	Number of client internal errors, for example, software errors.
connect_errs/_timeouts	Number of failed or broken connections.

Field	Description
msg_decode_errs	Number of server response messages for which the client failed to decode the headers.
msg_encode_errs	Number of send messages for which the client failed to encode the headers.
msg_xmit_errs	Number of send messages that the client failed to transmit to the server.
write_Q_full	Number of times that the client failed to enter a send message requested by an application into the transmit queue.
socket_rcv_errs	Number of socket read error events returned by TCP.
supported_method_errs	Number of unsupported methods requested by the application.
retries	Number of retransmitted messages.
late_responses	Number of messages that were decoded successfully but exceeded the timeout.
out_of_memory	Number of times that the client failed to allocate memory from Cisco IOS software.
mem_reallocs	Number of times that the client needed to readjust its buffer size because the server response message size exceeded the allocated buffer.
msg_malloced	Number of message buffers currently allocated for receiving messages from the server.
event_malloced	Number of event buffers currently allocated for application programming interface (API) requests.
cache_freed_by_ager	Number of HTTP client cache entries freed up by the background ager process.

Related Commands

Command	Description
clear http client statistics	Resets to zero all the counters that collect the information about the communication between the HTTP server and the client displayed in the output from the **show http client statistics** command.

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 inprivilegedEXEC mode.

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

Syntax Description

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

Command Default

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 following form of this command: **show interface dspfarm <x/y | x/y/z> dsp tdm**..

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
```

The table below describes significant fields shown in this output.

Table 10: 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 expediential 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.

Field	Description
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.
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.

Field	Description
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.
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.

Field	Description
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.
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.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.

show interfaces cable-modem

To display statistics for all interfaces configured on the cable modem port and to define Hybrid Fiber-Coax (HFC) statistics on the modem, use the **show interfaces cable-modem** command in privileged EXEC mode.

show interfaces cable-modem *port*

Syntax Description

port	The port number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command can be used to define the HFC state on the modem.

Examples

The following example shows the HFC state on the modem. The resulting output varies, depending on the network for which an interface has been configured.

```
Router# show interfaces cable-modem 0/1/0

cable-modem0/1/0 is up, line protocol is up
  HFC state is OPERATIONAL, HFC MAC address is 00d0.59e1.2073
  Hardware is Cable modem, address is 0014.f26d.10b2 (bia 0014.f26d.10b2)
  Internet address is 00.0.0.01/1
  MTU 1500 bytes, BW 1544 Kbit, DLY 6470 usec,
     reliability 255/255, txload 247/255, rxload 246/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:07:03
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 83594
  Queueing strategy: Class-based queueing
  Output queue: 61/1000/64/83594 (size/max total/threshold/drops)
     Conversations  2/5/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 232 kilobits/sec
  30 second input rate 2581000 bits/sec, 987 packets/sec
  30 second output rate 1585000 bits/sec, 639 packets/sec
  HFC input: 0 errors, 0 discards, 0 unknown protocols 0 flow control discards
  HFC output: 0 errors, 0 discards
     304582 packets input, 105339474 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 1 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     228195 packets output, 78392605 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the significant fields shown in the display.

Table 11: show interfaces cable-modem Field Descriptions

HFC State Values	Description
HFC state is OPERATIONAL	Current HFC state on the modem.
HFC MAC address	The HFC MAC address for this modem.
Hardware is Cable modem	Hardware type.
Internet address	The IP address for this modem.
MTU	Total MTU usage in bytes, kilobits, user seconds. Describes reliability, transmit load, and receiver load.
Encapsulation ARPA, loopback not set	Encapsulation type and whether loopback is set.
ARP type: ARPA, ARP Timeout	ARP type and timeout parameters.
Last input, output, output hang	Most recent input and output statistics.
Last clearing of "show interface" counters	Most recent usage of **show interface** command counters.
Input queue, Total output drops	Input queue and output drop statistics in the following format: size/max/drops/flushes.
Queueing strategy: Class-based queueing	Queueing type. In this case, class-based queueing.
Output queue	Output queue statistics in the following format: size/max total/threshold/drops.
Conversations	Type and number of conversations in the following format: active/max active/max total.
Reserved Conversations	Number of reserved conversations in the following format: allocated/max allocated.
Available Bandwidth	Allotted bandwidth in kilobits per second.
input rate, packets	Input rate and number of packets in bits per second, packets per second.
output rate, packets	Output rate and number of packets in bits per second, packets per second.
HFC input, output	HFC input statistics in the following format: errors, discards, unknown protocols, flow control discards.
packets input	Number of packets in bytes, with or without buffer.
Received broadcasts, runts, giants, throttles	Number of broadcasts, runts, giants, and throttles.
input errors	Number and type of input errors in the following format: cyclic redundancy check (CRC), frame, overrun, ignored.
packets output	Number of packets output in bytes and underruns.

HFC State Values	Description
output errors, collisions, interface resets	Number of output errors, collisions, and interface resets.
babbles, late collision, deferred	Number of babbles, late collisions, and deferred packets.
lost carrier, no carrier	Carrier statistics.
output buffer failures, output buffers swapped out	Buffer statistics.

The HFC state is the Data Over Cable Service Interface Specification (DOCSIS) state for the cable modem connection to the cable modem termination system (CMTS). The table below describes HFC state values.

Table 12: HFC State Values

HFC State Values	Description
NOT_READY	Cable modem controller is resetting.
NOT_SYNCHRONIZED	Cable modem controller is starting the downstream frequency scan.
PHY_SYNCHRONIZED	Cable modem controller locked the downstream signal and is collecting the upstream channel parameter information.
US_PARAMETERS_ACQUIRED	Cable modem controller collected upstream channel parameter information and is trying to lock upstream frequency.
RANGING_COMPLETE	Cable modem controller received the CMTS range response, has finished downstream/upstream lock process, and is initializing IP.
IP_COMPLETE	Cable modem controller has IP information.
WAITING_FOR_DHCP_OFFER	Cable modem controller is sending a Dynamic Host Configuration Protocol (DHCP) request to the CMTS.
WAITING_FOR_DHCP_RESPONSE	Cable modem controller is waiting for a DHCP response from the CMTS.
WAITING_FOR_TIME_SERVER	Cable modem controller is starting the time of day (ToD) service.
TOD_ESTABLISHED	Cable modem controller has received the ToD packet and has synchronized its local time.
WAITING_FOR_TFTP	Cable modem controller is downloading its running configuration from the CMTS-defined TFTP server.
PARAM_TRANSFER_COMPLETE	Cable modem controller has completed transferring its running configuration.
REGISTRATION_COMPLETE	Cable modem controller has sent out its registration request, and CMTS has accepted it.

HFC State Values	Description
REFUSED_BY_CMTS	Cable modem controller registration request has been rejected by CMTS.
FORWARDING_DENIED	Cable modem controller registration to CMTS was successful, but network access is disabled in the running configuration.
OPERATIONAL	Cable modem controller is ready for service.
UNKNOWN	Cable modem controller is an undefined state

The table below lists input error descriptions.

Table 13: Input Error Description

Input Error	Description
errors	The total number of input packets discarded on the cable modem controller.
discards	The number of input packets discarded due to a momentary lack of resources.
unknown protocols	The number of input packets discarded because they have unsupported or unknown protocol values.
flow control discards	The number of input packets discarded because the cable modem controller overflowed transferring packets to the router.

The table below lists output error descriptions.

Table 14: Output Error Description

Output Error	Description
errors	Total number of output packets discarded on the cable modem controller.
discards	Total number of output packets discarded due to a momentary lack of resources.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces.

show ip address trusted check

To check the trust of a call setup from a VoIP source, use the **show ip address trusted check** command in privileged EXEC mode.

show ip address trusted check {*IPv4 address IPv6 address*}

Syntax Description

IPv4 address/IPv6 address	IP address of the VoIP source that initiated the call setup.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

Use the **show ip address trusted check** command from the Toll-fraud prevention support feature, to check the trust of the incoming H.323 or SIP trunk calls. The IP address authentication validates the trust of the incoming call.

This command checks the IP address trusted list and the authentication is passed when an entry matches with source IP address. To display the IP address trusted list, use the **show ip address trusted list** command in privileged EXEC mode.

Example

The following example shows the IP address authentication passed for the VoIP source 15.1.0.1.

```
Router# show ip address trusted check 15.1.0.1
ip[15.1.0.1] authenticate is PASSED by peer ip addr
```

The following example shows the IP address authentication failed for the VoIP source 15.3.0.1.

```
Router# show ip address trusted check 15.3.0.1
ip[15.3.0.1] authentication is FAILED!
```

Related Commands

Command	Description
show ip address trusted list	Displays the IP address trusted list.
ip address trusted	Enables toll-fraud prevention support on a device.

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

all	Output displays information about all configured ASs.
name *as -name*	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, Cisco 3700 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use the **show iua as all** command to find the failover timer value. You need to know the current failover timer value before you changeit 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)
```

The table below describes significant fields shown in the output.

Table 15: 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 ms, although the value can also be configured through the CLI under AS.
Local address list : 10.1.2.345 10.2.3.456	Configured by the user.
Local port:2139	Configured by the user.
Interface IDs registered with this AS Interface id 0 (Dchannel0) 3 (Dchannel3) 2 (Dchannel2) 1 (Dchannel1)	The D channels that are bound to this AS.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Displays the current statistics for the association defined by the association ID.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays the currently defined SCTP instances.
show ip sctp statistics	Displays the overall statistics counts for SCTP.
show isdn	Displays information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels.

Command	Description
show iua asp	Displays 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

all	Displays information about all configured ASPs.
name *asp -name*	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
```

The table below describes significant fields shown in this output.

Table 16: show iua asp all Field Descriptions

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

Related Commands

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

show media-proxy sessions

To display the details of an active or completed SIP recording sessions on the CUBE Media Proxy, use the **show media-proxy sessions** command in privileged EXEC mode.

show media-proxy sessions [**summary** [**history**] | **call-id** *call-id* | **session-id** *WORD* | **metadata-session-id** *x-session-id*]

Syntax Description

summary	(Optional) Displays the summary of the active SIP recording sessions.
history	(Optional) Displays the summary of the completed SIP recording sessions.
call-id *call-id*	(Optional) Displays the details of the inbound and forked legs that are associated with the specified CCAPI call identifier of the SIP leg.
session-id *WORD*	(Optional) Displays the details of the Media Proxy recording sessions that are associated with the specified session-id.
metadata-session-id *x-session-id*	(Optional) Displays the details of the Media Proxy recording sessions that are associated with the x-session-id present in the "From" header of the INVITE from CUCM.

Command Default

Displays active recording session details.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar Release 16.10.1a	This command was introduced.
Cisco IOS XE Amsterdam 17.3.1a	The output of the command **show media-proxy sessions** was modified to include "SIPREC" field.

Usage Guidelines

The command **show media-proxy sessions** displays recording session details such as inbound call-ID, forked call-ID, session-ID, dial-peer tags, IP, port number, total sessions, and failed recording sessions.

You can also get details of a specific SIP leg call-ID. MSP call-ID is not a valid value for this command.

Example

The following example shows the sample output for **show media-proxy sessions**.

```
Device# show media-proxy sessions

No.   Call-ID          Session-ID                          Dialpeer   Secure   SIPREC
      Inbound/Forked   LocalUuid;RemoteUuid                Tag        (Y/N)    (Y/N)
=============================================================================================
1     36770/-          a234a20672ce596d969c59ee9767f127;   3           N        Y
                       aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

The following example shows the details for the active recording sessions.

```
Device# show media-proxy sessions summary

 No       Inbound/Forked      Dialpeer-Tag          IP:Port          Total/Failed Sessions
-------------------------------------------------------------------------------------------

 1         Forked               100          ipv4:8.0.0.200:6680             2/0
 2         Forked               200          ipv4:8.0.0.200:6220             2/0
 3         Inbound             5678                                          2/0
```

The following example shows the details for the completed recording sessions.

```
Device# show media-proxy sessions summary history

 No.      Inbound/Forked     Dialpeer Tag         IP:Port            Total/Failed Sessions
-------------------------------------------------------------------------------------------

 1         Inbound             5678                                         2/0
 2         Forked               100          ipv4:8.0.0.200:6680            2/0
 3         Forked               200          ipv4:8.0.0.200:6220            2/0
```

The following example shows the details of a specified SIP leg call-ID.

```
Device# show media-proxy sessions call-id 2

CC Call-ID: 1 Inbound-leg
Dur: 00:00:15 tx: 0/0 rx: 1484/296800 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6009 Local-Addr: 8.43.33.203:8000 rtt:0ms pl:0/0ms
Dialpeer-Tag: 100 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 6bde661e9767590b930f3427ad6e94e9 RemoteUUID: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

CC Call-ID: 2 Forked-leg (Primary)
Dur: 00:00:15 tx: 1484/296800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6000 Local-Addr: 8.43.33.203:8002 rtt:0ms pl:0/0ms
Dialpeer-Tag: 200 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 7 Forked-leg
Dur: 00:00:15 tx: 1480/296000 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6001 Local-Addr: 8.43.33.203:8004 rtt:0ms pl:0/0ms
Dialpeer-Tag: 300 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: cccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 9 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6004 Local-Addr: 8.43.33.203:8006 rtt:0ms pl:0/0ms
Dialpeer-Tag: 400 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: cccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 11 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6005 Local-Addr: 8.43.33.203:8008 rtt:0ms pl:0/0ms
Dialpeer-Tag: 500 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: cccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 13 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
```

```
Remote-Addr: 8.41.17.71:6008 Local-Addr: 8.43.33.203:8010 rtt:0ms pl:0/0ms
Dialpeer-Tag: 600 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9
```

The following example shows the details of a specified session-id.

```
Device# show media-proxy sessions session-id 6bde661e9767590b930f3427ad6e94e9
CC Call-ID: 1 Inbound-leg
Dur: 00:00:15 tx: 0/0 rx: 1484/296800 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6009 Local-Addr: 8.43.33.203:8000 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 100 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 6bde661e9767590b930f3427ad6e94e9 RemoteUUID: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

CC Call-ID: 2 Forked-leg (Primary)
Dur: 00:00:15 tx: 1484/296800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6000 Local-Addr: 8.43.33.203:8002 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 200 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 7 Forked-leg
Dur: 00:00:15 tx: 1480/296000 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6001 Local-Addr: 8.43.33.203:8004 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 300 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 9 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6004 Local-Addr: 8.43.33.203:8006 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 400 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 11 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6005 Local-Addr: 8.43.33.203:8008 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 500 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 13 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6008 Local-Addr: 8.43.33.203:8010 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 600 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9
```

The following example shows the details of Media Proxy recording sessions based on the x-session-id that is present in the "From" header of the INVITE from CUCM.

```
Device# show media-proxy sessions metadata-session-id 696dd5d3f7755c6abdc438e93d01febf
CC Call-ID: 77 Inbound-leg
Dur: 00:00:46 tx: 0/0 rx: 3105/578880 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.0.0.200:8010 Local-Addr: 8.43.33.203:8048 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 1 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 528b282b804c5fd098eaba3696c00de2 RemoteUUID: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

CC Call-ID: 78 Forked-leg (Primary)
Dur: 00:00:46 tx: 3105/578880 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
```

```
Remote-Addr: 8.0.0.200:8014 Local-Addr: 8.43.33.203:8050 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 2 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 528b282b804c5fd098eaba3696c00de2

CC Call-ID: 84 Forked-leg
Dur: 00:00:46 tx: 3100/577880 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.0.0.200:8018 Local-Addr: 8.43.33.203:8052 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 3 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 528b282b804c5fd098eaba3696c00de2

CC Call-ID: 86 Forked-leg
Dur: 00:00:46 tx: 3101/578080 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.0.0.200:8022 Local-Addr: 8.43.33.203:8054 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 4 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 528b282b804c5fd098eaba3696c00de2

CC Call-ID: 88 Forked-leg
Dur: 00:00:46 tx: 3101/578080 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.0.0.200:8026 Local-Addr: 8.43.33.203:8056 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 5 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 528b282b804c5fd098eaba3696c00de2

CC Call-ID: 91 Forked-leg
Dur: 00:00:46 tx: 3101/578080 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.0.0.200:8030 Local-Addr: 8.43.33.203:8058 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 6 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 528b282b804c5fd098eaba3696c00de2
```

show media resource status

To display the current media resource status, use the **show media resource status** command in privileged EXEC mode.

show media resource status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example displays the current media resource status:

```
Router# show media resource status
 Resource Providers:
 Resource  Provider ID :: FLEX_DSPRM Status :: REGISTERED
 Service Profiles
 MTP ::
 TRANSCODING :: 6 11
 CONFERENCING :: 10
 Applications :
 Application ID : SCCP, Status : REGISTERED
```

The table below describes significant fields shown in this output.

Table 17: show media resource status Field Descriptions

Field	Description
MTP	Displays the profile numbers configured for MTP resources.
TRANSCODING	Displays the profile numbers configured for transcoding resources.
CONFERENCING	Displays the profile numbers configured for conferencing resources.
Status	Displays the current status of the profile.

Related Commands

Command	Description
dsp services dspfarm	Configures DSP farm services for a specified voice card.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
show dspfarm profile	Displays configured DSP farm profile information for a Cisco CallManager group.

show mediacard

To display configuration information about media card conferencing, transcoding, Media Termination Points (MTPs) and Digital Signal Processors (DSPs), use the **show mediacard** command in privileged EXEC mode.

show mediacard slot [**conference** | **connections** | **dsp** *number*]

Syntax Description

slot	Specifies the slot number of the card to be displayed. Valid values are from 1 to 4.
conference	(Optional) Displays information on ad-hoc conferences.
connections	(Optional) Displays information on media card connections.
dsp *number*	(Optional) Displays information on the specified DSP resource pool. The *number*argument ranges in value from 1 to 4.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(3)	This command was integrated into Cisco IOS Release 12.4(3).

Usage Guidelines

Use this command to display media card status, statistics, and configuration information.

Examples

The following is sample output for the **show mediacard** command:

```
Router# show mediacard 3
Media Card 3: WS-SVC-CMM-ACT
 Service: Adhoc/Meetme conference and MTP/Transcoding
 State: ENABLE
 DSP image version (all DSPs): 1.1(06), build: 1.1(06)
 DSP status:
  DSP 1 | DSP 2 | DSP 3 | DSP 4
 -------|-------|-------|-------
  alive | alive | alive | alive
 Total 128 DSP channels, 1 active
 Resource pools                    | DSPs | Used by Active profile
 ----------------------------------|------|-----------------------
  Pool1                             |  2   |  1
  Pool2                             |  1   |
  Pool3                             |  1   |  2
Router# show mediacard 3 dsp 3
DSP image version (all DSPs): 1.1(06), build: 1.1(06)
 Card DSP status Chan status RxPkts TxPkts
  3   3   alive  1    idle   -      -
```

```
                    2    idle   -      -
                    3    idle   -      -
                    4    idle   -      -
                    5    idle   -      -
                    6    idle   -      -
                    7    idle   -      -
                    8    idle   -      -
                    9    idle   -      -
                    10   idle   -      -
                    11   idle   -      -
                    12   idle   -      -
                    13   idle   -      -
                    14   idle   -      -
                    15   idle   -      -
                    16   idle   -      -
                    17   idle   -      -
                    18   idle   -      -
                    19   idle   -      -
                    20   idle   -      -
                    21   idle   -      -
                    22   idle   -      -
                    23   idle   -      -
                    24   idle   -      -
                    25   idle   -      -
                    26   idle   -      -
                    27   idle   -      -
                    28   idle   -      -
                    29   idle   -      -
                    30   idle   -      -
                    31   idle   -      -
                    32   idle   -      -
 Total 32 DSP channels, 0 active
Router# show mediacard conference
Id  Slot/  RxPkts TxPkts RPort SPort Remote-Ip
    DSP/Ch
0   2/4/1 32024     16498    27004 27020  10.7.16.87
0   2/4/2 17368     17192    17582 17583  10.7.16.80
0   2/4/3 21904     16990    26155 26168  10.7.16.94
Total: 3
Router# show mediacard connections
Id  Type  Slot/  RxPkts TxPkts RPort SPort Remote-Ip
          DSP/Ch
0   conf  3/4/1  24028  16552 0      0      10.7.16.87
Total: 1
Router# show mediacard connections
Id  Type  Slot/  RxPktsTxPktsRPort SPort Remote-Ip
          DSP/Ch
0   mtp   3/1/1  16544 16488 1046   1046   10.1.2.15
0   mtp   3/1/2  19396 19662 1046   1046   10.1.80.50
0   mtp   3/1/3  17562 20122 626    626    10.1.2.15
0   mtp   3/1/4  17488 17328 626    626    10.1.80.5
```

The table below describes the significant fields shown in the display.

Table 18: show mediacard Field Descriptions

Field	Description
RxPkts	Number of packets transmitted
TxPkts	Number of packets received
RPort	Receiving port

Field	Description
SPort	Sending port
Remote-Ip	IP address of the remote endpoint

Related Commands

Command	Description
debug mediacard	Displays debugging information for DSPRM.

show mgcp

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

show mgcp [**connection** | **endpoint** | **nas** {**dump** *slot port chan-number* | **info**} | **notify-entity** | **profile** [*name*] | **statistics**]

Syntax Description

connection	(Optional) Displays the active MGCP-controlled connections.
endpoint	(Optional) Displays the MGCP-controlled endpoints.
nas	(Optional) Displays Network Access Server (NAS) information.
dump	(Optional) Display MGCP data channel data.
slot	(Optional) Slot number.
port	(Optional) Port number.
chan-number	(Optional) Channel number.
info	(Optional) Displays MGCP data channel information.
notify-entity	(Optional) Displays MGCP notify entity information.
profile [*name*]	(Optional) Displays information about all the configured MGCP profiles. • *name* --Displays information about the specified MGCP profile.
statistics	(Optional) Displays MGCP statistics regarding received and transmitted network messages.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was modified. Command output was updated to display additional gateway and platform information.
12.1(5)XM	This command was modified. Command 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	This command was modified. The **profile** keyword was added.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

Release	Modification
12.2(2)XB	This command was modified. Command output was enhanced to display the status of MGCP system resource check (SRC) call admission control (CAC) and Service Assurance Agent (SA Agent) CAC. (See the Cisco IOS Release 12.2(2)XB document *MGCP VoIP Call Admission Control* .) The **nas dump** *slot port channel*and **nas info** keywords and arguments were added. Because the number of keywords increased, the command page for the **show mgcp** command was separated into the following command pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(2)XN	This command was modified. 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 routers.
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 **mgcp sgcp disconnected notify**command.
12.2(13)T	This command was modified. Support was added for MGCP.
12.2(15)T	This command was implemented on Cisco 1751 and Cisco 1760 routers.
12.2(15)ZJ	This command was integrated into Cisco IOS Release 12.2(15)ZJ on the Cisco 26xxXM, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, and Cisco 37xx routers.
12.3(2)T	This command was implemented on the Cisco 26xxXM, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, and Cisco 37xx routers.
12.3(11)T	This command was modified. Command output was enhanced to display the enabled Secure Real-Time Transport Protocol (SRTP) package and enabled MGCP call-agent validation.
12.4(2)T	This command was modified. Command output was enhanced to display State Signaling Events (SSE) and Simple Packet Relay Transport (SPRT) configuration parameters.
12.4(11)T	This command was modified. The **show mgcp** command output was enhanced to display comedia-related configuration.
15.1(4)M	This command was integrated into Cisco IOS 15.1(4)M. The command output was enhanced to displays the configuration of the **tone-package keyword**in the MGCP- supported packages.

Usage Guidelines

This command provides high-level administrative information about the values configured for MGCP parameters on the router. For more specific information, use one of the optional keywords.

Use the **show mgcp** command to display SSE and SPRT parameters that have been configured to enable modem relay between IP secure telephone equipment (STE) and STE. The parameters are displayed only when the modem relay STE (mdste) package has been enabled using the **mgcp package-capability mdste-package**command.

Use the **show mgcp endpoint** command to display a list of MGCP endpoint responses when the configuring Media Gateway Control Protocol Basic Rate Interface Backhaul Signaling with Cisco CallManager feature.

The BRI endpoints are displayed in a similar manner to the way analog (Plain Old Telephone service) endpoints are displayed. The existing functions used for the analog endpoints are invoked. This display is independent of the platforms; hence the changes are required in the common code only.

This command checks for all the allocated "htsp_info_t" structures. These structures store information corresponding to all the endpoints. These structures are allocated only during system startup time. The structures are allocated for all the interfaces present, but the "vtsp_sdb_t" structure is allocated only for the first channel of the BRI port.

Since the endpoints that use the Media Gateway Control Protocol Application (MGCPAPP) as the application layer have to be displayed, the endpoints are displayed even if MGCPAPP is the only application being used by the endpoint. Because the MGCPAPP is shared across both the BRI channels and is port specific, both ports are displayed.

Examples

The following is partial sample output from the **show mgcp** command when the mdste modem relay package has been enabled:

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 10.7.0.200 3460 Initial protocol service is MGCP 0.1
MGCP validate call-agent source-ipaddr DISABLED
MGCP block-newcalls DISABLED
MGCP send SGCP RSIP: forced/restart/graceful/disconnected DISABLED
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 for VoAAL2 disabled for all codec types
MGCP voip modem passthrough mode: NSE, codec: g711ulaw, redundancy: DISABLED,
MGCP voaal2 modem passthrough disabled
MGCP voip nse modem relay: Disabled
MGCP voip mdste modem relay: Enabled
        SPRT rx v14 hold time: 50 (ms), SPRT tx v14 hold count: 16,
        SPRT tx v14 hold time: 20 (ms), SPRT Retries: 12
        SSE redundancy interval: 20 (ms), SSE redundancy packet: 3,
        SSE t1 timer: 1000 (ms), SSE retries: 3
MGCP TSE payload: 100
MGCP T.38 Named Signalling Event (NSE) response timer: 200
MGCP Network (IP/AAL2) Continuity Test timer: 200
MGCP 'RTP stream loss' timer: 5
MGCP request timeout 500
MGCP maximum exponential request timeout 4000
MGCP gateway port: 2427, MGCP maximum waiting delay 20000
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 ENABLED, MGCP endpoint offset DISABLED
```

```
MGCP simple-sdp ENABLED
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 Fax Playout Buffer is 300 in msec
MGCP media (RTP) dscp: ef, MGCP signaling dscp: af31
MGCP default package: line-package
MGCP supported packages: gm-package dtmf-package mf-package trunk-package
                         line-package hs-package rtp-package script-package ms-package
                         dt-package mo-package mt-package sst-package mdr-package
                         fxr-package pre-package mdste-package srtp-package tone-package
MGCP Digit Map matching order: shortest match
SGCP Digit Map matching order: always left-to-right
MGCP VoAAL2 ignore-lco-codec DISABLED
MGCP T.38 Max Fax Rate is DEFAULT
MGCP T.38 Fax is ENABLED
MGCP T.38 Fax ECM is ENABLED
MGCP T.38 Fax NSF Override is DISABLED
MGCP T.38 Fax Low Speed Redundancy: 0
MGCP T.38 Fax High Speed Redundancy: 0
MGCP control bind :DISABLED
MGCP media bind :DISABLED
MGCP Upspeed payload type for G711ulaw: 0,  G711alaw: 8
MGCP Dynamic payload type for G.726-16K codec
MGCP Dynamic payload type for G.726-24K codec
MGCP Dynamic payload type for G.Clear codec
```

The following sample output displays the status of media source checking and the gateway role:

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 10.7.0.201 2497 Initial protocol service is MGCP 1.0
.
.
.
MGCP Dynamic payload type for NTE is 99
MGCP rsip-range is enabled for TGCP only.
MGCP Comedia role is PASSIVE
MGCP Comedia check media source is ENABLED
MGCP Comedia sdp force is DISABLED
MGCP Guaranteed scheduler time is DISABLED
MGCP DNS stale threshold is 30 seconds
.
.
.
```

The following is partial sample output from the **show mgcp** command when the mdste package has been disabled:

```
Router(config)# no mgcp package-capability mdste-package
Router(config)# exit
Router# show mgcp
MGCP voip mdste modem relay: Disabled
```

The table below describes the significant fields shown in the displays.

Table 19: show mgcp Field Descriptions

Field	Description
MGCP Admin State...Oper State	Administrative and operational state of the MGCP daemon. The administrative state controls the starting and the stopping of the application using the **mgcp** and **mgcp block-newcalls**commands. The operational state controls the normal MGCP operations.
MGCP call-agent	Address of the call agent specified in the **mgcp call-agent** or **call-agent** command and the protocol initiated for this session.
MGCP block-newcalls	State of the **mgcp block-newcalls** command.
MGCP send SGCP RSIP, disconnected	Setting for the **mgcp sgcp restart notify** and the **mgcp sgcp disconnected notify**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	Specifies whether the SGCP persistent events are handled by the quarantine buffer.
MGCP dtmf-relay	Setting for the **mgcp dtmf-relay** command.
MGCP voip modem passthrough	Settings for mode, codec, and redundancy from the **mgcp modem passthrough mode**, **mgcp modem passthrough codec**, and **mgcp modem passthrough voip redundancy** commands.
MGCP voip mdste modem relay	Settings for the **mgcp modem relay voip sprt v14 receive playback**, **mgcp modem relay voip sprt v14 transmit maximum hold-count**, **mgcp modem relay voip sprt v14 transmit hold-time**, **mgcp modem relay voip sprt retries**, **mgcp modem relay voip sse redundancy**, and **mgcp modem relay voip sse t1** commands.
SPRT rx v14 hold time	Setting for the **mgcp modem relay voip sprt v14 receive playback hold-time** *time* command.
SPRT tx v14 hold count	Setting for the **mgcp modem relay voip sprt v14transmit maximum hold-count** *characters* command.
SPRT tx v14 hold time	Setting for the **mgcp modem relay voip sprt v14 transmit hold-time** *time*command.
SPRT Retries	Setting for the **mgcp modem relay voip sprt retries** command.
SSE redundancy interval	Setting for the **mgcp modem relay voip mode sse redundancy interval** *time* command.
SSE redundancy packet	Setting for the **mgcp modem relay voip mode sse redundancy packet**command.
SSE t1 timer	Setting for the **mgcp modem relay voip mode sse redundancy t1** command.

Field	Description
SSE retries	Setting for the **mgcp modem relay voip mode sse redundancy retries**command.
MGCP Comedia role	Location of gateway: • **ACTIVE** --inside NAT • **PASSIVE** --outside NAT
MGCP Comedia check media source	Global media IP and port address detection status (ENABLED or DISABLED).
MGCP Comedia sdp force	Configuration state of forced insertion of the direction attribute in the SDP (ENABLED or DISABLED)
MGCP TSE payload	Setting for the **mgcp tse payload** command.
MGCP Network (IP/AAL2) Continuity Test timer	Setting for the **net-cont-test** keyword in the **mgcp timer** command.
MGCP 'RTP stream loss' timer	Setting for the **receive-rtcp** keyword in the **mgcp timer** command.
MGCP request timeout	Setting for the **mgcp request timeout** command.
MGCP maximum exponential request timeout	Setting for the **mgcp request timeout max** command.
MGCP gateway port	UDP port specification for the gateway.
MGCP maximum waiting delay	Setting for the **mgcp max-waiting-delay** command.
MGCP restart delay	Setting for the **mgcp restart-delay** command.
MGCP vad	Setting for the **mgcp vad**command.
MGCP rtrcac	Specifies whether MGCP SA Agent CAC has been enabled with the **mgcp rtrcac** command.
MGCP system resource check	Specifies whether MGCP SRC CAC has been enabled with the **mgcp src-cac**command.
MGCP xpc-codec	Specifies whether the **mgcp sdp xpc-codec**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).
MGCP persistent hookflash	Specifies whether the **mgcp persistent hookflash** command has been configured to send persistent hookflash events to the call agent.
MGCP persistent offhook	Specifies whether the **mgcp persistent offhook** command has been configured to send persistent off-hook events to the call agent.

Field	Description
MGCP persistent onhook	Specifies whether the **mgcp persistent onhook**command has been configured to send persistent on-hook events to the call agent.
MGCP piggyback msg	Specifies whether the **mgcp piggyback message** command has been configured to enable piggyback messaging.
MGCP endpoint offset	Specifies whether the **mgcp endpoint offset** 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	Specifies whether the **mgcp sdp simple**command has been configured to enable simple mode SDP operation.
MGCP undotted-notation	Specifies whether the **mgcp sdp notation undotted** command has been configured to enable undotted SDP notation for the codec string.
MGCP codec type	Setting for the **mgcp codec**command.
MGCP packetization period	The **packetization period**parameter setting for the **mgcp codec**command.
MGCP JB threshold lwm	Jitter-buffer minimum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP JB threshold hwm	Jitter-buffer maximum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP LAT threshold lwm	Latency minimum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP LAT threshold hwm	Latency maximum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP PL threshold lwm	Packet-loss minimum-threshold parameter setting for the **mgcp quality-threshold**command.
MGCP PL threshold hwm	Packet-loss maximum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP CL threshold lwm	Cell-loss minimum-threshold parameter setting for the **mgcp quality-threshold**command.
MGCP CL threshold hwm	Cell-loss maximum-threshold parameter setting for the **mgcp quality-threshold**command.
MGCP playout mode is	Jitter-buffer packet type and size.
MGCP default package	Package configured as the default package with the **mgcp default-package**command.

Field	Description
MGCP supported packages	Packages configured with the **mgcp package-capability** command to be supported on this gateway in this session. The Line Control Signaling Package (lcs-package) display is new in Cisco IOS Release 12.3(8)T.
MGCP voaal2 modem passthrough	Settings for mode, codec, and redundancy from the **mgcp modem passthrough mode**and **mgcp modem passthrough codec** commands.
MGCP T.38 Fax	Settings for the **mgcp fax t.38** command. The following values are displayed: • MGCP T.38 fax: ENABLED or DISABLED. • Error correction mode (ECM): ENABLED or DISABLED. • Nonstandard facilities (NSF) override: ENABLED or DISABLED. If enabled, the override code is displayed. • MGCP T.38 fax low-speed redundancy: the factor set on the gateway for redundancy. • MGCP T.38 fax high-speed redundancy: the factor set on the gateway for redundancy.

Related Commands

Command	Description
ccm-manager config	Supplies the local MGCP voice gateway with the IP address or logical name of the TFTP server from which to download XML configuration files and enable the download of the configuration.
debug ccm-manager	Displays debugging information about the Cisco CallManager.
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
isdn bind-l3 (interface BRI)	Configures the BRI to support MGCP and to bind ISDN Layer 3 with Cisco CallManager backhaul.
mgcp	Allocates resources for the MGCP and starts the daemon.
mgcp behavior comedia-check-media-src	Enables IP address and port detection from the first RTP packet received for the entire MGCP gateway.
mgcp behavior comedia-role	Indicates the location of the MGCP gateway.
mgcp behavior comedia-sdp-force	Forces the SDP to place the direction attribute in the SDP using the command as a reference.
mgcp package-capability mdste-package	Specifies the MGCP package capability type for a media gateway.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.

Command	Description
show ccm-manager	Displays a list of Cisco CallManager servers and their current statuses, and availability.
show ccm-manager fallback-mgcp	Displays the status of the MGCP gateway fallback feature.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp endpoint	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp profile	Displays values for MGCP profile-related parameters.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp connection

To display information for active connections that are controlled by the Media Gateway Control Protocol (MGCP), use the **show mgcp connection** command inprivileged EXEC mode.

show mgcp connection

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp**command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp**command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	Output for the **show mgcp**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 *MGCP VoIP Call Admission Control* .) The **nas dump** *slot port channel* and **nas info** keywords and arguments were added. Because the number of keywords increased, the command page for the **show mgcp** command was separated into the following command pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
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.

Release	Modification
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.3(11)T	Command output was enhanced to display the encryption suite used on the Secure Real-Time Transport Protocol (SRTP) connection.
12.4(2)T	Command output was enhanced to display the current media state.
12.4(11)T	Command output was enhanced to display the detected NAT address and port.

Examples

The following is sample output from the **show mgcp connection**command displaying a secure call for which the media state is modem relay mode:

```
Router# show mgcp connection
Endpoint  Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (CO)dec (E)vent[SIFL] (R)esult[EA]
(ME)dia
1. S2/DS1-2/1   C=A0000000010000100000000F5,4,3  I=0x2  P=17098,2662  M=3 S=4,4 CO=1 E=3,0,0,3
  R=0,0  ME=2
```

The following is sample output from this command showing the detected NAT address and port. The (P)ort output shows the local and advertised ports prior to detection. The (COM)Addr/Port output shows the detected media address and port (10.7.1.21:1500):

```
Router# show mgcp connection
Endpoint   Call_ID(C) Conn_ID (I) (P)ort (M)ode(S)tate(CO)dec (E)vent[SIFL] (R)esult[EA]
(COM)Addr/Port
S7/DS1-4/1 C=201597,768784,768785 I=0x5DD85 P=18258,19062 M=3 S=4,4 CO=2 E=2,0,0,2
R=0,0,0,2 COM=10.7.1.21:15000
```

The following is sample output from this command for encrypted connections:

```
Router# show mgcp connection
Endpoint       Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (CO)dec (E)vent[SIFL] (R)esult[EA]
 Encryption(K)
1. S1/DS1-0/1   C=2,1,2  I=0x2  P=18204,0  M=2  S=4,4 CO=1 E=0,0,0,0  R=0,0 K=1
```

The following is sample output from this command for VoIP connections:

```
Router# show mgcp connection
Endpoint   Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (C)odec (E)vent[SIFL] (R)esult[EA]
1. S0/DS1-0/1 C=103,23,24 I=0x8 P=16586,16634 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
2. S0/DS1-0/2 C=103,25,26 I=0x9 P=16634,16586 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
3. S0/DS1-0/3 C=101,15,16 I=0x4 P=16506,16544 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
4. S0/DS1-0/4 C=101,17,18 I=0x5 P=16544,16506 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
5. S0/DS1-0/5 C=102,19,20 I=0,6 P=16572,16600 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
6. S0/DS1-0/6 C=102,21,22 I=0x7 P=16600,16572 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
Total number of active calls 6
```

The following is sample output from this command for Voice over ATM Adaptation Layer 2 (VoAAL2) connections:

```
Router# show mgcp connection
Endpoint  Call_ID(C) Conn_ID(I)(V)cci/cid (M)ode (S)tate (C)odec (E)vent[SIFL] (R)esult[EA]
1.aaln/S1/1   C=1,11,12    I=0x2    V=2/10     M=3    S=4,4    C=1    E=3,0,0,3     R=0,0
Total number of active calls 1
```

The table below describes the significant fields shown in the displays.

Table 20: show mgcpconnection Field Descriptions

Field	Description
Endpoint	Endpoint for each call shown in the digital endpoint naming convention of slot number (S0) and digital line (DS1-0) number (1).
Call_ID(C)	MGCP call ID sent by the call agent, the internal Call Control Application Programming Interface (CCAPI) call ID for this endpoint, and the CCAPI call ID of the peer call legs. (CCAPI is an API that provides call control facilities to applications.)
(COM)Addr/Port	Detected media address and port.
Conn_ID(I)	Connection ID generated by the gateway and sent in the ACK message.
(P)ort	Ports used for this connection. The first port is the local User Datagram Protocol (UDP) port. The second port is the remote UDP port.
(V)cci/cid	Virtual channel connection identifier (VCCI) and channel identifier (CID) used for the VoAAL2 call.
(Me)dia	Media state, where: • 0--Voice • 1--Modem pass-through • 2--Modem relay
(M)ode	Call mode, where: • 0--Invalid value for mode. • 1--Gateway should only send packets. • 2--Gateway should only receive packets. • 3--Gateway should send and receive packets. • 4--Gateway should neither send nor receive packets. • 5--Gateway should place the circuit in loopback mode. • 6--Gateway should place the circuit in test mode. • 7--Gateway should use the circuit for network access for data. • 8--Gateway should place the connection in network loopback mode. • 9--Gateway should place the connection in network continuity test mode. • 10--Gateway should place the connection in conference mode. All other values are used for internal debugging.
(S)tate	Call state. The values are used for internal debugging purposes.

Field	Description
(Co)dec	Codec identifier. The values are used for internal debugging purposes.
(E)vent [SIFL]	Used for internal debugging.
(R)esult [EA]	Used for internal debugging.
Encryption(K)	Encryption suite, where: • 0--None • 1--AES_CM_128_HMAC_SHA1_32

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
mgcp behavior comedia-check-media-src	Enables ip address and port detection from the first rtp packet received for the entire MGCP gateway.
mgcp behavior comedia-role	Indicates the location of the MGCP gateway.
mgcp behavior comedia-sdp-force	Forces the SDP to place the direction attribute in the SDP using the command as a reference.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays values for MGCP parameters.
show mgcp endpoints	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp profile	Displays values for MGCP profile-related parameters.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp endpoint

To display information for endpoints controlled by Media Gateway Control Protocol (MGCP), use the **show mgcp endpoint** command inprivileged EXEC mode.

show mgcp endpoint

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp**command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	The output for the **show mgcp** 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 *MGCP VoIP Call Admission Control.*) In addition, the **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. Because the number of keywords increased, the command-reference page for the **show mgcp** command was separated into the following command-reference pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
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.

Release	Modification
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Examples

The following is sample output from this command:

```
Router#
show mgcp endpoint
       ENDPOINT-NAME      V-PORT SIG-TYPE ADMIN
     ds1-0/1@nytnk116      0:1    fxs-gs     up
     ds1-0/2@nytnk116      0:1    fxs-gs     up
     ds1-0/3@nytnk116      0:1    fxs-gs     up
     ds1-0/4@nytnk116      0:1    fxs-gs     up
     ds1-0/5@nytnk116      0:1    fxs-gs     up
     ds1-0/6@nytnk116      0:1    fxs-gs     up
     ds1-0/7@nytnk116      0:1    fxs-gs     up
     ds1-0/8@nytnk116      0:1    fxs-gs     up
     ds1-0/9@nytnk116      0:1    fxs-gs     up
    ds1-0/10@nytnk116      0:1    fxs-gs     up
    ds1-0/11@nytnk116      0:1    fxs-gs     up
    ds1-0/12@nytnk116      0:1    fxs-gs     up
    ds1-0/13@nytnk116      0:1    fxs-gs     up
    ds1-0/14@nytnk116      0:1    fxs-gs     up
    ds1-0/15@nytnk116      0:1    fxs-gs     up
    ds1-0/16@nytnk116      0:1    fxs-gs     up
    ds1-0/17@nytnk116      0:1    fxs-gs     up
    ds1-0/18@nytnk116      0:1    fxs-gs     up
    ds1-0/19@nytnk116      0:1    fxs-gs     up
    ds1-0/20@nytnk116      0:1    fxs-gs     up
    ds1-0/21@nytnk116      0:1    fxs-gs     up
    ds1-0/22@nytnk116      0:1    fxs-gs     up
    ds1-0/23@nytnk116      0:1    fxs-gs     up
    ds1-0/24@nytnk116      0:1    fxs-gs     up
Interface T1 1
        ENDPOINT-NAME      V-PORT SIG-TYPE ADMIN
     ds1-1/1@nytnk116      1:1    e&m-imd    up
     ds1-1/2@nytnk116      1:1    e&m-imd    up
```

The table below describes significant fields shown in this output.

Table 21: show mgcp endpoint Field Descriptions

Field	Description
ENDPOINT-NAME	Name used by the call agent to identify a specific mgcp endpoint on a given gateway.
V-PORT	Voice port
SIG-TYPE	Signaling type for a given endpoint (for example, NONE for SS7 ISDN User Part (ISUP) and FXS-GS for Foreign Exchange Station (FXS) Ground Start).
ADMIN	Administrative status--Up or Down. (This field is populated only on residential gateway (RGW) platforms.

Related Commands

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

show mgcp nas

To display Media Gateway Control Protocol (MGCP) network access server (NAS) information for data ports, use the **show mgcp nas** command in privileged EXEC mode.

show mgcp nas {**dump** *slot port channel* | **info**}

Syntax Description

dump *slot port channel*	Displays NAS information for the specified port and channel. The arguments are as follows:
	• *slot* --Chassis slot for interface card. Values are as follows:
	  • Cisco AS5350: From 0 to 3.
	  • Cisco AS5400: From 0 to 7.
	  • Cisco AS5850: From 0 to 5 and from 8 to 13. Slots 6 and 7 are reserved for the route switch controller (RSC).
	• *port* --Modem interface port. Values are as follows:
	  • Cisco AS5350: For T1/E1, from 0 to 7. For T3, from 1 to 28.
	  • Cisco AS5400: For T1/E1, from 0 to 7. For T3, from 1 to 28.
	  • Cisco AS5850: For T1/E1, from 0 to 23. For T3, from 1 to 28.
	• *channel* --T1 or E1 channel. Values for T1 are from 1 to 24. Values for E1 are from 1 to 31.

info	Displays status of NAS channels.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp** command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

Release	Modification
12.2(2)XB	The output for the **show mgcp** 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 *MGCP VoIP Call Admission Control.*) In addition, the **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. Because the number of keywords increased, the command-reference page for the **show mgcp** command was separated into the following command-reference pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
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, Cisco AS5800, and Cisco AS5850 in this release.
12.3(7)YB	The valid values for the bearer cap field of the **show mgcp nas dump** command output were changed to include LAPB, V.120, and sync data. The Signaling field was added to the **show mgcp nas dump** command output. See the table below.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T

Examples

The following is sample output from this command for an autodetected V.120 call:

```
Router# show mgcp nas dump 1 7 24
Slot 1 state=Up
Port 7 state=Up
State In Use PortCb=0x6577949C ss_id=0x0 handle=0x65C88228
Bearer Cap=V.120 call_id=1 conn_id=6577B8EC
Sig Type=Autodetect
Events req- nas/crq- req id=7 :nas/of- req id=7 :
Endpt name=S1/DS1-7/24
call_id = 1, conn_id=0x6577B8EC cgn=1000 cdn=5555
Rx packets=610  Rx bytes=73242 Tx packets 716 Tx bytes 72987
```

The table below describes the significant fields shown in the display.

Table 22: show mgcp nas dump Field Descriptions

Field	Description
Slot state	Status of specified slot.

Field	Description
Port state	Status of specified port.
State	Call status for the specified channel.
bearer cap	Bearer capability. Values are: • Modem • LAPB • V.110 • V.120 • Digital 64 • Digital 56 V.110, V.120, modem, or digital values are displayed when autodetection is not enabled and the signaling type is set to External. LAPB, V.120, and digital values are displayed if autodetection is enabled, and the signaling type is set to Autodetect.
call_id	Call identification for the currently active call, if any.
conn_id	Connection identification for the currently active call, if any.
Signaling	Call type signaling. Values are: • External--Call type is signaled by the call agent. • Autodetect--Call type is autodetected by the gateway.
Events req	List of NAS events requested, if any, and their request IDs. The request ID identifies the MGCP message from the call agent that requested the events.
Endpt name	MGCP endpoint name.

The following sample output from this command shows the state, either Idle or In Use, for each channel:

```
Router# show mgcp nas info
Number of ports configured=1
Slot 1 configured  slot state=Up  Port 7 state=Up
=====Port 7 Channel States=====
 0  Idle
 1  Idle
 2  Idle
 3  Idle
 4  Idle
 5  Idle
 6  Idle
 7  Idle
 8  Idle
 9  Idle
 10 Idle
 11 Idle
```

```
 12 Idle
 13 Idle
 14 Idle
 15 Idle
 16 Idle
 17 Idle
 18 Idle
 19 Idle
 20 Idle
 21 Idle
 22 Idle
 23 In Use
=====================================
```

Related Commands

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

show mgcp profile

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

show mgcp profile [*profile-name*]

Syntax Description

profile -name	(Optional) Name of the MGCP profile for which information should be displayed; limited to 32 characters.

Command Default

If the optional *profile-name* argument is not used, all configured profiles are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp** command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	Output for the **show mgcp**command was enhanced to display the status of MGCP System Resource Check (SRC) Call Admission Control (CAC) and Service Assurance Agent (SA Agent) CAC. (See the Cisco IOS Release 12.2(2)XB online document *MGCP VoIP Call Admission Control.*) In addition, the **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. Because the number of keywords increased, the command-reference page for the **show mgcp** command was separated into the following command-reference pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**

Release	Modification
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, Cisco AS5800, and Cisco AS5850 in this release.
12.4(4)T	Output was added to show the order in which ANI and DNIS digits are sent to the call agent.

Examples

The following is sample output for this command for the default profile:

```
Router# show mgcp profile default
MGCP Profile default
Description: None
Call-agent: none Initial protocol service is unknown
Tsmax timeout is 20 sec, Tdinit timeout is 15 sec
Tdmin timeout is 15 sec, Tdmax timeout is 600 sec
Tcrit timeout is 4 sec, Tpar timeout is 16 sec
Thist timeout is 30 sec, MWI timeout is 16 sec
Ringback tone timeout is 180 sec, Ringback tone on connection timeout is 180 sec
Network congestion tone timeout is 180 sec, Busy tone timeout is 30 sec
Dial tone timeout is 16 sec, Stutter dial tone timeout is 16 sec
Ringing tone timeout is 180 sec, Distinctive ringing tone timeout is 180 sec
Continuity1 tone timeout is 3 sec, Continuity2 tone timeout is 3 sec
Reorder tone timeout is 30 sec,  Persistent package is ms-package
Max1 DNS lookup: ENABLED, Max1 retries is 5
Max2 DNS lookup: ENABLED, Max2 retries is 7
Source Interface: NONE
T3 endpoint naming convention is T1
CAS Notification Digit order is DNIS-ANI
```

The following is sample output for this command for a profile named "example"*:*

```
Router# show mgcp profile example
MGCP Profile example
Description:None
Call-agent:10.9.57.6 5003 Initial protocol service is MGCP 1.0
Tsmax timeout is 20, Tdinit timeout is 15
Tdmin timeout is 15, Tdmax timeout is 600
Tcrit timeout is 4, Tpar timeout is 16
Thist timeout is 30, MWI timeout is 16
Ringback tone timeout is 180, Ringback tone on connection timeout is 180
Network congestion tone timeout is 180, Busy tone timeout is 30
Dial tone timeout is 16, Stutter dial tone timeout is 16
Ringing tone timeout is 180, Distinctive ringing tone timeout is 180
Continuity1 tone timeout is 3, Continuity2 tone timeout is 3
Reorder tone timeout is 30,  Persistent package is ms-package
Max1 DNS lookup:ENABLED, Max1 retries is 4
Max2 DNS lookup:ENABLED, Max2 retries is 6
Voice port:1
```

The table below describes significant fields shown in these outputs.

Table 23: show mgcp profile Field Descriptions

Field	Description
MGCP Profile	The name configured for this profile with the **mgcp profile** command.

Field	Description
Description	Description configured for this profile with the **description MGCP profile**command.
Call-agent	Domain name server (DNS) or IP address of the call agent, as configured for this profile with the **call-agent**command.
Initial protocol service	Protocol service to be used, as configured for this profile with the **call-agent** command.
Tsmax timeout	Maximum timeout value for removing messages from the retransmission queue, as configured for this profile by the **timeout tsmax** command.
Tdinit timeout	Initial waiting delay, as configured for this profile by the **timeout tdinit** command.
Tdmin timeout	Minimum timeout value for the disconnected procedure, as configured for this profile by the **timeout tdmin** command.
Tdmax timeout	Maximum timeout value for the disconnected procedure, as configured for this profile by the **timeout tdmax** command.
Tcrit timeout	Critical timeout value for the interdigit timer used in digit matching, as configured for this profile by the **timeout tcrit** command.
Tpar timeout	Partial timeout value for the interdigit timer used in digit matching, as configured for this profile by the **timeout tpar** command.
Thist timeout	Packet storage timeout value, as configured for this profile by the **timeout thist** command.
MWI timeout	Timeout value for message-waiting-indicator tone, as configured for this profile by the **timeout tone mwi** command.
Ringback tone timeout	Timeout value for ringback tone, as configured for this profile by the **timeout tone ringback** command.
Ringback tone on connection timeout	Timeout value for ringback tone on connection, as configured for this profile by the **timeout tone ringback connection** command.
Network congestion tone timeout	Timeout value for the network congestion tone, as configured for this profile by the **timeout tone network congestion** command.
Busy tone timeout	Timeout value for the busy tone, as configured for this profile by the **timeout tone busy** command.
Dial tone timeout	Timeout value for the dial tone, as configured for this profile by the **timeout tone dial** command.
Stutter dial tone timeout	Timeout value for the stutter dial tone, as configured for this profile by the **timeout tone dial stutter** command.
Ringing tone timeout	Timeout value for the ringing tone, as configured for this profile by the **timeout tone ringing** command.

Field	Description
Distinctive ringing tone timeout	Timeout value for the distinctive ringing tone, as configured for this profile by the **timeout tone ringing distinctive** command.
Continuity1 tone timeout	Timeout value for the continuity1 tone, as configured for this profile by the **timeout tone cot1** command.
Continuity2 tone timeout	Timeout value for the continuity2 tone, as configured for this profile by the **timeout tone cot2** command.
Reorder tone timeout	Timeout value for the reorder tone, as configured for this profile by the **timeout tone reorder** command.
Persistent package	Name of package configured as persistent for this profile by the **package persistent** command.
Max1 lookup	Domain name server (DNS) lookup for the call agent after the suspicion threshold is reached, as configured for this profile by the **max1 lookup** command.
Max1 retries	Number of retries to reach the call agent before a new DNS lookup is performed, as configured for this profile by the **max1 retries** command.
Max2 lookup	DNS lookup for the call agent after the disconnected threshold is reached, as configured by the **max2 lookup** command.
Max2 retries	Maximum number of retries to reach the call agent before a new DNS lookup is performed, as configured by the **max2 retries** command.
CAS Notification Digit order	Order in which ANI and DNIS digits are sent in the notify message as configured with the **notify** command.

Related Commands

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

show mgcp srtp

To display information for active Secure Real-Time Transport Protocol (SRTP) connections that are controlled by Media Gateway Control Protocol (MGCP), use the **show mgcp srtp** command inprivileged EXEC mode.

show mgcp srtp {**summary** | **detail** [*endpoint*]}

Syntax Description

summary	Displays MGCP SRTP connections summary.

detail *endpoint*	Displays MGCP SRTP connections details.
	• The *endpoint* argument allows you to limit the display to endpoints for a specific connection. The *endpoint*argument can take the following values:
	  • Port numbers.
	  • The asterisk wildcard character*.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

This command provides information about secure calls created by the MGCP application. To specify connection endpoints for display, use the **show mgcp srtp detail endpoint** command. To display valid values for the *endpoint* argument, that is, the endpoint port numbers, use the **show mgcp connection** command. Use the **show mgcp srtp detail** command to display a hashed version of the primary key and salts (encryption mechanisms) used on each connection. This display allows you to validate keys and salts for each endpoint of a call without revealing the actual primary key and salt.

Examples

The following is sample output from this command for encrypted connections:

```
Router# show mgcp srtp summary
MGCP SRTP Connection Summary
Endpoint             Conn Id    Crypto Suite
aaln/S3/SU0/0        8          AES_CM_128_HMAC_SHA1_32
aaln/S3/SU0/1        9          AES_CM_128_HMAC_SHA1_32
S3/DS1-0/1           6          AES_CM_128_HMAC_SHA1_32
S3/DS1-0/2           7          AES_CM_128_HMAC_SHA1_32
4 SRTP connections active


Router# show mgcp srtp detail
MGCP SRTP Connection Detail for Endpoint *

Definitions: CS=Crypto Suite, KS=HASHED Key/Salt, SSRC=Syncronization Source, ROC=Rollover
 Counter, KDR=Key Derivation Rate, SEQ=Sequence Number, FEC=FEC Order, MLT=Key Lifetime,
MKI=Key Index:MKI Size

Endpoint aaln/S0/SU2/1 Call ID 40294955 Conn ID 4
```

```
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=2FFkUcBi/+XbiwKapdySC0F4nOQ= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=XrCnoQ4ef8385GRNdTIUnFkbkN0= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0

1 SRTP connections displayed


Router# show mgcp srtp detail S3/DS1-0/
*
show mgcp srtp detail aaln/S0/SU2/1
MGCP SRTP Connection Detail for Endpoint aaln/S0/SU2/1

Definitions: CS=Crypto Suite, KS=HASHED Key/Salt, SSRC=Syncronization Source, ROC=Rollover
 Counter, KDR=Key Derivation Rate, SEQ=Sequence Number, FEC=FEC Order, MLT=Key Lifetime,
MKI=Key Index:MKI Size

Endpoint aaln/S0/SU2/1 Call ID 40294955 Conn ID 4
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=2FFkUcBi/+XbiwKapdySC0F4nOQ= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=ayYP5V9d+z2L4fUNyk8E7VwOGs8= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0

1 SRTP connections displayed
```

The table below describes the significant fields shown in the display.

Table 24: show mgcpsrtp Field Descriptions

Field	Description
Endpoint	Endpoint for each call, shown in the digital endpoint naming convention of slot number (S0) and digital line (DS1-0) number (1).
Call ID	MGCP call ID sent by the call agent.
Conn ID	Connection ID generated by the gateway and sent in the ACK message.
Crypto Suite	Identifies the cryptographic suite used on the connection.

Related Commands

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

Command	Description
show mgcp profile	Displays values for MGCP profile-related parameters.

show mgcp statistics

To display Media Gateway Control Protocol (MGCP) statistics regarding received and transmitted network messages, use the **show mgcp statistics**command in privileged EXEC mode.

show mgcp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp** command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	Output for the **show mgcp** 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 *MGCP VoIP Call Admission Control.*) The **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. To simplify the command reference, the command page for the **show mgcp** command was separated into the following command pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
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.

Release	Modification
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.3(11)T	Output was enhanced to display dropped packets from unconfigured call agents if call-agent validation is enabled.

Examples

The following is sample output from this command for VoIP and VoAAL2 statistics:

```
Router# show mgcp statistics
UDP pkts rx 8, tx 9
Unrecognized rx pkts 0, MGCP message parsing errors 0
Duplicate MGCP ack tx 0, Invalid versions count 0
Rx packets from unknown Call Agent 0
CreateConn rx 4, successful 0, failed 0
DeleteConn rx 2, successful 2, failed 0
ModifyConn rx 4, successful 4, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 4, failed 0
AuditConnection rx 0, successful 0, failed 0
AuditEndpoint rx 0, successful 0, failed 0
RestartInProgress tx 1, successful 1, failed 0
Notify tx 0, successful 0, failed 0
ACK tx 8, NACK tx 0
ACK rx 0, NACK rx 0
IP address based Call Agents statistics:
IP address 10.24.167.3, Total msg rx 8, successful 8, failed 0
```

The following is an example of the MGCP VoIP SRC CAC portion of this command output for a gateway configured with MGCP VoIP SRC CAC:

```
Router# show mgcp statistics
MGCP System Resource Check Statistics:
-------------------------------------
Total CreateConn checked by SRC :0
CreateConn accepted by SRC:0
CreateConn rejected by SRC:0
Total ModifyConn checked by SRC :0
ModifyConn accepted by SRC:0
ModifyConn rejected by SRC:0
Reason          Num. of requests rejected
------          -------------------------
cpu-5sec:       0
cpu-avg:        0
total-mem:      0
io-mem:         0
proc-mem:       0
total-calls:    0
```

The table below describes significant fields shown in this output.

Table 25: show mgcp statistics Field Descriptions

Field	Description
UDP pkts rx, tx	Number of User Datagram Protocol (UDP) packets transmitted and received from the call agent by the gateway MGCP application.

Field	Description
Unrecognized rx pkts	Number of unrecognized UDP packets received by the MGCP application.
MGCP message parsing errors	Number of MGCP messages received with parsing errors.
Duplicate MGCP ack tx	Number of duplicate MGCP acknowledgment messages transmitted to the call agents.
Invalid versions count	Number of MGCP messages received with invalid MGCP protocol versions.
Rx packets from unknown Call Agent	Number of dropped packets from unconfigured call agents.
CreateConn rx	Number of Create Connection (CRCX) messages received by the gateway, the number that were successful, and the number that failed.
DeleteConn rx	Number of Delete Connection (DLCX) messages received by the gateway, the number that were successful, and the number that failed.
DeleteConn tx	Number of DLCX messages sent from the gateway to the call agent (CA).
ModifyConn rx	Number of Modify Connection (MDCX) messages received by the gateway, the number that were successful, and the number that failed.
NotifyRequest rx	Number of Notify Request (RQNT) messages received by the gateway, the number that were successful, and the number that failed.
AuditConnection rx	Number of Audit Connection (AUCX) messages received by the gateway, the number that were successful, and the number that failed.
AuditEndpoint rx	Number of Audit Endpoint (AUEP) messages received by the gateway, the number that were successful, and the number that failed.
RestartInProgress tx	Number of Restart in Progress (RSIP) messages sent by the gateway, the number that were successful, and the number that failed.
Notify tx	Number of Notify (NTFY) messages sent by the gateway, the number that were successful, and the number that failed.
ACK tx, NACK tx	Number of Acknowledgment and Negative Acknowledgment messages sent by the gateway.
ACK rx, NACK rx	Number of Acknowledgment and Negative Acknowledgment messages received by the gateway.
IP address based Call Agents statistics: IP address, Total msg rx	IP address of the call agent, the total number of MGCP messages received from that call agent, the number of messages that were successful, and the number of messages that failed.
Total CreateConn checked by SRC	Total number of Create Connection (CRCX) messages that have been checked against the SRC component.

Field	Description
CreateConn accepted by SRC	Number of CRCX messages that have been accepted after being checked by the SRC component.
CreateConn rejected by SRC	Number of CRCX messages that have been rejected by SRC because of resource constraints.
Total ModifyConn checked by SRC	Total number of Modify Connection (MDCX) messages that have been checked against the SRC component.
ModifyConn accepted by SRC	Number of MDCX messages that have been accepted after being checked by the SRC component.
ModifyConn rejected by SRC	Number of MDCX messages that have been rejected by SRC because of resource constraints.
Reason	Specific threshold that was exceeded to cause the rejection.
Num. of requests rejected	Number of requests that have been rejected.
cpu-5sec	CPU utilization for previous 5 seconds threshold was exceeded.
cpu-avg	Average CPU utilization threshold was exceeded.
total-mem	Total memory utilization threshold was exceeded.
io-mem	I/O memory utilization threshold was exceeded.
proc-mem	Processor memory utilization threshold was exceeded.
total-calls	Total number of calls threshold was exceeded.

Related Commands

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

show modem relay statistics

To display various statistics for modem relay, use the **show modem relay statistics** command in privileged EXEC mode.

show modem relay statistics {**all** | **phy** | **pkt** | **queue** | **sprt** | **timer** | **v14** | **v42**} [**call-identifier** *call-setup-time call-index*]

Syntax Description

all	All statistics associated with the modem-relay feature.
phy	Modem-relay physical layer statistics.
pkt	Modem-relay packetizer statistics.
queue	Modem-relay queue statistics.
sprt	Modem-relay SPRT layer statistics.
timer	Modem-relay timer statistics.
v14	Modem-relay V.14 statistics
v42	Modem-relay V.42 statistics.
call -identifier *call-setup-time*	(Optional) Value of the system UpTime when the call that is associated with this entry was started. Range is from 0 to 4294967295.
call -identifier *call-index*	(Optional) Dial-peer identification number used to distinguish between calls with the same setup time. Range is from 0 to 4294967295.

Command Default

No statistics are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 7200 series, and Cisco AS5300.
12.4(2)T	The **v14** keyword was added.

Usage Guidelines

Use this command to display various modem-relay call statistics, including counts of different types of packets, errors, and events, for all modem-relay calls.

Display statistics for a specific modem-relay call by using the **call-identifier** keyword and specifying the call-setup time and call index of the desired call. Obtain values for the call-setup time and call index from the SetupTime and Index fields at the start of each call record in the **show call active** command output.

Examples

The following is sample output from the **show modem relay statistics v14** command:

```
Router# show modem relay statistics v14
```

ID:11D6

V14 Layer Statistics

```
        sync_count=47 sync_loss_count=46
        min_bundle_size_rcvd_local=1 max_bundle_size_rcvd_local=20
        min_bundle_size_rcvd_remote=0 max_bundle_size_rcvd_remote=0
        info_bytes_removed_dueto_phy_rcv_q=0
        overflow_count_rcv_q=0
        info_bytes_removed_dueto_old_age_rcv_q=0
        info_bytes_discarded_bad_offset_rcv_q=0
        info_bytes_overwrite_rcv_q=0
        info_bytes_filled_rcv_q=0
        total_bytes_rcv_local=310
        min_bundle_size_send_local=0, max_bundle_size_send_local=0
        min_bundle_size_send_network=1, max_bundle_size_send_network=22
        info_bytes_removed_dueto_phy_xmit_q=0, overflow_count_xmit_q=0
        info_bytes_discarded_bad_offset_xmit_q=0
        info_bytes_overwrite_xmit_q=0
        info_bytes_filled_xmit_q=0, total_bytes_xmit_local=0
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics all call-identifier 43009 1
ID:3
SPRT Layer Statistics
        sprt_info_frames_rcvd=10 sprt_xid_frames_rcvd=0
        sprt_tc0_explicit_acks_rcvd=6 sprt_tc1_explicit_acks_rcvd=122
        sprt_tc2_explicit_acks_rcvd=126 sprt_destructive_brks_rcvd=0
        sprt_expedited_brks_rcvd=0
        sprt_non_expedited_brks_rcvd=0
        sprt_info_tframes_sent=9 sprt_info_tframes_resent=0
        sprt_xid_frames_sent=0 sprt_tc0_explicit_acks_sent=8
        sprt_tc1_explicit_acks_sent=129 sprt_tc2_explicit_acks_sent=132
        sprt_destructive_brks_sent=0
        sprt_expedited_brks_sent=0
        sprt_non_expedited_brks_sent=0
        sprt_info_tframes_asked_to_consumed=10
        sprt_info_tframes_consumed=10
        sprt_info_tframes_failed_to_consume=0
        sprt_info_bytes_rcvd=10 sprt_info_bytes_sent=76
        sprt_pkts_dropped_intf_busy=289 sprt_min_rexmit_timeout=500
        sprt_max_rexmit_timeout=500
Queue Statistics
        sprt_tc1_rcv_qdrops=0 sprt_tc1_xmit_qdrops=0
        sprt_tc2_rcv_qdrops=0 sprt_tc2_xmit_qdrops=0
        pktizer_out_qdrops=4 pktizer_in_qdrops=0 v42_xmit_qdrops=0
V42 Layer Statistics
        vs_chng_dueto_timeouts=0 vs_chng_dueto_rej=0
        vs_chng_dueto_rnr_resp_f1_set=0 nr_seq_exception=0
        good_rcvd_lapm_pkts=1385 discarded_rcvd_lapm_pkts=0
        rejected_rcvd_lapm_pkts=0 v42_rcvd_iframe=9
        v42_rcvd_rr=1374 v42_rcvd_rnr=0 v42_rcvd_rej=0
        v42_rcvd_srej=0 v42_rcvd_sabme=0 v42_rcvd_dm=0
        v42_rcvd_ui=0 v42_rcvd_disc=0 v42_rcvd_ua=1
        v42_rcvd_frmr=0 v42_rcvd_xid=1 v42_rcvd_test=0
        v42_rcvd_destructive_brk=0 v42_rcvd_expedited_brk=0
        v42_rcvd_non_expedited_brk=0 v42_rcvd_brkack=0
        v42_sent_iframe=10 v42_sent_rr=1464 v42_sent_rnr=0
```

```
        v42_sent_rej=0 v42_sent_srej=0 v42_sent_sabme=1
        v42_sent_dm=0 v42_sent_ui=0 v42_sent_disc=0
        v42_sent_ua=0 v42_sent_frmr=0 v42_sent_xid=1
        v42_sent_test=0 v42_sent_destructive_brk=0
        v42_sent_expedited_brk=0
        v42_sent_non_expedited_brk=0
        v42_sent_brkack=0
Physical Layer Statistics
        num_local_retrain=0 num_remote_retrain=0
        num_local_speed_shift=0 num_remote_speed_shift=0
        num_sync_loss=0
Packetizer Statistics
        frames_inprogress=5 good_crc_frames=1385
        bad_crc_frames=31 frame_aborts=124
        hdlc_sync_detects=1 hdlc_sync_loss_detects=0
        bad_frames=0
Timer Statistics
        xid_timer_cnt=0 sabme_timer_cnt=0 ack_timer_cnt=0
        chkpnt_timer_cnt=1333
```

The following is sample output from this command:

```
Router# show modem relay statistics all
ID:3
SPRT Layer Statistics
        sprt_info_frames_rcvd=10 sprt_xid_frames_rcvd=0
        sprt_tc0_explicit_acks_rcvd=6 sprt_tc1_explicit_acks_rcvd=155
        sprt_tc2_explicit_acks_rcvd=158 sprt_destructive_brks_rcvd=0
        sprt_expedited_brks_rcvd=0
        sprt_non_expedited_brks_rcvd=0
        sprt_info_tframes_sent=9 sprt_info_tframes_resent=0
        sprt_xid_frames_sent=0 sprt_tc0_explicit_acks_sent=8
        sprt_tc1_explicit_acks_sent=161 sprt_tc2_explicit_acks_sent=165
        sprt_destructive_brks_sent=0
        sprt_expedited_brks_sent=0
        sprt_non_expedited_brks_sent=0
        sprt_info_tframes_asked_to_consumed=10
        sprt_info_tframes_consumed=10
        sprt_info_tframes_failed_to_consume=0
        sprt_info_bytes_rcvd=10 sprt_info_bytes_sent=76
        sprt_pkts_dropped_intf_busy=357 sprt_min_rexmit_timeout=500
        sprt_max_rexmit_timeout=500
Queue Statistics
        sprt_tc1_rcv_qdrops=0 sprt_tc1_xmit_qdrops=0
        sprt_tc2_rcv_qdrops=0 sprt_tc2_xmit_qdrops=0
        pktizer_out_qdrops=4 pktizer_in_qdrops=0 v42_xmit_qdrops=0
V42 Layer Statistics
        vs_chng_dueto_timeouts=0 vs_chng_dueto_rej=0
        vs_chng_dueto_rnr_resp_f1_set=0 nr_seq_exception=0
        good_rcvd_lapm_pkts=1910 discarded_rcvd_lapm_pkts=0
        rejected_rcvd_lapm_pkts=0 v42_rcvd_iframe=9
        v42_rcvd_rr=1899 v42_rcvd_rnr=0 v42_rcvd_rej=0
        v42_rcvd_srej=0 v42_rcvd_sabme=0 v42_rcvd_dm=0
        v42_rcvd_ui=0 v42_rcvd_disc=0 v42_rcvd_ua=1
        v42_rcvd_frmr=0 v42_rcvd_xid=1 v42_rcvd_test=0
        v42_rcvd_destructive_brk=0 v42_rcvd_expedited_brk=0
        v42_rcvd_non_expedited_brk=0 v42_rcvd_brkack=0
        v42_sent_iframe=10 v42_sent_rr=1988 v42_sent_rnr=0
        v42_sent_rej=0 v42_sent_srej=0 v42_sent_sabme=1
        v42_sent_dm=0 v42_sent_ui=0 v42_sent_disc=0
        v42_sent_ua=0 v42_sent_frmr=0 v42_sent_xid=1
        v42_sent_test=0 v42_sent_destructive_brk=0
        v42_sent_expedited_brk=0
        v42_sent_non_expedited_brk=0
```

```
        v42_sent_brkack=0
Physical Layer Statistics
        num_local_retrain=0 num_remote_retrain=0
        num_local_speed_shift=0 num_remote_speed_shift=0
        num_sync_loss=0
Packetizer Statistics
        frames_inprogress=5 good_crc_frames=1910
        bad_crc_frames=31 frame_aborts=124
        hdlc_sync_detects=1 hdlc_sync_loss_detects=0
        bad_frames=0
Timer Statistics
        xid_timer_cnt=0 sabme_timer_cnt=0 ack_timer_cnt=0
        chkpnt_timer_cnt=1809
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics sprt
ID:3
SPRT Layer Statistics
        sprt_info_frames_rcvd=10 sprt_xid_frames_rcvd=0
        sprt_tc0_explicit_acks_rcvd=6 sprt_tc1_explicit_acks_rcvd=177
        sprt_tc2_explicit_acks_rcvd=180 sprt_destructive_brks_rcvd=0
        sprt_expedited_brks_rcvd=0
        sprt_non_expedited_brks_rcvd=0
        sprt_info_tframes_sent=9 sprt_info_tframes_resent=0
        sprt_xid_frames_sent=0 sprt_tc0_explicit_acks_sent=8
        sprt_tc1_explicit_acks_sent=183 sprt_tc2_explicit_acks_sent=187
        sprt_destructive_brks_sent=0
        sprt_expedited_brks_sent=0
        sprt_non_expedited_brks_sent=0
        sprt_info_tframes_asked_to_consumed=10
        sprt_info_tframes_consumed=10
        sprt_info_tframes_failed_to_consume=0
        sprt_info_bytes_rcvd=10 sprt_info_bytes_sent=76
        sprt_pkts_dropped_intf_busy=403 sprt_min_rexmit_timeout=500
        sprt_max_rexmit_timeout=500
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics queue
ID:3
Queue Statistics
        sprt_tc1_rcv_qdrops=0 sprt_tc1_xmit_qdrops=0
        sprt_tc2_rcv_qdrops=0 sprt_tc2_xmit_qdrops=0
        pktizer_out_qdrops=4 pktizer_in_qdrops=0 v42_xmit_qdrops=0
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics v42
ID:3
V42 Layer Statistics
        vs_chng_dueto_timeouts=0 vs_chng_dueto_rej=0
        vs_chng_dueto_rnr_resp_f1_set=0 nr_seq_exception=0
        good_rcvd_lapm_pkts=2442 discarded_rcvd_lapm_pkts=0
        rejected_rcvd_lapm_pkts=0 v42_rcvd_iframe=9
        v42_rcvd_rr=2431 v42_rcvd_rnr=0 v42_rcvd_rej=0
        v42_rcvd_srej=0 v42_rcvd_sabme=0 v42_rcvd_dm=0
        v42_rcvd_ui=0 v42_rcvd_disc=0 v42_rcvd_ua=1
        v42_rcvd_frmr=0 v42_rcvd_xid=1 v42_rcvd_test=0
        v42_rcvd_destructive_brk=0 v42_rcvd_expedited_brk=0
```

```
        v42_rcvd_non_expedited_brk=0 v42_rcvd_brkack=0
        v42_sent_iframe=10 v42_sent_rr=2539 v42_sent_rnr=0
        v42_sent_rej=0 v42_sent_srej=0 v42_sent_sabme=1
        v42_sent_dm=0 v42_sent_ui=0 v42_sent_disc=0
        v42_sent_ua=0 v42_sent_frmr=0 v42_sent_xid=1
        v42_sent_test=0 v42_sent_destructive_brk=0
        v42_sent_expedited_brk=0
        v42_sent_non_expedited_brk=0
        v42_sent_brkack=0
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics phy
ID:3
Physical Layer Statistics
        num_local_retrain=0 num_remote_retrain=0
        num_local_speed_shift=0 num_remote_speed_shift=0
        num_sync_loss=0
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay stat pkt
ID:3
Packetizer Statistics
        frames_inprogress=5 good_crc_frames=2573
        bad_crc_frames=61 frame_aborts=150
        hdlc_sync_detects=1 hdlc_sync_loss_detects=0
        bad_frames=0
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay stat timer
ID:3
Timer Statistics
        xid_timer_cnt=0 sabme_timer_cnt=0 ack_timer_cnt=0
        chkpnt_timer_cnt=2750
        Total Modem Relay Call Legs = 1
```

Related Commands

Command	Description
debug voip ccapi inout	Traces the execution path through the call control API.
debug vtsp all	Displays all VTSP debugging except statistics, tone, and event.
show call active	Displays active call information for voice calls or fax transmissions in progress.
show call active voice	Displays current call information for a call in progress.
show modems	Displays all modem configurations.