

show pas caim

To show debug information about the data compression Advanced Interface Module (CAIM) daughtercard, use the **show pas caim** command in user EXEC and privileged EXEC mode.

```
show pas caim {rings | dma | coprocessor | stats | cnxt_table | page_table} element-number
```

Syntax Description		
rings <i>element-number</i>		Displays current content of the Direct Memory Access (DMA) ring buffer.
dma <i>element-number</i>		Displays registers of the Jupiter DMA controller.
coprocessor <i>element-number</i>		Displays registers of the Hifn 9711 compression coprocessor.
stats <i>element-number</i>		Displays statistics describing operation of the data compression Advanced Interface Module (AIM).
cnxt_table <i>element-number</i>		Displays the context of the specific data compression AIM element.
page_table <i>element-number</i>		Displays the page table for each CAIM element.

Command Modes	
	User EXEC Privileged EXEC

Command History	Release	Modification
	12.0(2)T	This command was introduced.

Usage Guidelines This command displays performance statistics that describe the operation of the CAIM. This command is primarily intended for engineering debug, but it can also be useful to Cisco support personnel and to Cisco customers in troubleshooting network problems. [Table 45](#) lists the output values for this command.

Table 45 *show pas caim Output Values and Descriptions*

Value	Description
uncomp paks in	Number of packets containing uncompressed data input to the CAIM for compression.
comp paks out	Number of packets containing uncompressed data that were successfully compressed.
comp paks in	Number of packets containing compressed data input to the CAIM for compression.
uncomp paks out	Number of packets containing compressed data that were successfully decompressed.

Table 45 *show pas caim Output Values and Descriptions (continued)*

Value	Description
uncomp bytes in / comp bytes out	Summarizes the compression performance of the CAIM. The “uncomp bytes in” statistic gives the total number of uncompressed bytes submitted to the CAIM for compression. The “Comp bytes out” statistic gives the resulting number of compressed bytes output by the CAIM. If one forms the ratio of “uncomp bytes in” to “comp bytes out”, one obtains the average compression ratio achieved by the CAIM.
comp bytes in / uncomp bytes out	Summarizes the decompression performance of the CAIM. The “comp bytes in” statistic gives the total number of compressed bytes submitted to the CAIM for decompression. The “uncomp bytes out” statistic gives the resulting number of uncompressed bytes output by the CAIM. The average decompression ratio achieved can be computed as the ratio of “uncomp bytes out” to “comp bytes in”. Note that each packet submitted for compression or decompression has a small header at the front which is always clear data and hence never compressed nor decompressed. The “comp bytes in / uncomp bytes out” and “uncomp bytes in / comp bytes out” statistics do not include this header.
uncomp paks/sec in	A time average of the number of packets per second containing uncompressed data submitted as input to the CAIM for compression. It is computed as the ratio of the “uncomp paks in” statistic to the “seconds since last clear” statistic.
comp paks/sec out	A time average of the number of packets per second containing uncompressed data which were successfully compressed by the CAIM. It is computed as the ratio of the “comp paks out” statistic to the “seconds since last clear” compressed by the CAIM. It is computed as the ratio of the “comp paks out” statistic to the “seconds since last clear” statistic.
comp paks/sec in	A time average of the number of packets per second containing compressed data submitted as input to the CAIM for decompression. It is computed as the ratio of the “comp paks in” statistic to the “seconds since last clear” statistic.

Table 45 *show pas caim Output Values and Descriptions (continued)*

Value	Description
uncomp paks/sec out	<p>A time average of the number of packets per second containing compressed data which were successfully decompressed by the CAIM. It is computed as the ratio of the “uncomp paks out” statistic to the “seconds since last clear” statistic.</p> <p>Note that the “uncomp paks/sec in”, “comp paks/sec out”, “comp paks/sec in”, and “uncomp paks/sec out” statistics are averages over the entire time since the last “clear count” command was issued. This means that as time progresses, these statistics become averages over an ever larger time interval. As time progresses, these statistics become ever less sensitive to current prevailing conditions. Note also that the “uncomp paks in”, “comp paks out”, “comp paks in”, and “uncomp paks out” statistics are 32-bit counters and can roll over from 0xffff ffff to 0. When they do so, the “uncomp paks/sec in”, “comp paks/sec out”, “comp paks/sec in”, and “uncomp paks/sec out” statistics can be rendered meaningless. It is therefore recommend that one issue a “clear count” command before sampling these statistics.</p>
uncomp bits/sec in	A time average of the number of bits per second of uncompressed data which were submitted to the CAIM for compression. It is computed as the ratio of the “uncomp bytes in” statistic, times 8, to the “seconds since last clear” statistic.
comp bits/sec out	A time average of the number of bits per second of uncompressed data which were successfully compressed by the CAIM. It is computed as the ratio of the “comp bytes out” statistic, times 8, to the “seconds since last clear” statistic.
comp bits/sec in	A time average of the number of bits per second of compressed data which were submitted to the CAIM for decompression. It is computed as the ratio of the “comp bytes in” statistic, times 8, to the “seconds since last clear” statistic.
uncomp bits/sec out	<p>A time average of the number of bits per second of compressed data which were successfully decompressed by the CAIM. It is computed as the ratio of the “uncomp bytes in” statistic, times 8, to the “seconds since last clear” statistic.</p> <p>Note again that these “bits/sec” statistics are time averages over the “seconds since last clear” statistics, and therefore become less and less sensitive to current conditions as time progresses. Also, these “bits/sec” statistics are computed from 32-bit counters, and when the counters roll over from the maximum 32-bit value to 0, the “bits/sec” statistics become inaccurate. It is again recommended that one issue the “clear count” command before sampling the “bits/sec” statistics.</p>

The remaining statistics summarize operational state and error conditions encountered by the CAIM, and have the following interpretations:

Table 45 *show pas caim Output Values and Descriptions (continued)*

Value	Description
holdq	Gives the number of packets occupying the “hold queue” of the CAIM. The hold queue is a holding area, or “overflow” area, for packets to be processed by the CAIM. Normally, the CAIM is fast enough that no overflow into the hold queue occurs, and so normally this statistic should show zero.
hw_enable	Flag indicating if the CAIM is disabled or not. Zero implies disabled; one implies enabled. The CAIM can become disabled if certain fatal hardware error conditions are detected. It can be reenabled by issuing the clear aim element-number command.
src_limited	Flag indicating if the CAIM is in “source limited” mode. In source limited mode, the CAIM can only process a single command at a time. In non source limited mode, the CAIM can process several commands at a time using a pipeline built into the 9711 coprocessor. Note that the normal mode of operation is “non-source limited”, and there is no command to place the CAIM in “source limited” mode. Hence, this statistic should always read zero.
num cnxts	Gives the number of “contexts” which are currently open on the CAIM. Each interface configured for compression opens two contexts, one for each direction of data transfer.
no data	Counts the number of times in which the CAIM performed either a compress or decompression operation, and the output data length was reported with a length of zero. In normal operation, this statistic should always read zero. A nonzero value is an indication of a malfunctioning CAIM.
drops	Counts the total number of times in which the CAIM was forced to drop a packet it was asked to compress or decompress. This can happen for a number of reasons, and the remaining statistics summarize these reasons. This statistic indicates that the CAIM is being overloaded with requests for compression/decompression.
nobuffers	Counts the total number of times the CAIM needed to allocate memory for buffers but could not obtain memory. The CAIM allocates memory for buffers for holding the results of compression or decompression operations. In normal operation, there is plenty of memory available for holding CAIM results. This statistic, if nonzero, indicates that there is a significant backup in memory, or perhaps a memory leak.
enc adj errs	Each packet compressed or decompressed involves an adjustment of the encapsulation of the packet between the LZS-DCP, FRF9, or MPPC encapsulation used to transport compressed packets to the standard encapsulation used to transport clear data. This statistic counts the number of times this encapsulation adjustment failed. In normal operation, this statistic should be zero. A nonzero value indicates that we are short in a specific memory resource referred to as “paktypes”, and that packets are being dropped because of this shortage.

Table 45 *show pas caim Output Values and Descriptions (continued)*

Value	Description
fallbacks	Number of times the data compression AIM card could not use its pre-allocated buffers to store compression results and had to “fallback” to using a common buffer pool.
no replace	Each time a compression or decompression operation is completed and the resultant data fill up a buffer, the CAIM software allocates a new buffer to replace the buffer filled. If no buffers are available, then the packet involved in this operation is dropped and the old buffer reused. This statistic thus represents the number of times such an allocation failure occurred. In normal operation there is plenty of memory available for these buffers. A nonzero value for this statistic is thus a serious indication of a memory leak or other backup in buffer usage somewhere in the system.
num seq errs	This statistic is incremented when the CAIM produces results in a different order than that in which the requests were submitted. Packets involved in such errors are dropped. A nonzero value in this statistic indicates a serious malfunction in the CAIM.
num desc errs	Incremented when the CAIM reports error in a compression or decompression operation. Such errors are most likely bus errors, and they indicate a serious malfunction in the CAIM.
cmds complete	Reports the number of compression/decompression commands completed. This statistic should steadily increase in normal operation (assuming that the CAIM is continuously being asked to perform compression or decompression). If this statistic is not steadily increasing or decreasing when a steady stream of compression/decompression is expected, this is an indication of a malfunctioning CAIM.
bad reqs	Reports the number of compression/decompression requests that the CAIM software determined it could not possibly handle. This occurs only if a severely scattered packet (with more than 64 “particles”, or separate buffers of data) is handed to the CAIM to compress or decompress. This statistic should not increment during normal operation. A nonzero value indicates a software bug.
dead cntxts	Number of times a packet was successfully compressed or decompressed, only to find that the software “context”, or stream sourcing the packet, was no longer around. In such a case the packet is dropped. This statistic can be incremented at times when a serial interface is administratively disabled. If the timing is right, the CAIM may be right in the middle of operating on a packet from that interface when the disable takes effect. When the CAIM operation completes, it finds that the interface has been disabled and all “compression contexts” pertaining to that interface have been deleted. Another situation in which this can occur is when a Frame Relay DLC goes down. This is a normal and tolerable. If this statistic is incrementing when no such situations exist, it is an indication of a software bug.

Table 45 *show pas caim Output Values and Descriptions (continued)*

Value	Description
no paks	If a packet to be compressed or decompressed overflows into the hold queue, then it must undergo an operation called “reparenting”. This involves the allocation of a “paktype” structure for the packet. If no paktype structures are available, then the packet is dropped and this statistic is incremented. A nonzero value of this statistic indicates that the CAIM is being overtaxed, that is, it is being asked to compress/decompress at a rate exceeding its capabilities.
enq errors	Closely related to the “no paks” statistic. The hold queue for the CAIM is limited in length, and if the hold queue grows to this length, no further packets may be placed on it. A nonzero value of this statistic therefore also indicates that the CAIM is being overtaxed.
rx pkt drops	Contains the total number of packets dropped because of “no paks” or “enq errors”, which were destined to be decompressed.
tx pkt drops	Contains the total number of packets dropped because of “no paks” or “enq errors”, which were destined to be compressed
dequeues	Indicates the total number of packets which were removed from the CAIM hold queue when the CAIM became available for servicing its hold queue.
requeues	Indicates the total number of packets that were removed from the hold queue, only to find that the necessary CAIM resources were not available (it is not possible to determine whether CAIM resources are available until the packet is dequeued). Such packets are requeued onto the hold queue, with order in the queue preserved.
drops disabled	Indicates the total number of packets which were submitted for compression or decompression, but that were dropped because the CAIM was disabled.
clears	Indicates the number of times the CAIM was reset using the clear aim element-number command.
# ints	Indicates the number of interrupts serviced by the CAIM software. This statistic should steadily increase (assuming that the CAIM workload is steady). If this statistic is not incremented when expected, it indicates a severe CAIM malfunction.
# purges	Indicates the total number of times the compression history for a session had to be purged. This statistic is incremented a couple of times at startup. Thereafter, any increase in this statistic is an indication that the other side of the serial link detected bad data or gaps in the compressed packets being passed to it, and hence signalled a request to purge compression history in order to get back in synchronization. This can indicate that the CAIM is being overtaxed or that the serial interface is overtaxed and being forced to drop output packets.

Table 45 *show pas caim Output Values and Descriptions (continued)*

Value	Description
no cnxts	Indicates the total number of times a request was issued to open a context, but the CAIM could not support any more contexts. Recall that two contexts are required for each interface configured for compression.
bad algos	Indicates the total number of times a request was issued to open a context for a compression algorithm not supported by the CAIM. Recall that the CAIM supports the LZS and MPPC algorithms only.
no crams	Indicates the total number of times a request was issued to open a context but there was insufficient compression DRAM to open another context. The CAIM software is set up to run out of contexts before it runs out of compression DRAM, so this statistic should always be zero.
bad paks	Indicates the total number of times a packet was submitted for compression or decompression to the CAIM, but the packet had an invalid size.
# opens	Indicates the total number of times a context was opened.
# closes	Indicates the total number of times a context was closed.
# hangs	Indicates the total number of times a CAIM appeared hung up, necessitating a clear of the CAIM.

Examples

The `show pas caim rings element-number` command displays the current state of the DMA ring buffers maintained by the CAIM software. These rings feed the CAIM with data and commands. It is intended for an engineering debug of the compression AIM. It produces the following output:

```
Router# show pas caim rings 0

CAIM Command Ring: 0x01A2BC00 Stack: 0x01A2BE40 Shadow: 0x80F88BAC
  Head: 0021 Tail: 0021 Count: 0000
CAIM Source Ring: 0x01A2C900 Shadow: 0x80F88BAC
  Head: 0021 Tail: 0021 Num: 0000
CAIM Results Ring: 0x01A2C280 Stack: 0x01A2C4C0
  Head=021 Tail=021
CAIM Dest Ring: 0x01A2CB40 Shadow: 0x80F892D8 Head=021 Tail=000
  Desc: 0x01A2CBE8 flags: 0x8000060C dptr: 0x019E7EB8 part: 0x80F84BE0
  Desc: 0x01A2CBF0 flags: 0x8000060C dptr: 0x019FC63C part: 0x80F85240
----cut----
```

Table 46 describes the fields shown in the display.

Table 46 *show pas caim rings Field Descriptions*

Field	Description
CAIM Command Ring	Feeds commands to the CAIM.
command ring address	Address of the command ring.
Command Ring Stack	Ring that feeds additional commands to the CAIM.
command ring stack address	Address of the command ring stack.

Table 46 *show pas caim rings Field Descriptions (continued)*

Field	Description
Command Ring Shadow	Software ring that stores additional information about each command.
command ring shadow address	Address of the command ring shadow.
Command Ring Head	Index into the Source Ring, specifying where the next entry will be extracted from.
Command Ring Tail	Index into the Source Ring, specifying where the next entry will be inserted.
CAIM Source Ring	Feeds information about input data to the CAIM.
source ring address	Address of the source ring.
Source Ring Shadow	Ring that contains additional information about each source buffer.
source ring shadow address	Address of the source ring shadow.
Source Ring Head	Specifies where the next entry will be extracted from.
Source Ring Tail	Specifies where the next entry will be inserted.
CAIM Results Ring	Receives information about each CAIM command as it is completed.
results ring address	Address of the results ring.
Results Ring Stack	Ring that receives additional information about each completed command.
results ring stack address	Address of the results ring stack.
Results Ring Head	Specifies where the next entry will be extracted from.
Results Ring Tail	Specifies where the next entry will be inserted.
CAIM Dest Ring	Holds information about the buffers available to the CAIM for output data.
dest ring address	Address of the dest ring.
Dest Ring Shadow	Ring that holds additional information about each output buffer.
dest ring shadow address	Address of the dest ring shadow.
Dest Ring Head	Index into the Source Ring, specifying where the next entry will be extracted from.
Dest Ring Tail	Index into the Source Ring, specifying where the next entry will be inserted.
The remaining fields describe each output data buffer.	
dest	Address of a so-called descriptor, used by the Jupiter DMA engine.
flags	Contains flags describing attributes of the buffer.
dptr	Displays the actual address of the output buffer.
part	Displays the address of the corresponding particle type structure, a software-defined structure that describes a buffer when it is a component of a network data buffer.

The **show pas caim dma *element-number*** command displays the registers of the Jupiter DMA Controller. These registers control the operation of the Jupiter DMA Controller. This command is intended for Engineering debug of the CAIM. You can find detailed descriptions of the various fields in the Jupiter DMA Controller specification. It produces the following output:

```
Router# show pas caim dma 0

Jupiter DMA Controller Registers: (0x40200000
  Cmd Ring: 0x01A2BCA8  Src Ring: 0x01A2C9A8
  Res Ring: 0x01A2C328  Dst Ring: 0x01A2CBE8
  Status/Cntl: present: 0x80808084  last int: 0x80808084
  Inten: 0x10100000  config: 0x00100003
  Num DMA ints: 143330469
```

The **show pas caim compressor *element-number*** command displays the registers of the Hifn 9711 compression coprocessor. These registers control the operation of the Hifn 9711 part. This command is intended for engineering to debug the CAIM. Detailed descriptions of the various fields may be found in the Hifn 9711 data book. It produces the following output:

```
Router# show pas caim compressor 0

Hifn9711 Data Compression Coprocessor Registers (0x40201000):
  Config: 0x000051D4  Inten: 0x00000E00
  Status: 0x00004000  FIFO status: 0x00004000
  FIFO config: 0x00000101
```

[Table 47](#) describes the fields shown in the preceding display.

Table 47 *show pas caim compressor Field Descriptions*

Field	Description
Hifn9711 Data Compression Coprocessor Registers	Controls the operation of the Hifn 9711 part.
registers address	Address of the registers in the address space of the processor.
Config	Displays the current contents of the 9711 configuration register.
Inten	Displays the contents of the 9711 interrupt enable register.
Status	Displays the contents of the 9711 status register.
FIFO status	Contents of the 9711 FIFO Status register.
FIFO config	Contents of the 9711 FIFO Config register.

The **show pas caim cnxt_table *element-number*** form of this command displays the context table for the specified CAIM element. The context table is a table of information concerning each compression context. It produces the following output:

```
Router# show pas caim scnxt_table 0

CAIM0 Context Table
Context: 0x8104F320  Type: Compr  Algo: Stac
  Hdrlen: 0006  History: 0x0000
  Callback: 0x8011D68C  Shutdown: x8011EBE4  Purge: N
  Comp_db: 0x81034BC0  idb: 0x81038084  ds: 0x8104E514
Context: 0x8104F340  Type: Decompr Algo: Stac
  Hdrlen: 0002  History: 0x0000
  Callback: 0x8011E700  Shutdown: x8011EBE4  Purge: N
  Comp_db: 0x81034BC0  idb: 0x81038084  ds: 0x8104E514
```

Table 48 describes the fields shown in the preceding display.

Table 48 *show pas caim cnxt-table Fields Descriptions*

Field	Description
Context	Numeric internal reference for the compression context.
Type	Gives the type of context: <ul style="list-style-type: none"> • Compr—compression context • Decomp—decompression context
Algo	Gives the compression algorithm used: <ul style="list-style-type: none"> • Stac • Mppc
Hdrlen	Gives the number of bytes in the compression header for each compressed packet.
History	Gives the 16-KB page number in compression RAM for the context.
Callback	Gives an internal numeric reference for a control structures or procedure to facilitate debugging.
Shutdown	Gives an internal numeric reference for a control structures or procedure to facilitate debugging.
Comp_db	Gives an internal numeric reference for a control structures or procedure to facilitate debugging.
idb	Gives an internal numeric reference for a control structures or procedure to facilitate debugging.
idb	Gives an internal numeric reference for a control structures or procedure to facilitate debugging.
Purge	Indicates whether the compression context has been flagged to have its history purged.

The **show pas caim page_table** *element-number* command displays the page table for the selected CAIM element. The page table is a table of entries describing each page in compression RAM. It produces the following output:

```
Router# show pas caim page_table 0

CAIM0 Page Table
  Page 0x0000 Comp cnxt: 8104F320 Decmp cnxt: 8104F340 Algo: Stac
```

Table 49 describes the fields shown in the preceding display.

Table 49 *show pas caim page_table Field Descriptions*

Field	Description
Page	16 Kbyte page number of the page.
Comp cnxt	Contains an internal numeric reference to the context structures using this page.

Table 49 *show pas caim page_table* Field Descriptions

Field	Description
Decmp cnxt	Contains an internal numeric reference to the context structures using this page.
Algo	Gives the compression algorithm used: <ul style="list-style-type: none"> • Stac • Mppc

The following example shows statistics of an active data compression AIM session:

```
Router# show pas caim stats 0
```

```
CompressionAim0
  ds:0x80F56A44 idb:0x80F50DB8
    422074 uncomp paks in -->      422076 comp paks out
    422071 comp paks in  -->      422075 uncomp paks out
  633912308 uncomp bytes in-->    22791798 comp bytes out
  27433911 comp bytes in  -->    633911762 uncomp bytes out
    974 uncomp paks/sec in-->     974 comp paks/sec out
    974 comp paks/sec in  -->     974 uncomp paks/sec out
  11739116 uncomp bits/sec in-->  422070 comp bits/sec out
    508035 comp bits/sec in -->  11739106 uncomp bits/sec out
  433 seconds since last clear
  holdq: 0 hw_enable: 1 src_limited: 0 num cnxts: 4
  no data: 0 drops: 0 nobuffers: 0 enc adj errs: 0 fallbacks: 0
  no Replace: 0 num seq errs: 0 num desc errs: 0 cmds complete: 844151
  Bad reqs: 0 Dead cnxts: 0 No Paks: 0 enq errs: 0
  rx pkt drops: 0 tx pkt drops: 0 dequeues: 0 requeues: 0
  drops disabled: 0 clears: 0 ints: 844314 purges: 0
  no cnxts: 0 bad algos: 0 no crams: 0 bad paks: 0
  # opens: 0 # closes: 0 # hangs: 0
```

Related Commands

Command	Description
show compress	Displays compression statistics.

show pas eswitch address

To display the Layer 2 learned addresses for an interface, use the **show pas eswitch address** command in user EXEC and privileged EXEC mode.

```
show pas eswitch address [ethernet | fastethernet] [slot/port]
```

Syntax Description	ethernet fastethernet	(Optional) Type of interface.
	<i>slot</i>	(Optional) Slot number of the interface.
	<i>port</i>	(Optional) Interface number.

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

Command History	Release	Modification
	11.2 P	This command was introduced.

Examples

The following sample output shows that the first PA-12E/2FE interface (listed below as port 0) in port adapter slot 3 has learned the Layer 2 address 00e0.f7a4.5100 for bridge group 30 (listed below as BG 30):

```
Router# show pas eswitch address fastethernet 3/0
U 00e0.f7a4.5100, AgeTs 56273 s, BG 30 (vLAN 0), Port 0
```

show pas isa controller

To show controller information that is specific to the Virtual Private Network (VPN) accelerator controller when an Integrated Services Adapter (ISA) is installed, use the **show pas isa controller EXEC** command.

show pas isa controller

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Examples The following is sample output from the **show pas isa controller** command:

```
Router# show pas isa controller

Interface ISA5/1 :

Encryption Mode = IPSec

Addresses of Rings and instance structure:
High Priority Rings
  TX: 0x4B0E97C0 TX Shadow:0x62060E00
  RX: 0x4B0EB840 RX Pool:0x4B0EBC80 RX Pool Shadow:0x62068E58
Low Priority Rings
  TX: 0x4B0EA800 TX Shadow:0x62066E2C
  RX: 0x4B0EC0C0, RX Shadow:0x62069284

Instance Structure address:0x620603D8

Firmware write head/tail offset:0x4B0EC900
Firmware read head/tail offset:0x3EA00000
```

Related Commands	Command	Description
	show pas isa interface	Displays interface status information that is specific to the VPN accelerator card.

show pas isa interface

To display interface information that is specific to the Virtual Private Network (VPN) accelerator card when an Integrated Services Adapter (ISA) is installed, use the **show pas isa interface** command in privileged EXEC mode.

show pas isa interface

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.

Examples

The following is sample output from the **show pas isa interface** command:

```
Router# show pas isa interface

Interface ISA5/1 :
  Statistics of packets and bytes through this interface:
    2876894 packets in           2910021 packets out
      420 paks/sec in             415 paks/sec out
    2327 Kbits/sec in           2408 Kbits/sec out
      632 commands out           632 commands acknowledged
  low_pri_pkts_sent      1911   low_pri_pkts_rcvd:      1911
  invalid_sa:            260     invalid_flow:          33127
  invalid_dh:             0      ah_seq_failure:        0
  ah_spi_failure:         0      esp_auth_failure:     0
  esp_seq_failure:        0      esp_spi_failure:       0
  esp_protocol_absent:    0      ah_protocol_absent:   0
  bad_key_group:          0      no_shared_secret:     0
  no_skeyids:             0      pad_size_error:        0
  cmd_ring_full:          0      bulk_ring_full:        990
  bad_peer_pub_len:       0      authentication_failure: 0
  fallback:               1606642 no_particle:           0
  6922 seconds since last clear of counters
```

[Table 50](#) describes the significant fields shown in the display.

Table 50 *show pas isa interface Field Descriptions*

Field	Description
packets in/out	Number of data packets received from, or sent to, the Integrated Service Adapter (ISA).
paks/sec in/out	Number of packets received in, or sent out, with the total number of seconds that the ISA is active.
Kbits/sec in/out	Number of kilobits (Kbits) received in, or sent out, with the total number of seconds that the ISA is active.

Table 50 *show pas isa interface Field Descriptions (continued)*

Field	Description
commands out	Number of commands going to the ISA. Examples of commands include setting up encryption sessions and retrieving statistics or status from the ISA.
commands acknowledged	Number of commands returning from the ISA. Examples of commands include setting up encryption sessions and retrieving statistics or status from the ISA.
low_pri_pkts_sent	This is a summary counter for number of Internet Key Exchange (IKE) and IPsec commands submitted to ISA.
low_pri_pkts_rcvd	This is a summary counter for number of IKE & IPSEC command responses received from ISA.
invalid_sa	Reference to an unusable security association key pair.
invalid_flow	An invalid packet using an IPsec key is received for encryption or decryption. Example: session has expired.
invalid_dh	Reference to an unusable Diffie-Hellman(DH) key pair.
ah_seq_failure	Unacceptably late Authentication Header (AH) header received.
ah_spi_failure	SPI specified in the AH header does not match the SPI associated with the IPsec AH key.
esp_auth_failure	Number of ESP packets received with authentication failures.
esp_seq_failure	Unacceptably late ESP packet received.
esp_spi_failure	SPI specified in the ESP header does not match the SPI associated with the IPsec ESP key.
esp_protocol_absent	Packet is missing expected ESP header.
ah_protocol_absent	Packet is missing expected AH header.
bad_key_group	Unsupported key group requested during a Diffie-Hellman generation.
no_shared_secret	Attempting to use a Diffie-Hellman shared secret that is not generated.
no_keyids	Attempting to use a shared secret that is not generated.
pad_size_error	The length of the ESP padding is greater than the length of the entire packet.
cmd_ring_full	New IKE setup messages are not queued for processing until the previous queued requests are processed.
bulk_ring_full	New packets requiring IPsec functionality are not queued to the ISA until the ISA completes the processing of existing requests.
bad_peer_pub_len	Length of peer's DH public key does not match the length specified for the negotiated DH key group.
authentication_failure	Authentication failed.

Table 50 *show pas isa interface Field Descriptions (continued)*

Field	Description
fallback	The number of instances when the driver is successful in getting a replacement buffer from the global pool.
no_particle	The number of instances when the driver was unable to get a replacement buffer from the driver pool and the global (fallback) pool.

Related Commands

Command	Description
show pas isa controller	Displays controller status information that is specific to the VPN accelerator card.

show pas vam controller

To display controller information that is specific to the VPN Acceleration Module (VAM), use the **show pas vam controller** command in privileged EXEC mode.

show pas vam controller

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(9)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples The following is sample output from the **show pas vam controller** command:

```
Router# show pas vam controller

Encryption Mode = IPSec

Addresses of Rings and instance structure:
Low Priority Queue:
  OMQ=0xF2CB2E0, OMQ Shadow = 0x630E6638, {1, 1, 0, 256}
  PKQ=0xF2CF320, PKQ Shadow = 0x630EBE64, {232, 232, 0, 256}
  ERQ=0xF2D3360, ERQ Shadow = 0x630F1690, {0, 0, 0, 256}
High Priority Rings:
  TX: 0x0F2D73A0 TX Shadow:0x630F6EBC, {6, 6, queued=0}
  RX: 0x7F2D93E0 {13, 0, 256}
  RX Pool:0x7F2DA420 RX Pool Shadow:0x630FCAB8, {6, 0, 255}
Instance Structure address:0x630E5898

Misc registers:
mini-omq=0xF2DB460, shdw=0x63102714
Group0=0x3D800000, Group1=0x3D801000
IndexReg = 0xDFFE700
Heartbeat info:<Addr, Value> = <0xF2DB520, 0x2A55A>
Running default HSP (addr=0x629D36AC, size=294268)
```

Related Commands	Command	Description
	show pas vam interface	Displays interface status information specific to the VPN accelerator module.

show pas vam interface

To display interface information that is specific to the VPN Acceleration Module (VAM), use the **show pas vam interface** command in privileged EXEC mode.

show pas vam interface

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(9)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines Enter the **show pas vam interface** command to see if the VAM is currently processing crypto packets.

Examples The following is sample output from the **show pas vam interface** command:

```
Router# show pas vam interface

Interface VAM 2/1 :
  ds: 0x621CE0D8      idb:0x621C28DC
  Statistics of packets and bytes that through this interface:
    1110 packets in          1110 packets out
    123387 bytes in         100979 bytes out
    0 paks/sec in           0 paks/sec out
    0 Kbits/sec in          0 Kbits/sec out
    3507 commands out       3507 commands acknowledged
  ppq_full_err   : 0      ppq_rx_err     : 0
  cmdq_full_err  : 0      cmdq_rx_err    : 0
  no_buffer      : 0      fallback      : 0
  dst_overflow   : 0      nr_overflow    : 0
  sess_expired   : 0      pkt_fragmented : 0
  out_of_mem     : 0      access_denied  : 0
  invalid_fc     : 0      invalid_param  : 0
  invalid_handle : 0      output_overrun : 0
  input_underrun : 0      input_overrun  : 0
  key_invalid    : 0      packet_invalid : 0
  decrypt_failed : 0      verify_failed  : 0
  attr_invalid   : 0      attr_val_invalid : 0
  attr_missing   : 0      obj_not_wrap   : 0
  bad_imp_hash   : 0      cant_fragment  : 0
  out_of_handles : 0      compr_cancelled : 0
  rng_st_fail    : 0      other_errors   : 0
  3420 seconds since last clear of counters
```

Table 51 describes the significant fields shown in the display.

Table 51 *show pas vam interface Field Descriptions*

Field	Description
packets in/out	Number of data packets received from, or sent to, the VAM.
bytes in/out	Number of data bytes received from, or sent to, the VAM.
paks/sec in/out	Number of packets received in, or sent out, with the total number of seconds that the VAM is active.
Kbits/sec in/out	Number of kilobits (Kbits) received in, or sent out, with the total number of seconds that the VAM is active.
commands out	Number of commands going to the VAM. Examples of commands include setting up encryption sessions and retrieving statistics or status from the VAM.
commands acknowledged	Number of commands returning from the VAM. Examples of commands include setting up encryption sessions and retrieving statistics or status from the VAM.
ppq_full_err	Number of packets dropped because of a lack of space in the packet processing queues for the VAM. This usually means that input traffic has reached VAM maximum throughput possible.
ppq_rx_err	Summary counter for all errors related to packet processing.
cmdq_full_err	Number of commands dropped because of a lack of space in the command processing queues for the VAM. This error indicates that the input tunnel setup rate has reached the VAM maximum setup rate. The Internet Key Exchange (IKE) process retries the tunnel creation and deletion when commands are dropped by VAM.
cmdq_rx_err	Summary counter for all errors related to command processing (for example, IKE, or IPSec session creation or deletion).
no_buffer	Errors related to the VAM running out of buffers. May occur with large packets. Although VAM buffers cannot be tuned, try tuning buffers for other interfaces.
fallback	Internal VAM buffer pool is completely used up and VAM has to fallback to global buffer pool. This may cause minor performance impact, however, packets are still processed so this error can be ignored.
dst_overflow	Counter that is incremented when the VAM has completed an operation, but there is no available space into which to place the result.

Table 51 *show pas vam interface Field Descriptions (continued)*

Field	Description
nr_overflow	Counter that is incremented when the VAM has completed an operation, but there is no available space into which to place the result.
sess_expired	Counter that is incremented if the session used to encrypt or decrypt the packet has expired because of time or space limit.
pkt_fragmented	Counter that is incremented when the input packet has to be fragmented after encryption. This counter should always be 0 as fragmentation by VAM is disabled.
out_of_mem	Counter that is incremented when the VAM runs out of memory.
access_denied	Counter that is incremented when the VAM is requested to perform an operation on an object that can not be modified.
invalid_fc	Counter that is incremented when the VAM has received a request that is illegal for the specified object type.
invalid_param	Counter that is incremented when the VAM has received invalid parameters within a command.
invalid_handle	Counter that is incremented when the VAM receives a request for an operation to be performed on an object that does not exist.
output_overrun	Counter that is incremented when the space allocated for a response is not large enough to hold the result posted by the VAM.
input_underrun	Counter that is incremented when the VAM receives a packet for which it finds a premature end to the data, for example, a truncated packet.
input_overrun	Counter that is incremented when the VAM receives a buffer that is too large for the requested operation.
key_invalid	Counter that is incremented when the VAM receives a request for an operation on a key where the key is invalid or of the wrong type.
packet_invalid	Counter that is incremented when the VAM receives a packet whose body is badly formed.
decrypt_failed	Counter that is incremented when the VAM receives a packet that cannot be decrypted because the decrypted data was not properly formatted (for example, padding is wrong).
verify_failed	Counter that is incremented when the VAM receives a packet which could not be verified because the verification of a signature or authentication value failed.

Table 51 *show pas vam interface Field Descriptions (continued)*

Field	Description
attr_invalid	Counter that is incremented when the VAM receives a packet which specifies an attribute that is not correct for the specified object or operation.
attr_val_invalid	Counter that is incremented when the VAM encounters errors during packet or command processing. The packets or commands are dropped in such cases.
attr_missing	Counter that is incremented when the VAM receives an operation request for which the value of a required attribute is missing.
obj_not_wrap	Counter that is incremented when the VAM receives an operation request to retrieve an object that is hidden or unavailable for export beyond the FIPS boundary of the VPN Module.
bad_imp_hash	Counter that is incremented when the VAM sees a hash miscompare on unwrap.
cant_fragment	Counter that is incremented when the VAM determines a need to fragment a packet, but cannot fragment because the “don’t fragment” bit is set. This counter should always be zero because the fragmentation on the VAM is disabled.
out_of_handles	Counter that is incremented when the VAM has run out of available space for objects of the requested type.
comp_cancelled	<p>Due to the operation of the compression algorithm, some data patterns cannot be compressed. Usually data that has already been compressed or data that does not have a sufficient number of repetitive patterns cannot be compressed and a compress operation would actually result in expansion of the data.</p> <p>There are certain known data patterns which do not compress. In these cases, the compression engine cancels the compression of the data and returns the original, uncompressed data without an IPPCP header.</p> <p>These counters are useful to determine if the content of the traffic on the network is actually benefiting from compression. If a large percentage of the network traffic is already compressed files, these counters may indicate that compression on these streams are not improving the performance of the network.</p>
rng_st_fail	Counter that is incremented when the VAM detects a Random Number Generator self test failure.

Table 51 *show pas vam interface Field Descriptions (continued)*

Field	Description
pkt_replay_err	Counter that is incremented when a replay error is detected by the VAM.
other_errors	Counter that is incremented when the VAM encounters a packet or command error that is not listed in other error categories. An example could be if the packet IP header checksum is incorrect.

Related Commands

Command	Description
show pas vam controller	Displays controller status information that is specific to the VPN accelerator module.

show pci aim

To show the IDPROM contents for each compression Advanced Interface Module (AIM) daughtercard in the Cisco 2600 router, use the **show pic aim** command in user EXEC and privileged EXEC mode.

```
show pci aim
```

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.0(1)T	This command was introduced.

Usage Guidelines This command shows the IDPROM contents for each compression AIM daughtercard present in the system, by AIM slot number (currently 0, since that is the only daughtercard installed for Cisco IOS Release 12.0(1)T). The IDPROM is a small PROM built into the AIM board used to identify it to the system. It is sometimes referred to as an EEPROM because it is implemented using electronically erasable PROM.

Examples The following example shows the IDPROM output for the installed compression AIM daughtercard:

```
Router# show pic aim 0

AIM Slot 0: ID 0x012D
  Hardware Revision      : 1.0
  EEPROM format version 4
  EEPROM contents (hex):
    0x00: 04 FF 40 01 2D 41 01 00 FF FF FF FF FF FF FF FF
    0x10: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    0x20: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Related Commands	Command	Description
	clear aim	Clears data compression AIM registers and resets the hardware.
	test aim eeprom	Tests the data compression AIM after it is installed in a Cisco 2600 series router.

show power inline

To display the power status for a specified port or for all ports, use the **show power inline** command in privileged EXEC mode.

```
show power inline [interface-id] [actual | configured]
```

Syntax Description	
<i>interface-id</i>	(Optional) ID of the module and port number.
actual	(Optional) Displays the present power status, which might not be the same as the configured power.
configured	(Optional) Displays the configured power status.

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

Command History	Release	Modification
	12.0(5)XU	This command was introduced.
	12.2(2)XT	This command was introduced on the Cisco 2600 series, the Cisco 3600 series, and the Cisco 3700 series routers to support switchport creation.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation on Cisco 2600 series, the Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines	The show power inline command displays the amount of power used to operate a Cisco IP phone. To view the amount of power requested, use the show cdp neighbors command.
------------------	---

Examples	The following is sample output from the show power inline fa0/4 actual command asking for the actual status of each interface rather than what is configured for each:
----------	---

```
Router# show power inline fastethernet 0/4 actual
```

```
Interface          Power
-----
FastEthernet0/4    no
```

Notice that the status shown for the FastEthernet interface 0/4, there is no power.

Related Commands	Command	Description
	power inline	Determines how inline power is applied to devices on the specified Fast Ethernet port.
	show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.

show smf

To display the configured software MAC address filter (SMF) on various interfaces of a router, use the **show smf** command in user EXEC and privileged EXEC mode.

```
show smf [interface-name]
```

Syntax Description

<i>interface-name</i>	(Optional) Displays information about the specified interface. Choices can include atm, ethernet, fastethernet, null, serial, tokenring, and async.
-----------------------	---

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced in a release prior to 10.0.

Usage Guidelines

The SMF is active whenever the router is doing bridging or Integrated Routing and Bridging (IRB). MAC address filtering can be used as a security feature in bridging or switching environments.

Examples

The following is sample output from the **show smf** command:

```
R2-81-7206#sh smf

Software MAC address filter on FastEthernet0/0.2
Hash Len   Address           Matches Act   Type
0x00:  0 ffff.ffff.ffff      0 RCV Physical broadcast
0x0C:  0 0100.0c00.0000      0 RCV ISL vLAN Multicast
0x2A:  0 0900.2b01.0001      0 RCV DEC spanning tree
0xA6:  0 0010.a6ae.6000      0 RCV Interface MAC address
0xC1:  0 0100.0ccc.cccd      0 RCV SSTP MAC address
0xC2:  0 0180.c200.0000      0 RCV IEEE spanning tree
0xC2:  1 0180.c200.0000      0 RCV IBM spanning tree
0xC2:  2 0100.0ccd.cdce      0 RCV VLAN Bridge STP
```

N

[Table 52](#) describes the fields shown in the display.

Table 52 *show smf* Field Descriptions

Field	Description
Hash	Position in the hash table for this entry.
Len	Length of the entry.
Address	MAC address for the interface.
Matches	Number of hits for the address.

Table 52 *show smf Field Descriptions (continued)*

Field	Description
Act	Action taken. Values can be receive (RCV), forward (FWD), or discard (DIS).
Type	Type of MAC address.

show storm-control

To view switchport characteristics, including storm-control levels set on the interface, use the **show storm-control** command in privileged EXEC mode.

show storm-control

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(2)XT	This command was introduced.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Examples The following example shows how to verify the storm-control levels set on the interface:

```
Router# show storm-control
```

```
Storm control:broadcast multicast unicast threshold 25 with default packet-size 64
```

Notice that the display showing status of storm control includes the default packet size and the threshold level which limits the percentage of bandwidth placed on broadcast traffic. A threshold value of 100 percent means that no limit is placed on broadcast traffic. Valid entries are from 1 to 100. If no threshold is reported for each, then no threshold is set for that type of traffic.

Related Commands	Command	Description
	show interface counters	Displays the count of discarded packets.
	storm control	Sets the storm-control threshold value and blocks forwarding of unnecessary flooded traffic.

show tdm backplane

To display modem and PRI channel assignments with streams and channels on the modem side as assigned to the unit and channels on the PRI side of the time-division multiplexing (TDM) assignment, use the **show tdm backplane** command in privileged EXEC mode.

show tdm backplane stream *stream-number*

Syntax Description	stream	Backplane stream in the range 0 to 7. There are 8 backplane “streams” on the TDM backplane for the Cisco AS5300 access server. Each stream runs at 2 MHz and has 32 channels (running at 64 Hz) on the Cisco AS5300 access server backplane hardware.
	<i>stream-number</i>	Actual number entered (either 0 to 7 or 0 to 15). An actual number needs to be entered.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(2)XD	This command was introduced.
	12.0(3)T	This command was incorporated into Cisco IOS Release 12.0(3)T.

Usage Guidelines The **show tdm backplane** command shows the status of the TDM backplane, related data structure values, and TDM chip memory settings. This command is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

Examples The following example shows the general syntax used, and the output displayed for the **show tdm backplane** command. To display only a subset of the data on most of the commands, further specify particular slots, streams, and devices. When the **debug tdm detail** command is executed, more detail is shown. The following examples are run with the **debug tdm detail** command executed:

```
5300# show tdm backplane

Show BackPlane Connections
TDM Backplane Connection for Stream 0
  Modem (St/Ch)<->PRI (Unit/Ch)  xx/xx:Not Used ??/?:Unknown State
0  :  xx/xx<->xx/xx,  xx/xx<->xx/xx,  00/02<->00/30,  00/03<->03/10
4  :  00/04<->00/15,  00/05<->02/02,  00/06<->02/07,  00/07<->02/08
8  :  xx/xx<->xx/xx,  00/09<->03/11,  00/10<->02/09,  xx/xx<->xx/xx
12 :  00/12<->00/17,  00/13<->02/17,  00/14<->02/18,  00/15<->02/10
16 :  xx/xx<->xx/xx,  xx/xx<->xx/xx,  00/18<->00/19,  00/19<->02/19
20 :  00/20<->02/11,  xx/xx<->xx/xx,  xx/xx<->xx/xx,  00/23<->00/07
24 :  xx/xx<->xx/xx,  00/25<->00/01,  00/26<->00/20,  00/27<->02/20
28 :  xx/xx<->xx/xx,  00/29<->00/18,  xx/xx<->xx/xx,  xx/xx<->xx/xx

TDM Backplane Connection for Stream 1
  Modem (St/Ch)<->PRI (Unit/Ch)  xx/xx:Not Used ??/?:Unknown State
0  :  xx/xx<->xx/xx,  xx/xx<->xx/xx,  xx/xx<->xx/xx,  01/03<->03/09
```

show tdm backplane

```

4 : 01/04<->00/03, 01/05<->02/13, xx/xx<->xx/xx, xx/xx<->xx/xx
8 : xx/xx<->xx/xx, xx/xx<->xx/xx, 01/10<->02/14, 01/11<->00/04
12 : 01/12<->00/21, xx/xx<->xx/xx, 01/14<->00/05, xx/xx<->xx/xx
16 : xx/xx<->xx/xx, xx/xx<->xx/xx, xx/xx<->xx/xx, 01/08<->02/12
20 : 01/20<->00/06, 01/09<->00/02, xx/xx<->xx/xx, xx/xx<->xx/xx
24 : 01/24<->03/01, xx/xx<->xx/xx, 01/26<->02/15, xx/xx<->xx/xx
28 : 01/28<->03/05, xx/xx<->xx/xx, xx/xx<->xx/xx, xx/xx<->xx/xx
...

```

Related Commands

Command	Description
show tdm connections	Displays details about a specific TDM channel programmed on the Mitel chip.
show tdm data	Displays information about TDM bus connection memory on Cisco access servers.
show tdm detail	Displays information about the specified TDM device.
show tdm information	Displays TDM resources available for the specified TDM device.
show tdm pool	Displays information about the specified TDM pool.

show tdm connections

To display a snapshot of the time-division multiplexing (TDM) bus connection memory in a Cisco AS5200 access server or to display information about the connection memory programmed on the Mitel TDM chip in a Cisco AS5800 access server, use the **show tdm connections** command in privileged EXEC mode.

Cisco AS5200 Access Server

```
show tdm connections [motherboard | slot slot-number]
```

Cisco AS5800 Access Server

```
show tdm connections {motherboard {stream stream-number} | slot slot-number {device device-number {stream stream-number}}}
```

Syntax Description	
motherboard	<p>Cisco AS5200 Access Server</p> <p>(Optional) Motherboard in the Cisco AS5200 access server.</p> <p>Cisco AS5800 Access Server</p> <p>Motherboard in the Cisco AS5800 access server has ethernet and serial interfaces, console port, and aux port. The motherboard has one TDM device (MT8980) for the Cisco 5300 access server.</p>
slot slot-number	<p>Cisco AS5200 Access Server</p> <p>(Optional) Number of the slot being configured.</p> <p>Cisco AS5800 Access Server</p> <p>There are 3 slots on the Cisco AS5800 access server. The range of the slots is 0 to 2. A modem card or a trunk PRI card can be inserted into each slot. Each card in the slot has one or two TDM devices (either MT8980 or MT90820) on them.</p>
stream	<p>Device stream in the range 0 to 7. There are 8 backplane “streams” on the TDM backplane for the Cisco AS5800 access server. Each stream runs at 2 Mhz and has 32 channels (running at 64 Hz) on the Cisco AS5800 access server backplane hardware.</p>
stream-number	<p>Stream number (the range is 0 to 7 or 0 to 15).</p>
device	<p>TDM device on the motherboard or slot cards. The range for the Cisco AS5800 access server is 0 to 1. Each card has at least one TDM device (MT8980 or MT80920), and some of the slot cards have two devices (for example, the Octal PRI has two MT90820 TDM devices). The TDM device is also referred to as “TSI Chip Number” in the online help.</p>
device-number	<p>Valid range is 0 to 1.</p>

Command Modes Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(3)T	This command was modified to include support for the Cisco AS5800 access server.

Usage Guidelines**Cisco AS5200 Access Server**

The **show tdm connections** command shows the connection memory for all TDM bus connections in the access server if you do not limit the display to the motherboard or a slot.

Cisco AS5800 Access Server

The **show tdm connections** command shows the status of the TDM chip memory settings. This command is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

Examples**Cisco AS5200 Access Server**

The following example shows source stream 3 (ST3) channel 2 switched out of stream 6 (ST6) channel 2:

```
AS5200# show tdm connections motherboard
```

```
MT8980 motherboard unit 0, Control Register = 0x1F, ODE Register = 0x06
Connection Memory for ST6:
Ch0: 0x62, Ch1: 0x00, Ch2: 0x00, Ch3: 0x00
Ch4: 0x00, Ch5: 0x00, Ch6: 0x00, Ch7: 0x00
Ch8: 0x00, Ch9: 0x00, Ch10: 0x00, Ch11: 0x00
Ch12: 0x00, Ch13: 0x00, Ch14: 0x00, Ch15: 0x00
Ch16: 0x00, Ch17: 0x00, Ch18: 0x00, Ch19: 0x00
Ch20: 0x00, Ch21: 0x00, Ch22: 0x00, Ch23: 0x00
Ch24: 0x00, Ch25: 0x00, Ch26: 0x00, Ch27: 0x00
Ch28: 0x00, Ch29: 0x00, Ch30: 0x00, Ch31: 0x00
```

To interpret the hexadecimal number 0x62 into meaningful information, you must translate it into binary code. These two hexadecimal numbers represent a connection from any stream and a channel on any stream. The number 6 translates into the binary code 0110, which represents the third-source stream. The number 2 translates into the binary code 0010, which represents the second-source channel.

Stream 6 (ST6) channel 0 is the destination for source stream 3 (ST3) channel 2 in this example.

Cisco AS5800 Access Server

The following example shows the general syntax used and the output displayed for the **show tdm connections** command. To display only a subset of the data on most of the commands, further specify particular slots, streams, and devices. When the **debug tdm detail** command is executed, more detail is shown. The following examples are run with the **debug tdm detail** executed.

```
5300# show tdm connections slot 0
Slot 0 MT8980 TDM Device 0, Control Register = 0x1E, ODE Register = 0x01
Connection Memory for ST0:
Ch0: 0x00 0xE1, Ch1: 0x00 0xE2, Ch2: 0x01 0xDE, Ch3: 0x00 0x00
Ch4: 0x01 0xCF, Ch5: 0x00 0xE4, Ch6: 0x00 0xE5, Ch7: 0x00 0x00
Ch8: 0x00 0xEB, Ch9: 0x00 0xE6, Ch10: 0x00 0xE7, Ch11: 0x00 0x00
Ch12: 0x01 0xD1, Ch13: 0x00 0xE8, Ch14: 0x00 0x00, Ch15: 0x00 0xE9
Ch16: 0x00 0x00, Ch17: 0x00 0xD2, Ch18: 0x01 0xD3, Ch19: 0x00 0xEA
Ch20: 0x00 0xEB, Ch21: 0x00 0xC1, Ch22: 0x00 0xEC, Ch23: 0x01 0xC7
```

```

Ch24: 0x00 0xED, Ch25: 0x01 0xC1, Ch26: 0x01 0xD4, Ch27: 0x00 0xEE
Ch28: 0x00 0xE1, Ch29: 0x01 0xD2, Ch30: 0x00 0x00, Ch31: 0x00 0x00
Connection Memory for ST1:
Ch0: 0x00 0xEF, Ch1: 0x00 0xC2, Ch2: 0x00 0xED, Ch3: 0x00 0xF1
Ch4: 0x01 0xC3, Ch5: 0x00 0xF2, Ch6: 0x00 0xE2, Ch7: 0x00 0x00
Ch8: 0x00 0xF3, Ch9: 0x00 0xFF, Ch10: 0x00 0xF4, Ch11: 0x01 0xC4
Ch12: 0x01 0xD5, Ch13: 0x00 0xF5, Ch14: 0x01 0xC5, Ch15: 0x00 0xEE
Ch16: 0x00 0xF6, Ch17: 0x00 0xE3, Ch18: 0x00 0x00, Ch19: 0x00 0xF7
Ch20: 0x01 0xC6, Ch21: 0x01 0xC2, Ch22: 0x00 0xF8, Ch23: 0x00 0xE4
Ch24: 0x00 0xF9, Ch25: 0x00 0xC7, Ch26: 0x00 0x00, Ch27: 0x00 0xFA
Ch28: 0x00 0xFB, Ch29: 0x00 0xE5, Ch30: 0x00 0x00, Ch31: 0x00 0x00

```

Related Commands

Command	Description
show tdm data	Displays information about TDM bus connection memory on Cisco access servers.

show tdm data

To display a snapshot of the time-division multiplexing (TDM) bus data memory in a Cisco AS5200 access server or to display data memory that is programmed on the Mitel TDM chip in a Cisco 5800 access server, use the **show tdm data** command in privileged EXEC mode.

Cisco AS5200 Access Server

```
show tdm data [motherboard | slot slot-number]
```

Cisco AS5800 Access Server

```
show tdm data {motherboard {stream stream-number} | slot slot-number {device device-number
{stream stream-number}}}
```

Syntax	Description
motherboard	<p>Cisco AS5200 Access Server (Optional) Motherboard in the Cisco AS5200 access server.</p> <p>Cisco AS5800 Access Server Motherboard on the Cisco AS5300 access server has the ethernet I/Fs, serial I/Fs, console port, and aux port. The motherboard has one TDM device (MT8980) for the Cisco AS5300 access server.</p>
slot <i>slot-number</i>	<p>Cisco AS5200 Access Server (Optional) Number of the slot being configured.</p> <p>Cisco AS5800 Access Server In addition to the motherboard, there are three slots on the Cisco AS5300 access server. The range of the slots is 0 to 2. A modem card or a trunk PRI card can be inserted in each slot. Each card in the slot has one or two TDM devices (either MT8980 or MT90820) on them.</p>
stream	TDM device stream in the range 0 to 15. There are up to 16 streams on a TDM device (Mitel 90820). The TDM device is also known as the TSI chip. The help on the command (by typing ?) indicates whether the stream is “Stream number within the TSI chip” or “Backplane Stream.”
<i>stream-number</i>	Stream number within the range of either 0 to 7 or 0 to 15.
device	TDM device on the motherboard, or slot cards. Valid range for the Cisco AS5300 access server is 0 to 1. Each card has at least one TDM device (MT8980 or MT80920), and the Octal PRI has two MT90820 TDM devices. Also referred to as TSI Chip Number in the help pages.
<i>device-number</i>	Valid range is 0 to 1.

Command Modes Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(3)T	This command was modified to include support for the Cisco AS5800 access server.

Usage Guidelines**Cisco AS5200 Access Server**

The data memory for all TDM bus connections in the access server is displayed if you do not specify a motherboard or slot.

Cisco AS5800 Access Server

The **show tdm data** command shows the status of the TDM data structure values. This command is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

Examples**Cisco AS5200 Access Server**

The following example shows a snapshot of TDM memory in which the normal ISDN idle pattern (0x7E) is present on all channels of the TDM device resident on the motherboard:

```
AS5200# show tdm data motherboard

MT8980 motherboard unit 0, Control Register = 0x1F, ODE Register = 0x06
Data Memory for ST0:
Ch0: 0x7E, Ch1: 0x7E, Ch2: 0x7E, Ch3: 0x7E
Ch4: 0x7E, Ch5: 0x7E, Ch6: 0x7E, Ch7: 0x7E
Ch8: 0x7E, Ch9: 0x7E, Ch10: 0x7E, Ch11: 0x7E
Ch12: 0x7E, Ch13: 0x7E, Ch14: 0x7E, Ch15: 0x7E
Ch16: 0x7E, Ch17: 0x7E, Ch18: 0x7E, Ch19: 0x7E
Ch20: 0x7E, Ch21: 0x7E, Ch22: 0x7E, Ch23: 0x7E
Ch24: 0x7E, Ch25: 0x7E, Ch26: 0x7E, Ch27: 0x7E
Ch28: 0x7E, Ch29: 0x7E, Ch30: 0x7E, Ch31: 0x7E
Data Memory for ST1:
Ch0: 0x7E, Ch1: 0x7E, Ch2: 0x7E, Ch3: 0x7E
Ch4: 0x7E, Ch5: 0x7E, Ch6: 0x7E, Ch7: 0x7E
Ch8: 0x7E, Ch9: 0x7E, Ch10: 0x7E, Ch11: 0x7E
Ch12: 0x7E, Ch13: 0x7E, Ch14: 0x7E, Ch15: 0x7E
Ch16: 0x7E, Ch17: 0x7E, Ch18: 0x7E, Ch19: 0x7E
Ch20: 0x7E, Ch21: 0x7E, Ch22: 0x7E, Ch23: 0x7E
Ch24: 0x7E, Ch25: 0x7E, Ch26: 0x7E, Ch27: 0x7E
Ch28: 0x7E, Ch29: 0x7E, Ch30: 0x7E, Ch31: 0x7E
```

Cisco AS5800 Access Server

The following sample output shows the general syntax used, and the output displayed for the **show tdm data** command. To display a subset of the data on most the commands, further specify particular slots, streams, and devices. When the **debug tdm detail** command is executed, more detail is shown. The following example is run with the **debug tdm detail** executed:

```
Router# show tdm data

Motherboard MT8980 TDM Device 0, Control Register = 0x1F, ODE Register = 0xE1
Data Memory for ST0:
Ch0: 0xFF, Ch1: 0xFF, Ch2: 0x98, Ch3: 0x61
Ch4: 0x0C, Ch5: 0xE1, Ch6: 0x8D, Ch7: 0x86
Ch8: 0xFF, Ch9: 0xF3, Ch10: 0xE4, Ch11: 0xFF
Ch12: 0x51, Ch13: 0x02, Ch14: 0x18, Ch15: 0x14
```

show tdm data

```

Ch16: 0xFF, Ch17: 0xFF, Ch18: 0x05, Ch19: 0xC7
Ch20: 0x00, Ch21: 0xFF, Ch22: 0xFF, Ch23: 0x98
Ch24: 0xFF, Ch25: 0x15, Ch26: 0x5C, Ch27: 0x15
Ch28: 0xFF, Ch29: 0x80, Ch30: 0xFF, Ch31: 0xFF
Data Memory for ST1:
Ch0: 0xFF, Ch1: 0xFF, Ch2: 0xFF, Ch3: 0x62
Ch4: 0x94, Ch5: 0x88, Ch6: 0xFF, Ch7: 0xFF
Ch8: 0xFF, Ch9: 0xFF, Ch10: 0xFB, Ch11: 0x91
Ch12: 0xF7, Ch13: 0xFF, Ch14: 0x96, Ch15: 0xFF
Ch16: 0xFF, Ch17: 0xFF, Ch18: 0xFF, Ch19: 0x94
Ch20: 0x8F, Ch21: 0x95, Ch22: 0xFF, Ch23: 0xFF
Ch24: 0xE2, Ch25: 0xFF, Ch26: 0xD3, Ch27: 0xFF
Ch28: 0x87, Ch29: 0xFF, Ch30: 0xFF, Ch31: 0xFF
Data Memory for ST2:
...

```

Related Commands

Command	Description
show tdm connections	Displays details about a specific TDM channel programmed on the Mitel chip.

show tdm detail

To display details about a specific time-division multiplexing (TDM) channel programmed on the Mitel chip, use the **show tdm detail** command in privileged EXEC mode.

show tdm detail *slot-number/device-number source-stream-number/source-channel-number*

Syntax Description		
<i>slot-number</i>		There are three slots on the Cisco AS5300 access server. A modem card or a trunk PRI card can be inserted in each slot. Each card has one or two TDM devices (either MT8980 or MT90820) on it. The valid range is 0 to 2.
<i>device-number</i>		TDM device on the motherboard or slot cards. Each card has at least one TDM device (MT8980 or MT80920), and the Octal PRI has two MT90820 TDM devices. Also referred to a TSI Chip Number in the online help. The valid range is 0 to 1.
<i>source-stream-number</i>		Source stream number from the TDM device. The valid range is 0 to 15.
<i>source-channel-number</i>		Source channel from the TDM device stream. The valid range is 0 to 31.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(2)XD	This command was introduced.
	12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines The **show tdm detail** command shows the status of the TDM backplane, related data structure values, and TDM chip memory settings. This command is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

This command indicates connection memory and map, data memory, and whether the channel is enabled or disabled. Specify the specific slot, TDM device, TDM stream, and TDM channel.

Examples The following example shows the general syntax used and the output displayed for the **show tdm detail** command. To display only a subset of the data on most of the commands, further specify particular slots, streams, and devices. When the **debug tdm detail** command is executed, more detail is shown. The following example was run with the **debug tdm detail** command executed:

```
Router# show tdm detail 0/0 1/2

Show Detail TDM device info: slot 0 unit 0
ODE Register: 0x0001
Connection Memory: 0x00ED, Output is Disable
Connection Map: STi7 CHi13 ----> STo1 CHo2
Data Memory: 0x00FF
```

Related Commands	Command	Description
	show tdm backplane	Displays modem and PRI channel assignments with streams and channels on the modem side as assigned to the unit and channels on the PRI side of the TDM assignment.
	show tdm connections	Displays details about a specific TDM channel programmed on the Mitel chip.
	show tdm data	Displays information about TDM bus connection memory on Cisco access servers.
	show tdm information	Displays TDM resources available for the specified TDM device.
	show tdm pool	Displays information about the specified TDM pool.

show tdm information

To display information about the specified time-division multiplexing (TDM) device, use the **show tdm information** command in privileged EXEC mode.

```
show tdm information {motherboard | slot slot-number {device device-number}}
```

Syntax Description		
motherboard		Motherboard on the Cisco AS5300 access server has the ethernet I/Fs, serial I/Fs, console port, and aux port. The motherboard has one TDM device (MT8980) for the Cisco AS5300 access server.
slot		There are three slots on the Cisco AS5300 access server. The range of the slots is 0 to 2. A modem card or a trunk PRI card can be inserted in each slot. Each card has one or two TDM devices (either MT8980 or MT90820) on it.
<i>slot-number</i>		Valid range is 0 to 2.
device		TDM device on the motherboard or slot cards. The valid range is 0 to 1. Each card has at least one TDM device (MT8980 or MT80920), and the Octal PRI has two MT90820 TDM devices. Also referred to as TSI Chip Number in the online help.
<i>device-number</i>		Valid range is 0 to 1.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(2)XD	This command was introduced.
	12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines The **show tdm information** command shows the status of the TDM backplane, related data structure values, and TDM chip memory settings. This command is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

This command displays the register base address, device type, and capabilities on a per-slot basis.

Examples The following example shows the general syntax used and the output displayed for the **show tdm information** command. To display only a subset of the data on most of the commands, specify particular slots, streams, and devices. When the **debug tdm detail** command is executed, more detail is shown. The following example is run with the **debug tdm detail** command executed:

```
Router# show tdm information
```

```
TDM Slot Info display for Motherboard:
Slot Info ptr @0x610D39C0 Feature info ptr @0x60B737E8
Feature board is MOTHERBOARD, NIM ID: 0x30
TSI device is MT8980, 1 on this board. Each TSI device supports 0 DS1s
First TSI device is at offset: 0x100
```

show tdm information

```

TSI device 0, register base 0x3E801100
  TDM Device Info ptr @0x611AA3EC for slot -1
  TSI device Info ptr @0x60FCC0BC  memory size = 0x100
  This device supports 8 streams with 32 channels per stream
TDM Information display for slot 0:
  Slot Info ptr @0x610D39E4  Feature info ptr @0x60E73818
  Feature board is E1 Quad PRI, NIM ID: 0x43
  TSI device is MT8980, 2 on this board. Each TSI device supports 2 DS1s
  First TSI device is at offset: 0x100, Second TSI device is at Offset: 0x200
  HDLC  Streams start at 4
  Framers Streams start at 6
  TSI device 0, register base 0x3C400100
    TDM Device Info ptr @0x61222054 for slot 0
    TSI device Info ptr @0x60FCC0BC  memory size = 0x100
    This device supports 8 streams with 32 channels per stream
  TSI device 1, register base 0x3C400200
    TDM Device Info ptr @0x61222098 for slot 0
    TSI device Info ptr @0x60FCC0BC  memory size = 0x100
    This device supports 8 streams with 32 channels per stream
TDM Information display for slot 1:
  Slot Info ptr @0x610D3A08  Feature info ptr @0x60E738A8
  Feature board is High Density Modems, NIM ID: 0x47
  TSI device is MT8980, 1 on this board. Each TSI device supports 0 DS1s
  First TSI device is at offset: 0x100
  TSI device 0, register base 0x3C500100
    TDM Device Info ptr @0x612F1B80 for slot 1
    TSI device Info ptr @0x60FCC0BC  memory size = 0x100
    This device supports 8 streams with 32 channels per stream
TDM Information display for slot 2:
  Slot Info ptr @0x610D3A2C  Feature info ptr @0x60E738A8
  Feature board is High Density Modems, NIM ID: 0x47
  TSI device is MT8980, 1 on this board. Each TSI device supports 0 DS1s
  First TSI device is at offset: 0x100
  TSI device 0, register base 0x3C600100
    TDM Device Info ptr @0x613A6F60 for slot 2
    TSI device Info ptr @0x60FCC0BC  memory size = 0x100
    This device supports 8 streams with 32 channels per stream

```

Related Commands

Command	Description
show tdm backplane	Displays modem and PRI channel assignments with streams and channels on the modem side as assigned to the unit and channels on the PRI side of the TDM assignment.
show tdm connections	Displays details about a specific TDM channel programmed on the Mitel chip.
show tdm data	Displays information about TDM bus connection memory on Cisco access servers.
show tdm detail	Displays information about the specified TDM device.
show tdm pool	Displays information about the specified TDM pool.

show tdm pool

To display time-division multiplexor (TDM) resources available for the specified TDM device, use the **show tdm pool** command in privileged EXEC mode.

```
show tdm pool [slot slot-number]
```

Syntax Description	slot	(Optional) There are three slots on the Cisco AS5300 access server with a range of 0 to 2. A modem card or a trunk PRI card can be inserted in each slot. Each card has one or two TDM devices (either MT8980 or MT90820) on it.
	slot-number	(Optional) Valid range is 0 to 2 for the Cisco AS5300 access server.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(2)XD	This command was introduced.
	12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.

Usage Guidelines The **show tdm pool** command shows the status of the TDM backplane, related data structure values, and TDM chip memory settings. This command is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

This command displays TDM groups, where group 0 is streams 0 to 3 and group 1 is streams 4-7. It also displays register address and capabilities on a per-slot basis.

Examples The following example shows the general syntax used and the output displayed for the **show tdm pool** command. To display only a subset of the data on most of the commands, further specify particular slots, streams, and devices. When the **debug tdm detail** command is executed, more detail is shown. The following example was run with the **debug tdm detail** command executed:

```
Router# show tdm pool

Dynamic Backplane Timeslot Pool:
Grp ST  Ttl/Free  Req(Cur/Ttl/Fail)  Queues (Free/Used)  Pool Ptr
0 0-3  120 60    60 361    0    0x61077E28 0x61077E28 0x61077E20
1 4-7   0  0     0  0     0    0x61077E38 0x61077E28 0x61077E24
```

Related Commands	Command	Description
	show tdm backplane	Displays modem and PRI channel assignments with streams and channels on the modem side as assigned to the unit and channels on the PRI side of the TDM assignment.
	show tdm connections	Displays details about a specific TDM channel programmed on the Mitel chip.
	show tdm data	Displays information about TDM bus connection memory on Cisco access servers.
	show tdm detail	Displays information about the specified TDM device.
	show tdm information	Displays TDM resources available for the specified TDM device.

shutdown (interface)

To disable an interface, use the **shutdown** command in interface configuration mode. To restart a disabled interface, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

Using this command assumes that the interface is already enabled. By default, if this command is not issued the interface remains enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **shutdown** command disables all functions on the specified interface. On serial interfaces, this command causes the data terminal ready (DTR) signal to be dropped. On Token Ring interfaces, this command causes the interface to be removed from the ring. On FDDI interfaces, this command causes the optical bypass switch, if present, to go into bypass mode.

This command also marks the interface as unavailable. To check whether an interface is disabled, use the **show interfaces EXEC** command. An interface that has been shut down is shown as administratively down in the display from this command.

Examples

The following example turns off Ethernet interface 0:

```
Router(config)# interface ethernet 0
Router(config-if)# shutdown
08:32:03:%LINK-5-CHANGED:Interface Ethernet 0, changed state to administratively down
```

The following example turns the interface back on:

```
Router(config)# interface ethernet 0
Router(config-if)# no shutdown
08:32:16:%LINK-3-UPDOWN:Interface Ethernet 0, changed state to up
08:32:17:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet 0, changed state to up
```

Related Commands

Command	Description
interface	Configures an interface type and enters interface configuration mode.
show interfaces	Displays the statistical information specific to a serial interface.

smt-queue-threshold

To set the maximum number of unprocessed FDDI station management (SMT) frames that will be held for processing, use the **smt-queue-threshold** command in global configuration mode. To restore the queue to the default, use the **no** form of this command.

smt-queue-threshold *number*

no smt-queue-threshold

Syntax Description	<i>number</i>	Number of buffers used to store unprocessed SMT messages that are to be queued for processing. Acceptable values are positive integers. The default value is equal to the number of FDDI interfaces installed in the router.
---------------------------	---------------	--

Defaults The default threshold value is equal to the number of FDDI interfaces installed in the router.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command helps ensure that routers keep track of FDDI *upstream* and *downstream* neighbors, particularly when a router includes more than one FDDI interface.

In FDDI, upstream and downstream neighbors are determined by transmitting and receiving SMT Neighbor Information Frames (NIFs). The router can appear to lose track of neighbors when it receives an SMT frame and the queue currently contains an unprocessed frame. This occurs because the router discards incoming SMT frames if the queue is full. Discarding SMT NIF frames can cause the router to lose its upstream or downstream neighbor.



Caution

Use this command carefully because the SMT buffer is charged to the inbound interface (input hold queue) until the frame is completely processed by the system. Setting this value to a high limit can impact buffer usage and the ability of the router to receive routable packets or routing updates.

Examples The following example specifies that the SMT queue can hold ten messages. As SMT frames are processed by the system, the queue is decreased by one:

```
Router(Config)# smt-queue-threshold 10
```

snmp ifindex clear

To clear any previously configured SNMP ifIndex commands issued in interface configuration mode for a specific interface, use the **snmp ifindex clear** command in interface configuration mode.

snmp ifindex clear

Syntax Description This command has no arguments or keywords.

Defaults SNMP index is not cleared.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(11)S	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)Tn.

Usage Guidelines Interface Index Persistence means that ifIndex values in the IF-MIB persist across reboots, allowing for consistent identification of specific interfaces using Simple Network Management Protocol (SNMP).

Use the **snmp ifindex clear** command on a specific interface when you want that interface to use the global configuration setting for ifIndex persistence. This command clears any ifIndex configuration commands previously entered for that specific interface.

Examples In the following example, ifIndex persistence is enabled for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

IfIndex persistence is then disabled for Ethernetinterface 0/1 only:

```
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

Later, the ifIndex configuration command is cleared from the configuration for Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# snmp ifindex clear
Router(config-if)# exit
```

This leaves ifIndex persistence enabled for all interfaces, as specified by the **snmp-server ifindex persist** global configuration command.

Related Commands	Command	Description
	snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) only on a specific interface.
	snmp-server ifindex persist	Enables ifIndex values that will remain constant across reboots for use by SNMP.

snmp ifindex persist

To enable ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface only, use the **snmp ifindex persist** command in interface configuration mode. To disable ifIndex persistence only on a specific interface, use the **no** form of this command.

snmp ifindex persist

no snmp ifindex persist

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(11)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Interface Index Persistence means that ifIndex values in the IF-MIB persist across reboots, allowing for consistent identification of specific interfaces using Simple Network Management Protocol (SNMP).

The **snmp ifindex persistence** interface configuration command enables and disables ifIndex persistence for individual entries (corresponding to individual interfaces) in the ifIndex table of the IF-MIB.

The **snmp-server ifindex persistence** global configuration command enables and disables ifIndex persistence for all interfaces on the routing device (this applies only to interfaces that have ifDescr and ifIndex entries in the ifIndex table of the IF-MIB).

IfIndex commands configured for an interface apply to all subinterfaces on that interface.

Examples

In the following example, ifIndex persistence is enabled for interface Ethernet interface 0/1 only:

```
Router(config)# interface ethernet 0/1
Router(config-if)# snmp ifindex persist
Router(config-if)# exit
```

In the following example, ifIndex persistence is enabled for all interfaces, and then disabled for interface Ethernet interface 0/1 only:

```
Router(config)# snmp-server ifindex persist
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

Related Commands	Command	Description
	snmp ifindex clear	Clears any previously configured snmp ifIndex commands issued in interface configuration mode for a specific interface.
	snmp-server ifindex persist	Enables ifIndex values that will remain constant across reboots for use by SNMP.

snmp-server ifindex persist

To globally enable ifIndex values which will remain constant across reboots for use by SNMP, use the **snmp-server ifindex persist** command in global configuration mode. To globally disable ifIndex persistence, use the **no** form of this command in global configuration mode.

snmp-server ifindex persist

no snmp-server ifindex persist

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(11)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Interface Index Persistence means that ifIndex values in the IF-MIB persist across reboots, allowing for consistent identification of specific interfaces using SNMP.

The **snmp-server ifindex persist** global configuration command will not override interface-specific configuration. Interface-specific configuration of ifIndex persistence is performed with the **[no] snmp ifindex persist** and **snmp ifindex clear** interface configuration commands.

The **[no] snmp-server ifindex persist** global configuration command enables and disables ifIndex persistence for all interfaces on the routing device using ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

Examples

In the following example, ifIndex persistence is enabled for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

Note that in this example if ifIndex persistence was previously disabled for a specific interface using the **no snmp ifindex persist** interface configuration command, ifIndex persistence will remain disabled for that interface. The global ifIndex command does not override the interface-specific commands.

Related Commands	Command	Description
	snmp ifindex clear	Clears any previously configured snmp ifIndex commands issued in interface configuration mode for a specific interface.
	snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) only on a specific interface.

snmp trap illegal-address

To issue an Simple Network Management Protocol (SNMP) trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router, use the **snmp trap illegal-address** command in hub configuration mode. To disable this function, use the **no** form of this command.

snmp trap illegal-address

no snmp trap illegal-address

Syntax Description This command has no arguments or keywords.

Defaults No SNMP trap is issued.

Command Modes Hub configuration

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines In addition to setting the **snmp trap illegal-address** command on the Ethernet hub, you can set the frequency that the trap is sent to the network management station (NMS). This is done on the NMS via the Cisco Repeater MIB. The frequency of the trap can be configured for once only or at a decaying rate (the default). If the decaying rate is used, the first trap is sent immediately, the second trap is sent after one minute, the third trap is sent after two minutes, and so on until 32 minutes, at which time the trap is sent every 32 minutes. If you use a decaying rate, you can also set the trap acknowledgment so that the trap will be acknowledged after it is received and will no longer be sent to the network management station.

Because traps are not reliable, additional information on a port basis is provided by the Cisco Repeater MIB. The network management function can query the following information: the last illegal MAC source address, the illegal address trap acknowledgment, the illegal address trap enabled, the illegal address first heard (timestamp), the illegal address last heard (timestamp), the last illegal address trap count for the port, and the illegal address trap total count for the port.

In addition to issuing a trap when a MAC address violation is detected, the port is also disabled as long as the MAC address is invalid. The port is enabled and the trap is no longer sent when the MAC address is valid (that is, either the address was configured correctly or learned).

Examples The following example enables an SNMP trap to be issued when a MAC address violation is detected on hub ports 2, 3, or 4. SNMP support must already be configured on the router.

```
Router(config)# hub ethernet 0 2 4
Router(config-hub)# snmp trap illegal-address
```

Related Commands	Command	Description
	hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

source-address

To configure source address control on a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **source-address** command in hub configuration mode. To remove a previously defined source address, use the **no** form of this command.

```
source-address [mac-address]
```

```
no source-address
```

Syntax Description	<i>mac-address</i> (Optional) MAC address in the packets that the hub will allow to access the network.				
Defaults	Disabled				
Command Modes	Hub configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>10.3</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.3	This command was introduced.
Release	Modification				
10.3	This command was introduced.				
Usage Guidelines	If you omit the MAC address, the hub uses the value in the last source address register, and if the address register is invalid, it will remember the first MAC address it receives on the previously specified port and allow only packets from that MAC address onto that port.				
Examples	<p>The following example configures the hub to allow only packets from MAC address 1111.2222.3333 on port 2 of hub 0:</p> <pre>Router(config)# hub ethernet 0 2 Router(config-hub)# source-address 1111.2222.3333</pre> <p>The following example configures the hub to use the value of the last source address register. If the address register is invalid, it will remember the first MAC address it receives on port 2 and allow only packets from the learned MAC address on port 2:</p> <pre>Router(config)# hub ethernet 0 2 Router(config-hub)# source-address</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>hub</td> <td>Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.</td> </tr> </tbody> </table>	Command	Description	hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.
Command	Description				
hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.				

speed

To configure the speed for a Fast Ethernet interface, use the **speed** command in interface configuration mode. To disable a speed setting, use the **no** form of this command.

speed { **10** | **100** | **auto** }

no speed

Syntax Description	10	Configures the interface to transmit at 10 Mbps.
	100	Configures the interface to transmit at 100 Mbps. This is the default.
	auto	Turns on the Fast Ethernet autonegotiation capability. The interface automatically operates at 10 or 100 Mbps depending on environmental factors, such as the type of media and transmission speeds for the peer routers, hubs, and switches used in the network configuration.

Defaults 100 Mbps

Command Modes Interface configuration

Command History	Release	Modification
	11.2(10)P	This command was introduced.

Usage Guidelines The autonegotiation capability is turned on for the Fast Ethernet interface by either configuring the **speed auto** interface configuration command or the **duplex auto** interface configuration command. [Table 53](#) describes the performance of the system for different combinations of the duplex and speed modes. The specified **duplex** command configured with the specified **speed** command produces the resulting system action.

Table 53 Relationship between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex auto	speed auto	Autonegotiates both speed and duplex modes.
duplex auto	speed 100 or speed 10	Autonegotiates both speed and duplex modes.
duplex half or duplex full	speed auto	Autonegotiates both speed and duplex modes.
duplex half	speed 10	Forces 10 Mbps and half duplex.
duplex full	speed 10	Forces 10 Mbps and full duplex.

Table 53 Relationship between duplex and speed Commands (continued)

duplex Command	speed Command	Resulting System Action
duplex half	speed 100	Forces 100 Mbps and half duplex.
duplex full	speed 100	Forces 100 Mbps and full duplex.

Examples

The following example shows the configuration options for the **speed** command:

```
Router(config)# interface fastethernet 0
Router(config-if)# speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration
```

Related Commands

Command	Description
duplex	Configures the duplex operation on an interface.
interface fastethernet	Selects a particular Fast Ethernet interface for configuration.
show controllers fastethernet	Displays information about initialization block information, transmit ring, receive ring, and errors for the Fast Ethernet controller chip on the Cisco 4500, Cisco 7200 series, or Cisco 7500 series routers.
show interfaces fastethernet	Displays information about the Fast Ethernet interfaces.

sqelch

To extend the Ethernet twisted-pair 10BASE-T capability beyond the standard 100 meters on the Cisco 4000 platform, use the **sqelch** command in interface configuration mode. To restore the default, use the **no** form of this command.

sqelch { **normal** | **reduced** }

no sqelch { **normal** | **reduced** }

Syntax Description

normal	Allows normal capability. This is the default.
reduced	Allows extended 10BASE-T capability.

Defaults

Normal range

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example extends the twisted-pair 10BASE-T capability on the cable attached to Ethernet interface 2:

```
Router(config)# interface ethernet 2
Router(config-if)# sqelch reduced
```

srp buffer-size

To make adjustments to buffer settings on the receive side for different priority traffic, use the **srp buffer-size** command in interface configuration mode. To disable buffer size configurations use the **no** form of this command.

srp buffer-size *receive* [*high* | *medium*]

no srp buffer-size *receive* [*high* | *medium*]

Syntax Description		
<i>receive</i>		Allocates synchronous dynamic random-access memory (SDRAM) buffer for incoming packets.
<i>high</i> <i>medium</i>		(Optional) Buffer size, in bytes, for high- or medium-priority packets. Any number from 16 to 8192.

Defaults low = 8192 kbytes, medium = 4096 kbytes, high = 4096 kbytes

Command Modes Interface configuration

Command History	Release	Modification
	12.0(6)S	This command was introduced.
	12.0(7)XE1	This command was introduced on Cisco 7500 series routers.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples The following example sets the buffer size for the receive side at the high setting of 17 kbytes:

```
Router(config-if)# srp buffer-size receive high 17
```

Related Commands	Command	Description
	mtu bytes	Adjusts the maximum packet size MTU size.
	srp deficit-round-robin	Transfers packets from the internal receive buffer to Cisco IOS software.

srp deficit-round-robin

To transfer packets from the internal receive buffer to IOS, use the **srp deficit-round-robin** command in interface configuration mode. To disable **srp deficit-round-robin**, use the **no** form of this command.

srp deficit-round-robin [*input* | *output*] [*high* | *medium* | *low*] [*quantum* | *deficit*]

no srp deficit-round-robin

Syntax Description		
<i>input</i> <i>output</i>	(Optional) Either input or output is specified.	
<i>high</i> <i>medium</i> <i>low</i>	(Optional) Priority queue level.	
<i>quantum</i>	(Optional) DRR quantum value. Any number from 9216 to 32,767. The default is 9,216.	
<i>deficit</i>	(Optional) DRR deficit value. Any number from 0 to 65,535. The default is 16,384.	

Defaults

quantum = 9216
deficit = 16384

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was introduced on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples

The following sample shows packets configured for the high-priority input queue:

```
Router(config)# srp deficit-round-robin input high deficit
```

Related Commands

Command	Description
srp priority-map	Sets priority mapping for transmitting and receiving packets.
srp buffer-size	Makes adjustments to buffer settings on the receive side for different priority traffic.
srp random-detect	Configures WRED parameters on packets received through an SRP interface.

srp loopback

To loop the spatial reuse protocol (SRP) interface on an OC-12c DPTIP, use the **srp loopback** command in interface configuration mode. To remove the loopback, use the **no** form of this command.

```
srp loopback {internal | line} {a | b}
```

```
no srp loopback
```

Syntax Description	internal line	Sets the loopback toward the network before going through the framer (internal), or loops the payload data toward the network (line).
	a	Loops back the A side of the interface (inner tx, outer rx).
	b	Loops back the B side of the interface (outer tx, inner rx).

Defaults Disabled

Command Modes Interface configuration

Command History	Release	Modification
	12.0(6)S	This command was introduced.
	12.0(7)XE1	This command was introduced on Cisco 7500 series routers.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines Use this command for troubleshooting purposes.

Examples The following example configures the loopback test on the A side of the SRP interface:

```
Router(config-if)# srp loopback line a
```

srp priority-map

To set priority mapping for transmitting and receiving packets, use the **srp priority-map** command in interface configuration mode. To disable priority mapping use the **no** form of this command.

```
srp priority-map {receive} {high | medium | low} {transmit} {high | medium}
```

```
no srp priority-map
```

Syntax Description	receive transmit	Receiving or transmitting.
	high medium	Mapping for high- or medium-priority packets. Range is between 1 and 8.
	low	Specifies mapping for low-priority packets on the receive side.

Defaults receive medium = 3, receive high = 5, transmit = 7

Command Modes Interface configuration

Command History	Release	Modification
	12.0(6)S	This command was introduced.
	12.0(7)XE1	This command was introduced on Cisco 7500 series routers.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines The spatial reuse protocol (SRP) interface provides commands to enforce quality of service (QoS) functionality on the transmit side and receive side of Cisco routers. SRP uses the IP type of service (ToS) field values to determine packet priority.

The SRP interface classifies traffic on the transmit side into high- and low-priority traffic. High-priority traffic is rate shaped and has higher priority than low-priority traffic. You have the option to configure high- or low-priority traffic and can rate limit the high-priority traffic.

The **srp priority-map transmit** command enables the user to specify IP packets with values equal to or greater than the ToS value to be considered as high-priority traffic.

On the receive side, when WRED is enabled, SRP hardware classifies packets into high-, medium-, and low-priority packets on the basis of the IP ToS value. After classification, it stores the packet into the internal receive buffer. The receive buffer is partitioned for each priority packet. Cisco routers can employ WRED on the basis of the IP ToS value. Routers also employ the Deficit Round Robin (DRR) algorithm to transfer packets from the internal receive buffer to Cisco IOS software.

The command **srp priority-map receive** enables the user to classify packets as high, medium, or low based on the IP ToS value.

Examples

The following example configures Cisco 7500 series routers to transmit packets with priority greater than 5 as high-priority packets:

```
Router(config-if)# srp priority-map transmit 5
```

Related Commands

Command	Description
srp random-detect	Configures WRED parameters on packets received through an SRP interface.

srp random-detect

To configure WRED (weighted RED) parameters on packets received through an spatial reuse protocol (SRP) interface, use the **srp random-detect** command in interface configuration mode. To return the value to the default, use the **no** form of this command.

```
srp random-detect { compute-interval | enable | input | [high | low | medium] |
                    [exponential-weight | precedence]
```

```
no srp random-detect
```

Syntax Description

<i>compute-interval</i>	Interval in the range of 1 to 128 nanoseconds used to specify the queue depth compute interval.
<i>enable</i>	Enables WRED.
<i>input</i>	WRED on packet input path.
<i>high</i> <i>low</i> <i>medium</i>	(Optional) Priority queue level.
<i>exponential-weight</i>	Queue weight in bits. Any number from 0 to 6.
<i>precedence</i>	Input queue precedence.

Defaults

128 seconds

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was introduced on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples

The following example configures WRED parameters on packets received through an SRP interface with a weight factor of 5:

```
Router(config-if)# srp random-detect input high exponential-weight 5
```

srp shutdown

To disable the spatial reuse protocol (SRP) interface, use the **srp shutdown** command in interface configuration mode. To restart a disabled interface, use the **no** form of this command.

srp shutdown [a | b]

no srp shutdown [a | b]

Syntax Description

a	(Optional) Specifies side A of the SRP interface.
b	(Optional) Specifies side B of the SRP interface.

Defaults

SRP continues to be enabled until this command is issued.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was introduced on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

The **srp shutdown** command disables all functions on the specified side.

Examples

The following example turns off side A of the SRP interface:

```
Router(config-if)# srp shutdown a
```

srp tx-traffic-rate

To limit the amount of high-priority traffic that the spatial reuse protocol (SRP) interface can handle, use the **srp tx-traffic-rate** command in interface configuration mode. Use the **no** form of this command to disable transmitted traffic rate.

srp tx-traffic *number*

no srp tx-traffic *number*

Syntax Description	<i>number</i>	Range in kilobits per second. The range is 1 to 65535.
Defaults	10 Kbps	
Command Modes	Interface configuration	
Command History	Release	Modification
	12.0(6)S	This command was introduced.
	12.0(7)XE1	This command was introduced on Cisco 7500 series routers.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples The following example configures SRP traffic to transmit at 1000 kilobits per second:

```
Router(config-if)# srp stx-traffic-rate 1000
```