show ip director dfp

To display information about the current status of the DistributedDirector connections with a particular Dynamic Feedback Protocol (DFP) agent, use the **show ip director dfp** command in EXEC mode.

show ip director dfp [*host-name* | *ip-address*]

Syntax Description

host-name	(Optional) Host name.
ip-address	(Optional) IP address.

Command Modes

EXEC

Command History

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

Examples

The following is sample output from the **show ip director dfp** command:

```
Router# show ip director dfp

172.24.9.9:
 Max retries: 5
 Timeout between connect attempts: 60
 Timeout between updates: 90
 Last update received: 00:00:12 ago
 Server         Port  BindID  Address   Mask
 172.28.9.9     80    0       0.0.0.0   0.0.0.0
192.168.25.25
 Max retries: 5
 Timeout between connect attempts: 60
 Timeout between updates: 90
 Last update received: 00:00:44 ago
 Server         Port BindID   Address  Mask
 192.168.30.30 80   0         0.0.0.0  0.0.0.0
```

show pas caim

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

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

Syntax Description

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

Command Modes

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 68 lists the output values for this command.

Table 68 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 68 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 68 show pas caim Output Values and Descriptions (continued)

Value	Description
uncomp paks/sec out	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. 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.
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	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. 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.
The remaining statistics summarize operational state and error conditions encountered by the CAIM, and have the following interpretations:	

Table 68 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 68 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 68 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 68 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:

```
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 69 describes the fields shown in the display.

Table 69 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.
Command Ring Shadow	Software ring that stores additional information about each command.

Table 69 show pas caim rings Field Descriptions (continued)

Field	Description
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:

```
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:

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

Table 70 describes the fields shown in the preceding display.

Table 70 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:

```
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: Decomp  Algo: Stac
    Hdrlen: 0002  History: 0x0000
    Callback: 0x8011E700  Shutdown: x8011EBE4  Purge: N
    Comp_db: 0x81034BC0  idb: 0x81038084  ds: 0x8104E514
```

Table 71 describes the fields shown in the preceding display.

Table 71 show pas caim cnxt-table Fields Descriptions

Field	Description
Context	Numeric internal reference for the compression context.
Type	Gives the type of context: • Compr—compression context • Decomp—decompression context
Algo	Gives the compression algorithm used: • 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:

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

Table 72 describes the fields shown in the preceding display.

Table 72 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 72 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: • 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 EXEC mode.

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

Syntax Description

ethernet | **fastethernet**	(Optional) Type of interface.
slot	(Optional) Slot number of the interface.
port	(Optional) Interface number.

Command Modes

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 73 describes the significant fields shown in the display.

Table 73 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 73 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_skeyids	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 73 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 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 EXEC mode.

show pci aim

Syntax Description

This command has no arguments or keywords.

Command Modes

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 FF
          0x20: FF 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 FF
          0x40: FF 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 FF
          0x60: FF 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 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 service-module serial

To display the performance report for an integrated CSU/DSU, use the **show service-module serial** command in privileged EXEC mode.

show service-module serial *number* [**performance-statistics** [*interval-range*]]

Syntax Description

number	Interface number 0 or 1.
performance-statistics	(Optional) Displays the CSU/DSU performance statistics for the past 24 hours. This keyword applies only to the fractional T1/T1 module.
interval-range	(Optional) Specifies the number of 15-minute intervals displayed. You can choose a range from 1 to 96, where each value represents the CSU/DSU activity performed in that 15-minute interval. For example, a range of 2-3 displays the performance statistics for the intervals two and three.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command applies to the 2- and 4-wire 56/64-kbps CSU/DSU module and FT1/T1 CSU/DSU module. The **performance-statistics** keyword applies only to the FT1/T1 CSU/DSU module.

Examples

The following sample output shows CSU/DSU performance statistics on a Cisco 2524 or Cisco 2525 router for intervals 30 to 32. Each interval is 15 minutes long. All the data is zero because no errors were discovered on the T1 line:

```
Router# show service-module serial 1 performance-statistics 30-32

Total Data (last 58 15 minute intervals):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in current interval (131 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 30:
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 31:
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

```
Data in Interval 32:
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

The following is sample output from the **show service-module serial** command for a fractional T1 line:

```
Router1# show service-module serial 0

Module type is T1/fractional
    Hardware revision is B, Software revision is 1.1 ,
    Image checksum is 0x2160B7C, Protocol revision is 1.1
Receiver has AIS alarm,
Unit is currently in test mode:
    line loopback is in progress
Framing is ESF, Line Code is B8ZS, Current clock source is line,
Fraction has 24 timeslots (64 Kbits/sec each), Net bandwidth is 1536 Kbits/sec.
Last user loopback performed:
    remote loopback
    Failed to loopup remote
Last module self-test (done at startup): Passed
Last clearing of alarm counters 0:05:50
    loss of signal        :    1, last occurred 0:01:50
    loss of frame         :    0,
    AIS alarm             :    1, current duration 0:00:49
    Remote alarm          :    0,
    Module access errors  :    0,
Total Data (last 0 15 minute intervals):
Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in current interval (351 seconds elapsed):
    1466 Line Code Violations, 0 Path Code Violations
    25 Slip Secs, 49 Fr Loss Secs, 40 Line Err Secs, 1 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 49 Unavail Secs
```

The following sample output from the **show service-module serial** command displays the status of a switched 56-KB line:

```
Router1# show service-module serial 1

Module type is 4-wire Switched 56
    Hardware revision is B, Software revision is 1.00,
    Image checksum is 0x44453634, Protocol revision is 1.0
Connection state: active,
Receiver has loss of signal, loss of sealing current,
Unit is currently in test mode:
    line loopback is in progress
Current line rate is 56 Kbits/sec
Last user loopback performed:
    dte loopback
    duration 00:00:58
Last module self-test (done at startup): Passed
Last clearing of alarm counters 0:13:54
    oos/oof               :    3, last occurred 0:00:24
    loss of signal        :    3, current duration 0:00:24
    loss of sealing curren:    2, current duration 0:04:39
    loss of frame         :    0,
    rate adaption attempts:    0,
```

The following shows sample output from the **show service-module serial** command issued on a Cisco 3640 modular access router:

```
Router# show service-module serial 0/1
```

```
Module type is 4-wire Switched 56
    Hardware revision is B, Software revision is 1.00,
    Image checksum is 0x42364436, Protocol revision is 1.0
Connection state: Idle
Receiver has no alarms.
CSU/DSU Alarm mask is 0
Current line rate is 56 Kbits/sec
Last module self-test (done at startup): Passed
Last clearing of alarm counters 4d02h
    oos/oof              :    0,
    loss of signal       :    0,
    loss of sealing curren:    0,
    loss of frame        :    0,
    rate adaptation attemp:    0,
```

The following shows sample output from the **show service-module serial** command issued on a Cisco 1605 router:

```
Router# show service-module serial 0

Module type is 4-wire Switched 56
    Hardware revision is B, Software revision is 1.00,
    Image checksum is 0x42364436, Protocol revision is 1.0
Receiver has oos/oof, loss of signal,
CSU/DSU Alarm mask is 4
Current line rate is 56 Kbits/sec
Last module self-test (done at startup): Passed
Last clearing of alarm counters 1d02h
    oos/oof              :    1, current duration 1d02h
    loss of signal       :    1, current duration 1d02h
    loss of frame        :    0,
    rate adaptation attemp:    0,
```

Table 74 describes the fields displayed by the **show service-module serial** command.

Table 74 show service-module serial Field Descriptions

Field	Description
Module type	CSU/DSU module installed in the router. The possible modules are T1/fractional, 2-wire switched 56-kbps, and 4-wire 56/64-kbps.
Receiver has AIS alarm	Alarms detected by the FT1/T1 CSU/DSU module or 2- and 4-wire 56/64-kbps CSU/DSU modules. Possible T1 alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms. Possible switched 56k alarms are as follows: • Receiver has loss of signal. • Receiver has loss of sealing current. • Receiver has loss of frame. • Receiver has rate adaptation attempts.
Unit is currently in test mode	Loopback tests are in progress.
Framing is ESF	Indicates frame type used on the line. Can be extended super frame or super frame.
Line Code is B8ZS	Indicated line-code type configured. Can be alternate mark inversion (AMI) or binary 8-zero substitution (B8ZS).
Current clock source is line	Clock source configured on the line, which can be supplied by the service provider (line) or the integrated CSU/DSU module (internal).
Fraction has 24 time slots	Number of time slots defined for the FT1/T1 module, which can range from 1 to 24.
Net bandwidth	Total bandwidth of the line (for example, 24 time slots multiplied by 64 kbps equals a bandwidth of 1536 kbps).
Last user loopback performed	Type and outcome of the last performed loopback.
Last module self-test (done at startup): Passed	Status of the last self-test performed on an integrated CSU/DSU module.
Last clearing of alarm counters	List of network alarms that were detected and cleared on the CSU/DSU module.
Total Data Data in current interval	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Indicates the occurrence of either a bipolar violation or excessive zeroes error event.
Path Code Violations	Indicates a frame synchronization bit error in the D4 and E1-no CRC formats or a CRC error in the ESF and E1-CRC formats.

Table 74 show service-module serial Field Descriptions (continued)

Field	Description
Slip Secs	Indicates the replication or detection of the payload bits of a DS1 frame. A slip may be performed when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Fr Loss Secs	Indicates the number of seconds an Out-of-Frame error is detected.
Line Err Secs	Line errored seconds is a second in which one or more line code violation errors are detected.
Errored Secs	In ESF and E1-CRC links, an errored second is a second in which one of the following is detected: one or more path code violations; one or more Out-of-Frame defects; one or more controlled slip events; a detected AIS defect. For D4 and E1-no CRC links, the presence of bipolar violation also triggers an errored second.
Bursty Err Secs	Second with fewer than 320 and more than 1 path coding violation errors. No severely errored frame defects or incoming AIS defects are detected. Controlled slips are not included in this parameter.
Severely Err Secs	For ESF signals, a second with one of the following errors: 320 or more path code violation errors; one or more Out-of-Frame defects; a detected AIS defect. For D4 signals, a count of 1-second intervals with framing errors, or an Out-of-Frame defect, or 1544 line code violations.
Unavail Secs	Total time the line was out of service.

Related Commands

Command	Description
clear service-module serial	Resets an integrated CSU/DSU.

show smf

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

show smf [*interface-name*]

Syntax Description

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

Command Modes

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 75 describes the fields shown in the display.

Table 75 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 75 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 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.
stream-number	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 commands 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
```

```
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	**Cisco AS5200 Access Server** (Optional) Motherboard in the Cisco AS5200 access server. **Cisco AS5800 Access Server** 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.
slot *slot-number*	**Cisco AS5200 Access Server** (Optional) Number of the slot being configured. **Cisco AS5800 Access Server** 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.
stream	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.
stream-number	Stream number (the range is 0 to 7 or 0 to 15).
device	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.
device-number	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 **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	**Cisco AS5200 Access Server** (Optional) Motherboard in the Cisco AS5200 access server. **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.
slot *slot-number*	**Cisco AS5200 Access Server** (Optional) Number of the slot being configured. **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.
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.”
stream-number	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.
device-number	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
```

```
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

slot-number	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.
device-number	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.
source-stream-number	Source stream number from the TDM device. The valid range is 0 to 15.
source-channel-number	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.
slot-number	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.
device-number	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:

```
5300# 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
  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 @0x60B73818
  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
  Framer 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 @0x60B738A8
  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 @0x60B738A8
  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:

```
5300# 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 (controller)

To disable the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **shutdown** command in controller configuration mode. To restart a disabled CT3IP, 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 controller is already enabled. By default, if this command is not issued the controller remains enabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Shutting down the CT3IP disables all functions on the interface and sends a blue alarm to the network. The **shutdown** command marks the interface as unavailable. To check if the CT3IP is disabled, use the **show controller t3** command.

Examples

The following example shuts down the CT3IP:

```
Router(config)# controller t3 9/0/0
Router(config-controller)#
```

Related Commands

Command	Description
show controllers t3	Displays the hardware and software driver information for a T3 controller.

shutdown (hub)

To shut down a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **shutdown** command in hub configuration mode. To restart the disabled hub, 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 hub is already enabled. By default, if this command is not issued the hub remains enabled.

Command Modes

Hub configuration

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following example shuts down hub 0, ports 1 through 3:

```
Router(config)# hub ethernet 0 1 3
Router(config-hub)# shutdown
```

Related Commands

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

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

number	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(5Tn.

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 Ethernet interface 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

mac-address	(Optional) MAC address in the packets that the hub will allow to access the network.

Defaults

Disabled

Command Modes

Hub configuration

Command History

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

The following example configures the hub to allow only packets from MAC address 1111.2222.3333 on port 2 of hub 0:

```
Router(config)# hub ethernet 0 2
Router(config-hub)# source-address 1111.2222.3333
```

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:

```
Router(config)# hub ethernet 0 2
Router(config-hub)# source-address
```

Related Commands

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 76 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 76 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 76 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# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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.

squelch

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

squelch {**normal** | **reduced**}

no squelch {**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)# squelch 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

receive	Allocates synchronous dynamic random-access memory (SDRAM) buffer for incoming packets.
high | *medium*	(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, u**se the **no** form of this command .

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

no srp deficit-round-robin

Syntax Description

input | *output*	(Optional) Either input or output is specified.
high | *medium* | *low*	(Optional) Priority queue level.
quantum	(Optional) DRR quantum value. Any number from 9216 to 32,767. The default is 9,216.
deficit	(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:

```
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

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

```
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

number	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 tx-traffic-rate 1000
```

t1

To create a logical T1 controller from each of the specified time slots of the T3 line, use the **t1** command in controller configuration mode. To delete the defined logical controller, use the **no** form of this command.

t1 *ds1* **controller**

no t1 *ds1* **controller**

Syntax Description

ds1	Time slot within the T3 line. The valid time-slot range is from 1 to 28.

Defaults

No default behavior or values.

Command Modes

Controller configuration

Command History

Release	Modification
11.3AAA	This command was introduced.

Usage Guidelines

The purpose of this command is to convert the collection of the 28 T1 controllers comprising the T3 controller into individual T1 controllers that the system can use. In other words, the Cisco AS5800 access server cannot pass data until a T1 controller is configured (using the **controller t1** command), and you cannot configure a T1 controller until it has been created using the **t1** command.

Examples

The following example configures a logical T1 controller at T1 time slot 1 for the T3 controller located in shelf 1, slot 4, port 0. Note that you have to enter the command from controller configuration mode.

```
Router(config)# controller t3 1/4/0
Router(config-controller)# t1 1 controller
Router(config-controller)# end
Router#
```

Related Commands

Command	Description
controller	Configures a T1 controller.
controller t3	Configures a T3 controller.

t1 bert

To enable or disable a bit error rate tester (BERT) test pattern for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 bert** command in controller configuration mode. To disable a BERT test pattern, use the **no** form of this command.

t1 *channel* **bert pattern** {**0s** | **1s** | **2^15** | **2^20** | **2^23**} **interval** *minutes* [**unframed**]

no t1 *channel* **bert pattern** {**0s** | **1s** | **2^15** | **2^20** | **2^23**} **interval** *minutes* [**unframed**]

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
pattern	Specifies the length of the repeating BERT test pattern.
0s	0s—Repeating pattern of zeros (...000...).
1s	1s—Repeating pattern of ones (...111...).
2^15	2^{15}—Pseudorandom repeating pattern that is 32,767 bits in length.
2^20	2^{20}—Pseudorandom repeating pattern that is 1,048,575 bits in length.
2^23	2^{23}—Pseudorandom repeating pattern that is 8,388,607 bits in length.
interval *minutes*	Specifies the duration of the BERT test, in minutes. The interval can be a value from 1 to 14400.
unframed	(Optional) Specifies T1 unframed BERT.

Defaults

No BERT test is performed.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2S	The **unframed** keyword was added to this command.

Usage Guidelines

The BERT test patterns from the CT3IP are framed test patterns (that is, the test patterns are inserted into the payload of the framed T1 signal).

To view the BERT results, use the **show controller t3** or **show controller t3 brief** EXEC commands. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT test
- Total bit errors
- Total bits received

When the T1 channel has a BERT test running, the line state is DOWN. Also, when the BERT test is running and the Status field is Not Sync, the information in the total bit errors field is not valid. When the BERT test is done, the Status field is not relevant.

The **t1 bert** command is not written to NVRAM because it is only used for testing the T1 channel for a short predefined interval and for avoiding accidentally saving the command, which could cause the interface not to come up the next time the router reboots.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Examples

The following example shows how to run a BERT test pattern of all zeros for 30 minutes on T1 channel 6 on the CT3IP in slot 9:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 6 bert pattern 0s interval 30
```

Related Commands

Command	Description
show controllers t3	Displays the hardware and software driver information for a T3 controller.

t1 clock source

To specify where the clock source is obtained for use by each T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 clock source** controller configuration command.

t1 *channel* **clock source** {**internal** | **line**}

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
internal	Specifies that the internal clock source is used. This is the default.
line	Specifies that the network clock source is used.

Defaults

Internal

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If you do not specify the **t1 clock source** command, the default clock source of **internal** is used by all the T1s on the CT3IP.

You can also set the clock source for the CT3IP by using the **clock source** (CT3IP) controller configuration command.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

This command does not have a **no** form.

Examples

The following example sets the clock source for T1 6 and T1 8 on the CT3IP to line:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 6 clock source line
Router(config-controller)# t1 8 clock source line
```

Related Commands

Command	Description
clock source (CT3IP)	Specifies where the clock source is obtained for use by the CT3IP in Cisco 7500 series routers.

t1 external

To specify that a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers is used as an external port so that the T1 channel can be further multiplexed on the Multichannel Interface Processor (MIP) or other multiplexing equipment, use the **t1 external** controller configuration command. To remove a T1 as an external port, use the **no** form of this command.

t1 external *channel* [**cablelength** *feet*] [**linecode ami** | **b8zs**]

no t1 external *channel*

Syntax Description

channel	Number 1, 2, or 3 that indicates the T1 channel.
cablelength *feet*	(Optional) Specifies the cable length, in feet, from the T1 channel to the external CSU or MIP. Values are 0 to 655 feet. The default is 133 feet.
linecode ami | **b8zs**	(Optional) Specifies the line coding used by the T1. Values are alternate mark inversion (AMI) or bipolar 8 zero suppression (B8ZS). The default is B8ZS.

Defaults

No external T1 is specified.

The default cable length is 133 feet.

The default line coding is B8ZS.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The first three T1 channels (1, 2, and 3) of the CT3IP can be broken out to the DSUP-15 connectors on the CPT3IP so that the T1 channel can be further demultiplexed by the MIP on the same router or on another router.

After you configure the external T1 channel, you can continue configuring it as a channelized T1 (also referred to as a *fractional* T1) from the MIP. All channelized T1 commands might not be applicable to the T1 interface. After you configure the channelized T1 on the MIP, you can continue configuring it as you would a normal serial interface. All serial interface commands might not be applicable to the T1 interface.

The line coding on the T1 channel and the MIP must be the same. Because the default line coding format on the T1 channel is B8ZS and the default line coding on the MIP is AMI, you must change the line coding on the MIP or on the T1 so that they match.

To determine if the external device connected to the external T1 port is configured and cabled correctly before configuring an external port, use the **show controllers t3** command and locate the line `Ext1...` in the display output. The line status can be one of the following:

- LOS—Loss of signal indicates that the port is not receiving a valid signal. This is the expected state if nothing is connected to the port.
- AIS—Alarm indication signal indicates that the port is receiving an all-ones signal.
- OK—A valid signal is being received and the signal is not an all-ones signal.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Note Although you can specify a cable length from 0 to 655 feet, the hardware only recognizes the following ranges: 0 to 133, 134 to 266, 267 to 399, 400 to 533, and 534 to 655. For example, entering 150 feet uses the 134 to 266 range. If you later change the cable length to 200 feet, there is no change because 200 is within the 134 to 266 range. However, if you change the cable length to 399, the 267 to 399 range is used. The actual number you enter is stored in the configuration file.

Examples

The following example configures the T1 1 on the CT3IP as an external port using AMI line coding and a cable length of 300 feet:

```
Router(config)# controllers t3 9/0/0
Router(config-controller)# t1 external 1 cablelength 300 linecode ami
```

Related Commands

Command	Description
show controllers t3	Displays the hardware and software driver information for a T3 controller.

t1 fdl ansi

To enable the 1-second transmission of the remote performance reports via the Facility Data Link (FDL) per ANSI T1.403 for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 fdl ansi** controller configuration command. To disable the performance report, use the **no** form of this command.

t1 *channel* **fdl ansi**

no t1 *channel* **fdl ansi**

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.

Defaults

Disabled

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The **t1 fdl ansi** command can be used only if the T1 framing type is Extended Super Frame (ESF).

To display the remote performance report information, use the **show controllers t3 remote performance** command.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Examples

The following example generates the performance reports for T1 channel 8 on the CT3IP:

```
Router(config)# controller t3 9/0/0
Router(config-controller)#  t1 8 fdl ansi
```

Related Commands

Command	Description
show controllers t3	Displays the hardware and software driver information for a T3 controller.

t1 framing

To specify the type of framing used by the T1 channels on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 framing** controller configuration command.

t1 *channel* **framing** {**esf** | **sf**}

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
esf	Specifies that Extended Super Frame (ESF) is used as the T1 framing type. This is the default.
sf	Specifies that Super Frame is used as the T1 framing type.

Defaults

Extended Super Frame (ESF)

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If you do not specify the **t1 framing** command, the default ESF is used.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

This command does not have a **no** form.

Examples

The following example sets the framing for the T1 6 and T1 8 on the CT3IP to super frame:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 6 framing sf
Router(config-controller)# t1 8 framing sf
```

t1 linecode

To specify the type of line coding used by the T1 channels on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 linecode** controller configuration command.

t1 *channel* **linecode** {**ami** | **b8zs**}

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
ami	Specifies that alternate mark inversion (AMI) line coding is used by the T1 channel.
b8zs	Specifies that bipolar 8 zero suppression (B8ZS) line coding is used by the T1 channel. This is the default.

Defaults

B8ZS

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If you do not specify the **t1 linecode** command, the default B8ZS is used.

AMI Line Coding

If you select **ami** line coding for the T1 channel, you must also invert the data on the T1 channel by using the **invert data** interface command. This is required because the T1 channel is bundled into the T3 signal, so there are no local T1 line drivers and receivers associated with it. Therefore, the **t1** *channel* **linecode ami** command does not modify local line driver settings. Rather, it advises the CT3IP what line code the remote T1 is using. The CT3IP uses this information solely for the purpose of determining whether or not to enable the pulse density enforcer for that T1 channel.

B8ZS Line Coding

When you select **b8zs** line coding, the pulse density enforcer is disabled. When you select **ami** line coding, the pulse density enforcer is enabled. To avoid having the pulse density enforcer corrupt data, the T1 channel should be configured for inverted data.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

This command does not have a **no** form.

Examples

The following example sets the line coding for T1 channel 16 on the CT3IP to AMI:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 16 linecode ami
Router(config-controller)# exit
Router(config)# interface serial 9/0/0:16
Router(config-if)# invert data
```

Related Commands

Command	Description
loopback remote (interface)	Loops packets through a CSU/DSU, over a DS3 link or a channelized T1 link, to the remote CSU/DSU and back.
invert data	Inverts the data stream.

t1 test

To break out a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers to the test port for testing, use the **t1 test** controller configuration command. To remove the T1 channel from the test port, use the **no** form of this command.

t1 test *channel* [**cablelength** *feet*] [**linecode** {**ami** | **b8zs**}]

no t1 test *channel*

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
cablelength *feet*	(Optional) Specifies the cable length from the T1 channel to the external CSU or Multi-Channel Interface Processor (MIP). Values are 0 to 655 feet. The default cable length is 133 feet.
linecode {**ami** | **b8zs**}	(Optional) Specifies the line coding format used by the T1 channel. Values are alternate mark inversion (AMI) or bipolar 8 zero suppression (B8ZS). The default is B8ZS.

Defaults

No test port is configured.

The default cable length is 133 feet.

The default line coding is B8ZS.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

You can use the T1 test port available on the CT3IP to break out any of the 28 T1 channels for testing (for example, 24-hour bit error-rate tester (BERT)testing as is commonly done by telephone companies before a line is brought into service).

The T1 test port is also available as an external port. For more information on configuring an external port, see the **t1 external** controller configuration command.

To determine if the external device connected to the T1 test port is configured and cabled correctly before configuring a test port, use the **show controllers t3** command and locate the line `Ext1...` in the display output. The line status can be one of the following:

- LOS—Loss of signal indicates that the port is not receiving a valid signal. This is the expected state if nothing is connected to the port.
- AIS—Alarm indication signal indicates that the port is receiving an all-ones signal.
- OK—A valid signal is being received and the signal is not an all-ones signal.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Note Although you can specify a cable length from 0 to 655 feet, the hardware only recognizes the following ranges: 0 to 133, 134 to 266, 267 to 399, 400 to 533, and 534 to 655. For example, entering 150 feet uses the 134 to 266 range. If you later change the cable length to 200 feet, there is no change because 200 is within the 134 to 266 range. However, if you change the cable length to 399, the 267 to 399 range is used. The actual number you enter is stored in the configuration file.

Examples

The following example configures T1 6 on the CT3IP as a test port using the default cable length and line coding:

```
Router(config)# controller t3 9/0/0
Router(config-controller)#  t1 test 6
```

Related Commands

Command	Description
show controllers t3	Displays the hardware and software driver information for a T3 controller.
t1 external	Specifies that a T1 channel on the CT3IP in Cisco 7500 series routers is used as an external port so the T1 channel can be further multiplexed on the MIP or other multiplexing equipment.

t1 timeslot

To specify the time slots and data rate used on each T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 timeslot** controller configuration command. To remove the configured T1 channel, use the **no** form of this command.

t1 *channel* **timeslot** *range* [**speed** {**56** | **64**}]

no t1 *channel* **timeslot**

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
range	Specifies the time slots assigned to the T1 channel. The range can be 1 to 24. A dash represents a range of time slots, and a comma separates time slots. For example, 1-10,15-18 assigns time slots 1 through 10 and 15 through 18.
speed {**56** | **64**}	(Optional) Specifies the data rate for the T1 channel. Values are 56 kbps or 64 kbps. The default is 64 kbps. The 56-kbps speed is valid only for T1 channels 21 through 28.

Defaults

No time slots are specified for the T1 channel.

The default data rate is 64 kbps.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

You must specify the time slots used by each T1 channel.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Examples

The following example assigns time slots 1 through 24 to T1 1 for full T1 bandwidth usage:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 1 timeslots 1-24
```

The following example assigns time slots 1 to 5 and 20 to 23 to T1 6 for fractional T1 bandwidth usage:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 6 timeslots 1-5,20-23
```

The following example configures T1 8 for *n* x 56 (where *n* is 24) bandwidth usage:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 8 timeslots 1-24 speed 56
```

t1 yellow

To enable detection and generation of yellow alarms for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 yellow** controller configuration command. To disable the detection and generation of yellow alarms, use the **no** form of this command.

t1 *channel* **yellow** {**detection** | **generation**}

no t1 *channel* **yellow** {**detection** | **generation**}

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
detection	Detects yellow alarms. This is the default, along with **generation**.
generation	Generates yellow alarms. This is the default, along with **detection**.

Defaults

Yellow alarms are detected and generated on the T1 channel.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If the T1 framing type is super frame (SF), you should consider disabling yellow alarm detection because the yellow alarm can be incorrectly detected with SF framing.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with Telco numbering schemes for T1 channels within channelized T3 equipment.

Examples

The following example disables the yellow alarm detection on T1 channel 6 on the CT3IP:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 6 framing sf
Router(config-controller)# no t1 6 yellow detection
```

test aim eeprom

To test the data compression Advanced Interface Module (AIM) after it is installed in the Cisco 2600 router, use the **test aim eeprom** global configuration command.

test aim eeprom

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

Caution Using this command can erase all locations in EEPROM memory.

This command does not have a **no** form.

This command is the AIM counterpart of the **test pas eeprom** command, which performs similar tasks for port modules.

Table 77 shows the questions asked of the user when the **test aim eeprom** command is entered, and the recommended user responses.

Table 77 test aim eeprom Command Questions and Responses

Questions	Responses
AIM Slot [0]:	User responds by entering the slot number of the AIM whose EEPROM is to be modified. If the user presses ENTER, the default slot 0 is used.
Use NMC93C46 ID EEPROM [y]:	User responds with "y" if the AIM contains an NMC93C46 type EEPROM and "n" if the AIM contains an X2444 EEPROM. The compression Advanced Interface Module (CAIM) contains a NMC93C46 EEPROM, and this is the default if the user just pressed ENTER.
AIM Slot %d eeprom (? for help)[%c]	General command prompt for the **test aim eeprom** command dialog. The AIM slot number chosen is displayed, and the default command is the last command entered.

Table 77 test aim eeprom Command Questions and Responses (continued)

Questions	Responses
Address within slot %d eeprom, [0x%02x]	Enter the desired address within the EEPROM to modify. The default is the next address beyond the byte last modified. If the user wishes to enter a hexadecimal number, it must be preceded by "0x".
Read or Write access to slot %d at 0x%02x [%c]?	Respond with a W to write to the addressed byte or with an R to read from the addressed byte. The default value is selected by just pressing Enter and is the same as the value specified in the last primitive access.
Write data (hex 8 bits) [%02x]?:	If you respond to prompt B with "W", then prompt C is issued, requesting the user to enter the data to write to the addressed byte. The user enters the desired value. Note that if the user desires to enter a hex value, the hex value entered must be preceded by "0x". Otherwise, the value entered is assumed to be in decimal radix.

There is a danger that you can erase all bytes in the entire EEPROM. Though it is good to have a diagnostic tool that allows you to read and write data, there is a danger that lost data will make the Advanced Interface Module (AIM) card fail.

During your session with the test dialog, you have access to the following commands:

H or h	Displays a summary of the available commands.
d	Dump EEPROM contents—Displays the contents of the EEPROM in hex.
e	Erase EEPROM—Erases the entire EEPROM (all bytes set to 0xff).
p	Primitive access—Erases the EEPROM.
q	Exit EEPROM test—Causes the **test aim eeprom** command dialog to exit to the command line interface (CLI).
z	Zero EEPROM—Zeros the entire EEPROM.

Examples

The following example displays the **test aim eeprom** command user dialog:

```
Router# test aim eeprom
 AIM Slot [0]: 0
 Use NMC93C46 ID EEPROM [y]: y
 AIM Slot 0 eeprom (? for help)[?]:  ?
  d - dump eeprom contents
  e - erase all locations (to 1)
  p - primitive access
  q - exit eeprom test
  z - zero eeprom

  'c' rules of radix type-in and display apply.

 AIM Slot 0 eeprom (? for help)[?]:
```

test interface fastethernet

To test the Fast Ethernet interface by causing the interface to ping itself, use the **test interface fastethernet** EXEC command.

test interface fastethernet *number*

Syntax Description

number	Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 series router, specifies the network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system and are displayed with the **show interfaces** command.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command sends pings from the specified interface to itself. Unlike the **ping** command, the **test interface fastethernet** command does not require the use of an IP address.

This command does not have a **no** form.

Examples

The following example tests a Fast Ethernet interface on a Cisco 4500 router:

```
Router# test interface fastethernet 0
```

Related Commands

Command	Description
ping (privileged)	Diagnoses basic network connectivity on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.
ping (user)	Provides simple ping diagnostics of network connectivity.

test service-module

To perform self-tests on an integrated CSU/DSU serial interface module, such as a 4-wire, 56/64 kbps CSU/DSU, use the **test service-module** privileged EXEC command.

test service-module *type number*

Syntax Description

type	Interface type.
number	Interface number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The following tests are performed on the CSU/DSU:

- ROM checksum test
- RAM test
- EEPROM checksum test
- Flash checksum test
- DTE loopback with an internal pattern test

These self-tests are also performed at power on.

This command cannot be used if a DTE loopback, line loopback, or remote loopback is in progress.

Data transmission is interrupted for 5 seconds when you issue this command. To view the output of the most recent self-tests, use the **show service-module** command.

This command does not have a **no** form.

Examples

This example performs a self-test on serial interface 0:

```
Router# test service-module serial 0
SERVICE_MODULE(0): Performing service-module self test
SERVICE_MODULE(0): self test finished: Passed
```

Related Commands

Command	Description
clear counters	Clears the interface counters.
clear service-module serial	Resets an integrated CSU/DSU.
show service-module serial	Displays the performance report for an integrated CSU/DSU.

timeslot

To enable framed mode on a serial interface on a G.703 E1 port adapter, an FSIP, or an E1-G.703/G.704 serial port adapter, use the **timeslot** interface configuration command. Framed mode allows you to specify a bandwidth for the interface by designating some of the 32 time slots for data and reserving the others for framing (timing). Unframed mode, also known as clear channel, does not reserve any time slots for framing. To restore the interface to unframed mode, use the **no** form of this command or set the start slot to 0.

timeslot *start-slot stop-slot*

no timeslot

Syntax Description

start-slot	First subframe in the major frame. Valid range is 1 to 31 and must be less than or equal to *stop-slot*.
stop-slot	Last subframe in the major frame. Valid range is 1 to 31 and must be greater than or equal to *start-slot*.

Defaults

The default G.703 E1 interface is not configured for framed mode.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
11.1 CA	This command was modified to include the E1-G.703/G.704 serial port adapter and Cisco 7200 series routers.

Usage Guidelines

This command applies to Cisco 4000, 7000, 7200, and 7500 series routers. G.703 E1 interfaces have two modes of operation, framed and unframed. When in framed mode, the range from *start-slot* to *stop-slot* gives the number of 64-kbps slots in use. There are 32 64-kbps slots available.

In framed mode, timeslot 16 is not used for data. To use timeslot 16 for data, use the **ts16** interface configuration command.

Examples

The following example enables framed mode on a serial interface on a G.703 E1 port adapter or a E1-G.703/G.704 port adapter:

```
Router(config)# interface serial 3/0
Router(config-if)# timeslot 1-3
```

Related Commands

Command	Description
ts16	Controls the use of timeslot 16 for data on a G.703 E1 interface or on an E1-G703/G.704 serial port adapter.

transmit-buffers backing-store

To buffer short-term traffic bursts that exceed the bandwidth of the output interface, use the **transmit-buffers backing-store** interface configuration command. To disable this function, use the **no** form of this command.

transmit-buffers backing-store

no transmit-buffers backing-store

Syntax Description

This command has no arguments or keywords.

Defaults

The default is off, unless weighted fair queueing is enabled on the interface. If weighted fair queueing is enabled on the interface, the **transmit-buffers backing-store** command is enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced on the Cisco 7500 router.

Usage Guidelines

If the **transmit-buffers backing-store** command is enabled and a full hardware transmit queue is encountered, packets are swapped out of the original memory device (MEMD) into a system buffer in DRAM. If the **transmit-buffers backing-store** command is *not* enabled and the output hold queue is full, packets are dropped instead of being copied if a full hardware transmit queue is encountered. In both cases, the original MEMD buffer is freed so that it can be reused for other input packets.

To preserve packet order, the router checks the output hold queue and outputs previously queued packets first.

Examples

The following example shows how to enable the **transmit-buffers backing-store** command on a FDDI interface:

```
Router(config)# interface fddi 3/0
Router(config-if)#  transmit-buffers backing-store
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.

transmit-clock-internal

To enable the internally generated clock on a serial interface on a Cisco 7200 series or Cisco 7500 series router when a DTE does not return a transmit clock, use the **transmit-clock-internal** interface configuration command. To disable the feature, use the **no** form of this command.

transmit-clock-internal

no transmit-clock-internal

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example enables the internally generated clock on serial interface 3/0 on a Cisco 7000 series or Cisco 7500 series router:

```
Router(config)# interface serial 3/0
Router(config-if)#  transmit-clock-internal
```

transmitter-delay

To specify a minimum dead-time after transmitting a packet, use the **transmitter-delay** command in interface configuration mode. To restore the default, use the **no** form of this command.

transmitter-delay *delay*

no transmitter-delay

Syntax Description

delay	On the FSIP, high-speed serial interface (HSSI, and) on the IGS router, the minimum number of High-Level Data Link Control HDL) flags to be sent between successive packets. On all other serial interfaces and routers, approximate number of microseconds of minimum delay after transmitting a packet. The valid range is 0 to 13,1071. The default is 0.

Defaults

0 flags or microseconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command is especially useful for serial interfaces that can send back-to-back data packets over serial interfaces faster than some hosts can receive them.

The transmitter delay feature is implemented for the following Token Ring cards: CSC-R16, CSC-R16M, CSC-1R, CSC-2R, and CSC-CTR. For the first four cards, the command syntax is the same as the existing command and specifies the number of microseconds to delay between sending frames that are generated by the router. Transmitter delay for the CSC-CTR uses the same syntax, but specifies a relative time interval to delay between transmission of all frames.

Examples

The following example specifies a delay of 300 microseconds on serial interface 0:

```
Router(config)# interface serial 0
Router(config-if)#  transmitter-delay 300
```

ts16

To control the use of time slot 16 for data on a G.703 E1 interface or on a E1-G.703/G.704 serial port adapter, use the **ts16** interface configuration command. To restore the default, use the **no** form of this command.

ts16

no ts16

Syntax Description

This command has no arguments or keywords.

Defaults

Time slot 16 is used for signaling.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
11.1 CA	This command was modified to include the E1-G.703/G.704 serial port adapter and Cisco 7200 series routers.

Usage Guidelines

This command applies to Cisco 4000, 7000, 7200, and 7500 series routers. By default, time slot 16 is used for signaling. Use this command to configure time slot 16 to be used for data. When in framed mode, in order to get all possible subframes or time slots, you must use the **ts16** command.

Examples

The following example configures time slot 16 to be used for data on a G.703 E1 interface or a E1-G.703/G.704 serial port adapter:

```
Router(config-if)# ts16
```

Related Commands

Command	Description
timeslot	Enables framed mode serial interface on a G.703 E1 port adapter, an FSIP, or an E1-G.703/G.704 serial port adapter.

tunnel checksum

To enable encapsulator-to-decapsulator checksumming of packets on a tunnel interface, use the **tunnel checksum** interface configuration command. To disable checksumming, use the **no** form of this command.

tunnel checksum

no tunnel checksum

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command currently applies to generic route encapsulation (GRE) only. Some passenger protocols rely on media checksums to provide data integrity. By default, the tunnel does not guarantee packet integrity. By enabling end-to-end checksums, the routers will drop corrupted packets.

Examples

In the following example, all protocols will have encapsulator-to-decapsulator checksumming of packets on the tunnel interface:

```
Router(config-if)# tunnel checksum
```

tunnel destination

To specify the destination for a tunnel interface, use the **tunnel destination** interface configuration command. To remove the destination, use the **no** form of this command.

tunnel destination {*hostname* | *ip-address*}

no tunnel destination

Syntax Description

hostname	Name of the host destination.
ip-address	IP address of the host destination expressed in decimal in four-part, dotted notation.

Defaults

No tunnel interface destination is specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface. Refer to *Cisco IOS AppleTalk and Novell IPX Configuration Guide* for more information on AppleTalk Cayman tunneling.

Examples

The following example enables Cayman tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

The following example enables GRE (generic routing encapsulation) tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre ip
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel mode	Sets the encapsulation mode for the tunnel interface.
tunnel source	Sets the source address of a tunnel interface.

tunnel key

To enable an ID key for a tunnel interface, use the **tunnel key** interface configuration command. To remove the ID key, use the **no** form of this command.

tunnel key *key-number*

no tunnel key

Syntax Description

key-number	Number from 0 to 4,294,967,295 that identifies the tunnel key.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command currently applies to generic route encapsulation (GRE) only. Tunnel ID keys can be used as a form of *weak* security to prevent improper configuration or injection of packets from a foreign source.

Note IP multicast traffic is not supported when a tunnel ID key is configured unless the traffic is process-switched. You must configure the **no ip mroute-cache** command in interface configuration mode on the interface if an ID key is configured. This note applies only to Cisco IOS Release 12.0 and earlier releases.

Note When GRE is used, the ID key is carried in each packet. We do *not* recommend relying on this key for security purposes.

Examples

The following example sets the tunnel key to 3:

```
Router(config-if)# tunnel key 3
```

tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** interface configuration command. To restore the default, use the **no** form of this command.

tunnel mode {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **ipip** [**decapsulate-any**] | **iptalk** | **mpls** | **nos**}

no tunnel mode

Syntax Description

aurp	AppleTalk Update Routing Protocol (AURP).
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible CLNS tunnel.
gre	Generic route encapsulation (GRE) protocol. This is the default.
ipip	IP over IP encapsulation.
decapsulate-any	(Optional) Terminates any number of IP-in-IP tunnels at one tunnel interface. Note that this tunnel will not carry any outbound traffic; however, any number of remote tunnel endpoints can use a tunnel configured this way as their destination.
iptalk	Apple IPTalk encapsulation.
mpls	MPLS encapsulation.
nos	KA9Q/NOS compatible IP over IP.

Defaults

GRE tunneling

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keywords were added: • **aurp** • **dvmrp** • **ipip**
11.2	The optional **decapsulate-any** keyword was added.

Usage Guidelines

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Cayman tunneling implements tunneling as designed by Cayman Systems. This enables our routers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers or between our router and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address. This means that there is no way to ping the other end of the tunnel.

Use DVMRP when a router connects to an mrouted router to run DVMRP over a tunnel.You must configure Protocol-Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

GRE (generic routing encapsulation) tunneling can be done between our routers only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. This means that you can ping the other end of the tunnel.

Examples

The following example enables Cayman tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)  tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

The following example enables GRE tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre ip
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel source	Sets the source address of a tunnel interface.

tunnel path-mtu-discovery

To enable Path MTU Discovery (PMTUD) on a GRE or IP-in-IP tunnel interface, use the **tunnel path-mtu-discovery** command in interface configuration mode. To disable PMTUD on a tunnel interface, use the **no** form of this command.

tunnel path-mtu-discovery [**age-timer** {*aging-mins* | **infinite**}]

no tunnel path-mtu-discovery

Syntax Description

age-timer	(Optional) Sets a timer to run for a specified interval, in minutes, after which the tunnel interface resets the maximum transmission unit (MTU) of the path to the default tunnel MTU minus 24 bytes for GRE tunnels or minus 20 bytes for IP-in-IP tunnels. • *aging-mins*—Number of minutes. Range is from 10 to 30. Default is 10. • **infinite**—Disables the age timer.

Defaults

Path MTU Discovery is disabled for a tunnel interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)WC5	This command was introduced.
12.0(7)T3	This command was integrated into Cisco IOS Release 12.0(7)T3.

Usage Guidelines

When PMTUD (RFC 1191) is enabled on a tunnel interface, the router performs PMTUD processing for the GRE (or IP-in-IP) tunnel IP packets. The router always performs PMTUD processing on the original data IP packets that enter the tunnel. When PMTUD is enabled, no packet fragmentation occurs on the encapsulated packets that travel through the tunnel. Without packet fragmentation, there is a better throughput of TCP connections, and this makes PMTUD a method for maximizing the use of available bandwidth in the network between the endpoints of a tunnel interface.

After PMTUD is enabled, the Don’t Fragment (DF) bit of the IP packet header that is forwarded into the tunnel is copied to the IP header of the external IP packets. The external IP packet is the encapsulating IP packet. Adding the DF bit allows the PMTUD mechanism to work on the tunnel path of the tunnel. The tunnel endpoint listens for ICMP unreachable too-big messages and modifies the IP MTU of the tunnel interface, if required.

When the aging timer is configured, the tunnel code resets the tunnel MTU after the aging timer expires. After the tunnel MTU is reset, a set of full-size packets with the DF bit set is required to trigger the tunnel PMTUD and lower the tunnel MTU. At least two packets are dropped each time the tunnel MTU changes.

When PMTUD is disabled, the DF bit of an external (encapsulated) IP packet is set to zero even if the encapsulated packet has a DF bit set to one.

Note PMTUD on a tunnel interface requires that the tunnel endpoint be able to receive ICMP messages generated by routers in the path of the tunnel. Check that ICMP messages can be received before using PMTUD over firewall connections.

PMTUD currently works only on GRE and IP-in-IP tunnel interfaces.

Use the **show interfaces tunnel** command to verify the tunnel PMTUD parameters.

Examples

The following example shows how to enable tunnel PMTUD:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel path-mtu-discovery
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interfaces tunnel	Displays information about the specified tunnel interface.

tunnel sequence-datagrams

To configure a tunnel interface to drop datagrams that arrive out of order, use the **tunnel sequence-datagrams** interface configuration command. To disable this function, use the **no** form of this command.

tunnel sequence-datagrams

no tunnel sequence-datagrams

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command currently applies to generic route encapsulation (GRE) only. This command is useful when carrying passenger protocols that behave poorly when they receive packets out of order (for example, LLC2-based protocols).

Examples

The following example configures the tunnel to drop datagrams that arrive out of order:

```
Router(config-if)# tunnel sequence-datagrams
```

tunnel source

To set source address for a tunnel interface, use the **tunnel source** interface configuration command. To remove the source address, use the **no** form of this command.

tunnel source {*ip-address* | *type number*}

no tunnel source

Syntax Description

ip-address	IP address to use as the source address for packets in the tunnel.
type	Interface type.
number	Specifies the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system and can be displayed with the **show interfaces** command.

Defaults

No tunnel interface source address is set.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Encapsulation Mode

Two tunnels cannot use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

IP Addresses

The IP address specified as the source address must be an address of an interface on the router.

When using tunnels to Cayman boxes, you must set the **tunnel source** command to an explicit IP address on the same subnet as the Cayman box, not the tunnel itself.

Examples

The following example enables Cayman tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 131.108.164.19
Router(config-if)# tunnel mode cayman
```

The following example enables GRE (generic routing encapsulation) tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 131.108.164.19
Router(config-if)# tunnel mode gre ip
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.

tx-queue-limit

To control the number of transmit buffers available to a specified interface on the MCI and SCI cards, use the **tx-queue-limit** interface configuration command.

tx-queue-limit *number*

Syntax Description

number	Maximum number of transmit buffers that the specified interface can subscribe.

Defaults

Defaults depend on the total transmit buffer pool size and the traffic patterns of all the interfaces on the card. Defaults and specified limits are displayed with the **show controllers mci** EXEC command.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command should be used only under the guidance of a technical support representative.

This command does not have a **no** form.

Examples

The following example sets the maximum number of transmit buffers on the interface to 5:

```
Router(config)# interface ethernet 0
Router(config-if)#  tx-queue-limit 5
```

Related Commands

Command	Description
show controllers mci	Displays all information under the MCI card or the SCI.

yellow

To enable generation and detection of yellow alarms, use the **yellow** command in interface configuration mode.

yellow {*generation* | *detection*}

Syntax Description

generation	This setting enables or disables generation of yellow alarms.
detection	This setting enables or disables detection of yellow alarms.

Defaults

Yellow alarm generation and detection are enabled.

Command Modes

Interface Configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(7)XE1	Support for Cisco 7100 series routers added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Use this command to generate and detect yellow alarms.

Examples

The following example enables generation and detection of yellow alarms on a Cisco 7500 series router:

```
interface atm 3/1/0
  yellow generation
  yellow detection
```

Related Commands

Command	Description
show controllers [**atm** *slot*/**ima** *group-number*]	Displays detailed information about IMA groups and the links they include, as well as about current queues.