show dsc clock

To display information about the dial shelf controller clock, use the **show dsc clock** command in privileged EXEC mode with the line card execute (**execute-on**) command.

execute-on *slot-number* **show dsc clock**

Syntax Description

slot-number	Displays information for a specific slot. Slot number (12 or 13) must be occupied by a DSC card.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

You must use the **show dsc clock** command from the router using the **execute-on** command.

Examples

The following is sample output from the **show dsc clock** command:

```
Router# execute-on slot 12 show dsc clock

Router#
Primary Clock:
--------------
Slot: 3, Port 1, Line 0, Priority = 3 up since 00:37:56
Time elapsed since last failure of the primary = 00:38:59

Backup clocks:
Source  Slot    Port    Line    Priority    Status      State
-------------------------------------------------------------
Trunk   1       2       0       10          Good        Configured

All feature boards present are getting good clock from DSC
```

Table 46 describes the significant fields shown in the display:

Table 46 show dcs clock Field Descriptions

Field	Description
Primary clock	The clock designated as the master timing clock.
Priority	The order in which a clock is designated to back up the primary clock or the next higher priority clock in case of its failure.
Backup Source	The clock signal source, such as a trunk, internal clock, or external generator.
Feature board	An application-specific card in the dial shelf, such as a line card.
Trunk	The trunk line connected to the ISP or central office.

Table 46 show dcs clock Field Descriptions (continued)

Field	Description
Status	Whether the clock source is capable of providing a synch source signal.
State	Whether the clock source is connected and assigned a priority.

Related Commands

Command	Description
execute-on	Executes commands remotely on a line card.

show dsi

To display information about the dial shelf interconnect (DSI) port adapter parameters, use the **show dsi** command in privileged EXEC mode with the line card execute (**execute-on**) command.

execute-on show dsi

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

The dial shelf interconnect (DSI) port adapter connects the Cisco 5814 dial shelf to the Cisco 7206 router shelf. The DSI port adapter allows data transfers between the dial shelf and the router shelf. Data is converted into packets by the feature cards, transmitted to a hub on the dial shelf controller card, and from there sent to the router shelf. Conversely, packets from the router shelf are sent to the dial shelf controller card, where they are transmitted over the backplane to the modem and trunk cards. The **show dsi** command is used to show information about the dial shelf interconnect hardware, interface, physical link, PCI registers, and address filters.

Examples

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

```
Router# execute-on slot 1 show dsi

DSI-Tx-FastEthernet0 is up, line protocol is up
  Hardware is DEC21140A, address is 0008.26b7.b008 (bia 0008.26b7.b008)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Half-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 01:17:09, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6 packets input, 596 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     6170 packets output, 813483 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
DSI-Rx-FastEthernet1 is up, line protocol is up
```

```
Hardware is DEC21140A, address is 0008.26b7.b008 (bia 0008.26b7.b008)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6280 packets input, 362493 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Interface DSI-Tx-FastEthernet0
Hardware is DEC21140A
 dec21140_ds=0x604C9FC4, registers=0x3C000000, ib=0x1912E00
 rx ring entries=128, tx ring entries=256
 rxring=0x1912F00, rxr shadow=0x604CA16C, rx_head=6, rx_tail=0
 txring=0x1913740, txr shadow=0x604CA398, tx_head=138, tx_tail=138, tx_count=0
 PHY link up
 CSR0=0xFE024882, CSR3=0x1912F00, CSR4=0x1913740, CSR5=0xFC660000
 CSR6=0x320CA002, CSR7=0xFFFFA261, CSR8=0xE0000000, CSR9=0xFFFDC3FF
 CSR11=0xFFFE0000, CSR12=0xFFFFFF09, CSR15=0xFFFFFEC8
 DEC21140 PCI registers:
  bus_no=0, device_no=1
  CFID=0x00091011, CFCS=0x02800006, CFRV=0x02000022, CFLT=0x0000FF00
  CBIO=0x00000001, CBMA=0x48000000, CFIT=0x28140100, CFDA=0x00000000
 MII registers:
  Register 0x00:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x08:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x10:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x18:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
 throttled=0, enabled=0, disabled=0
 rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
 tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
 tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
 tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
 HW addr filter: 0x604CABC4, ISL Disabled
  Entry= 0:  Addr=FFFF.FFFF.FFFF
  Entry= 1:  Addr=FFFF.FFFF.FFFF
  Entry= 2:  Addr=FFFF.FFFF.FFFF
  Entry= 3:  Addr=FFFF.FFFF.FFFF
  Entry= 4:  Addr=FFFF.FFFF.FFFF
  Entry= 5:  Addr=FFFF.FFFF.FFFF
  Entry= 6:  Addr=FFFF.FFFF.FFFF
  Entry= 7:  Addr=FFFF.FFFF.FFFF
  Entry= 8:  Addr=FFFF.FFFF.FFFF
  Entry= 9:  Addr=FFFF.FFFF.FFFF
  Entry=10:  Addr=FFFF.FFFF.FFFF
  Entry=11:  Addr=FFFF.FFFF.FFFF
  Entry=12:  Addr=FFFF.FFFF.FFFF
  Entry=13:  Addr=FFFF.FFFF.FFFF
  Entry=14:  Addr=FFFF.FFFF.FFFF
  Entry=15:  Addr=0008.26B7.B008

Interface DSI-Rx-FastEthernet1
```

```
Hardware is DEC21140A
dec21140_ds=0x604DDA4C, registers=0x3C000800, ib=0x1A01FC0
rx ring entries=128, tx ring entries=256
 rxring=0x1A020C0, rxr shadow=0x604DDBF4, rx_head=55, rx_tail=0
 txring=0x1A02900, txr shadow=0x604DDE20, tx_head=2, tx_tail=2, tx_count=0
 PHY link up
 CSR0=0xFE024882, CSR3=0x1A020C0, CSR4=0x1A02900, CSR5=0xFC660000
 CSR6=0x320CA202, CSR7=0xFFFFA261, CSR8=0xE0000000, CSR9=0xFFFDC3FF
 CSR11=0xFFFE0000, CSR12=0xFFFFFF09, CSR15=0xFFFFFEC8
 DEC21140 PCI registers:
  bus_no=0, device_no=2
  CFID=0x00091011, CFCS=0x02800006, CFRV=0x02000022, CFLT=0x0000FF00
  CBIO=0x00000001, CBMA=0x48000800, CFIT=0x28140100, CFDA=0x00000000
 MII registers:
  Register 0x00:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x08:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x10:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x18:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
 throttled=0, enabled=0, disabled=0
 rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
 tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
 tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
 tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
 HW addr filter: 0x604DE64C, ISL Disabled
  Entry= 0:  Addr=FFFF.FFFF.FFFF
  Entry= 1:  Addr=FFFF.FFFF.FFFF
  Entry= 2:  Addr=FFFF.FFFF.FFFF
  Entry= 3:  Addr=FFFF.FFFF.FFFF
  Entry= 4:  Addr=FFFF.FFFF.FFFF
  Entry= 5:  Addr=FFFF.FFFF.FFFF
  Entry= 6:  Addr=FFFF.FFFF.FFFF
  Entry= 7:  Addr=FFFF.FFFF.FFFF
  Entry= 8:  Addr=FFFF.FFFF.FFFF
  Entry= 9:  Addr=FFFF.FFFF.FFFF
  Entry=10:  Addr=FFFF.FFFF.FFFF
  Entry=11:  Addr=FFFF.FFFF.FFFF
  Entry=12:  Addr=FFFF.FFFF.FFFF
  Entry=13:  Addr=FFFF.FFFF.FFFF
  Entry=14:  Addr=FFFF.FFFF.FFFF
  Entry=15:  Addr=0008.26B7.B008
```

Table 47 describes the significant fields shown in the display.

Table 47 show dsi Field Descriptions

Field	Description
FastEthernet0 ... is up ... is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, MCI Ethernet, SCI,[1] CBus[2] Ethernet) and address.
Internet address	Internet address followed by subnet mask.
MTU	Maximum Transmission Unit of the interface.
BW	Bandwidth of the interface in kilobits per second.

Table 47 show dsi Field Descriptions (continued)

Field	Description
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
ARP type:	Type of Address Resolution Protocol assigned.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2^{31}ms (and less than 2^{32}ms) ago.
Output queue, input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.

Table 47 show dsi Field Descriptions (continued)

Field	Description
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
Received ... broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Number of packets whose receipt was aborted.
watchdog	Number of times watchdog receive timer expired. It happens when receiving a packet with length greater than 2048.
multicast	Number of multicast packets received.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.

Table 47 show dsi Field Descriptions (continued)

Field	Description
underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted due to an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Number of times a Type 2 Ethernet controller was restarted because of errors.
babbles	The transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Deferred indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission.
output buffer failures	Number of failed buffers and number of buffers swapped out.

1. SCI = Single Cell Input
2. CBus = Command Bus

Related Commands

Command	Description
execute-on	Executes commands on a line card.
show dsip	Displays all information about the DSIP.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip

To display all information about the Distributed System Interconnect Protocol (DSIP) on a Cisco AS5800, use the **show dsip** command in EXEC mode.

show dsip

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

Your Cisco AS5800 universal access server uses a protocol used by the Cisco 7206 router shelf to communicate back and forth with the Cisco 5814 dial shelf controller card(s) and feature cards. Although dial shelf interconnect (DSI) configuration is transparent to the user, there are several show commands to help you view your setup, and debug commands to help you troubleshoot your system.

To display a subset of this information, use the **show dsip clients**, **show dsip nodes**, **show dsip ports**, **show dsip queue**, **show dsip tracing**, **show dsip transport**, and **show dsip version** commands.

Examples

The following is sample output from the **show dsip** command. For a description of the fields shown in the sample output, refer to the individual **show dsip** commands listed in the "Usage Guidelines" section.

```
Router# show dsip

DSIP Transport Statistics:
 IPC : input msgs=8233, bytes=699488; output msgs=8233, bytes=483558
        total consumed ipc msgs=682;  total freed ipc msgs = 682
        transmit contexts in use = 11, free = 245, zombie = 0, invalid = 0
        ipc getmsg failures = 0, ipc timeouts=0
        core getbuffer failures=0, api getbuffer failures=0
       dsip test msgs rcvd = 2770, sent = 0
 CNTL: input msgs=1112, bytes=91272; output msgs=146, bytes=8760
        getbuffer failures=0
 DATA: input msgs=0, bytes=0; output msgs=426, bytes=5112

DSIP Private  Buffer Pool Hits  = 0

DSIP Registered Addresses:
 Shelf0 : Master: 00e0.b093.2238, Status=local
 Shelf1 : Slot1 : 0007.5387.4808, Status=remote
 Shelf1 : Slot5 : 0007.5387.4828, Status=remote
 Shelf1 : Slot6 : 0007.5387.4830, Status=remote
 Shelf1 : Slot7 : 0007.5387.4838, Status=remote
 Shelf1 : Slot8 : 0007.5387.4840, Status=remote
 Shelf1 : Slot9 : 0007.5387.4848, Status=remote
 Shelf1 : Slot11: 0007.5387.4858, Status=remote
 Shelf1 : Slot12: 0007.4b67.8260, Status=remote
```

```
DSIP Clients:
-------------
ID    Name
0   Console
1   Clock
2   Modem
3   Logger
4   Trunk
5   Async data
6   TDM
7   Dial shelf manager
8   Environment Mon
9   DSIP Test

Dsip Local Ports:
-----------------
Client:Portname              Portid    In-Msgs   Bytes     Last-i/p
Console:Master               10004     0         0         never
Clock:Master                 10005     29        3464      00:00:40
Modem:Master                 10006     90        70162     00:23:44
Logger:Master                10007     0         0         never
Trunk:Master                 10008     1765      140480    00:00:08
Async data:Master            10009     0         0         never
TDM:Master                   1000A     7         112       00:24:19
Dial shelf manager:Master    1000B     28        4752      00:00:36
DSIP Test:Master             1000C     2922      2922      00:00:00

Dsip Remote Ports:
------------------
Client:Portname              Portid    Out-Msgs  Bytes     Last-o/p  Last-act
Clock:Slave1                 101005F   1         24        00:24:21  00:24:21
Trunk:Slave1                 1010061   12        1776      00:24:21  00:24:21
Modem:Slave5                 1050050   96        2148      00:23:56  00:24:19
Modem:Slave6                 1060050   105       2040      00:24:00  00:24:22
Modem:Slave7                 1070050   106       2188      00:23:56  00:24:20
Modem:Slave8                 1080050   112       2212      00:24:13  00:24:35
Modem:Slave9                 1090050   115       2224      00:24:09  00:24:35
Modem:Slave11                10B0050   107       2192      00:24:09  00:24:32
Clock:Slave12                10C000D   1         24        00:24:37  00:24:37
Dial shelf manager:Slave12   10C000E   28        4752      00:00:49  00:24:35
DSIP Test:Slave12            10C000F   0         0         never     00:24:35

DSIP ipc queue:
---------------
There are 0 IPC messages waiting for acknowledgement in the transmit queue.
There are 0 messages currently in use by the system.

DSIP ipc seats:
---------------
There are 9 nodes in this IPC realm.
   ID     Type                Name                      Last  Last
                                                        Sent  Heard
   10000 Local       IPC Master                           0      0
 1060000 DSIP        Seat:Slave6                          10     10
 10C0000 DSIP        Seat:Slave12                         2963   13
 1080000 DSIP        Seat:Slave8                          10     10
 1090000 DSIP        Seat:Slave9                          10     10
 1010000 DSIP        Seat:Slave1                          16     16
 1070000 DSIP        Seat:Slave7                          10     10
 10B0000 DSIP        Seat:Slave11                         10     10
 1050000 DSIP        Seat:Slave5                          10     10

DSIP version information:
```

```
------------------------
Local DSIP major version =  3,    minor version = 2

All DS slots are running DSIP versions compatible with RS

Local Clients Registered Versions:
-----------------------------------
Client Name      Major Version   Minor Version
Console          3               2
Clock            1               1
Modem            0               0
Logger           No version      No version
Trunk            No version      No version
Async data       No version      No version
TDM              No version      No version
DSIP Test        No version      No version

Mismatched  Remote Client Versions:
-----------------------------------
```

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the processors running the DSIP.
show dsip ports	Displays information about local and remote ports.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip clients

To display information about Distributed System Interconnect Protocol (DSIP) clients, use the **show dsip clients** command in EXEC mode.

show dsip clients

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

Use this command to see whether a client is actually registered with DSIP and using its services.

Consider the following example: a client “Trunk” seems to be defunct on a particular node with absolutely no input/output activity. The command **show dsip ports** does not show any Trunk port among its local ports though all other client ports show up. The problem might be that the Trunk client did not even register with DSIP. To confirm this, use the **show dsip clients** command.

Examples

The following is sample output from the **show dsip clients** command. This command lists the clients.

```
Router# show dsip clients

ID    Name
0   Console
1   Clock
2   Modem
3   Logger
4   Trunk
5   Async data
6   TDM
7   Dial shelf manager
8   Environment Mon
9   DSIP Test
```

Related Commands

Command	Description
show dsip nodes	Displays information about the processors running the DSIP.
show dsip ports	Displays information about local and remote ports
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.

show dsip nodes

To display information about the processors running the Distributed System Interconnect Protocol (DSIP), use the **show dsip nodes** command in EXEC mode.

show dsip nodes

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

Use **show dsip nodes** to see the nodes (slots) connected by DSIP and the node specific sequence numbers. The former information is also available from **show dsip transport**. The sequence numbers are useful for support engineers while debugging a problem.

Examples

The following is sample output from the **show dsip nodes** command:

```
Router# show dsip nodes

DSIP ipc nodes:
---------------
There are 9 nodes in this IPC realm.
   ID     Type                 Name                      Last  Last
                                                         Sent  Heard
   10000 Local      IPC Master                             0      0
 1130000 DSIP       Dial Shelf:Slave12                     12     12
 1080000 DSIP       Dial Shelf:Slave1                      1      1
 10A0000 DSIP       Dial Shelf:Slave3                      1      1
 10C0000 DSIP       Dial Shelf:Slave5                      1      1
 10D0000 DSIP       Dial Shelf:Slave6                      1      1
 10E0000 DSIP       Dial Shelf:Slave7                      1      1
 10F0000 DSIP       Dial Shelf:Slave8                      1      1
 1100000 DSIP       Dial Shelf:Slave9                      1      1
```

Table 48 describes the significant fields shown in the display.

Table 48 show dsip nodes Field Descriptions

Field	Description
ID	DSIP uses Cisco's IPC (Inter Process Communication) module for nondata related (client control messages etc.) traffic. A seat or node is a computational element, such as a processor, that can be communicated with using IPC services. A seat is where entities and IPC ports reside. The IPC maintains a seat table which contains the seatids of all the seats in the system. Normally this seatid is a function of the slot number.
Type	Local: Local node. DSIP: Remote DSIP node.
Name	Each seat (node) has a name to easily identify it. There is only one master node and rest are slave nodes. The master node name is "IPC Master" and the slave node name is "Seat:Slave X", where "X" is the slot number of the node.
Last Sent/Last Heard	Each node maintains two sequence numbers for the last sent and last heard.
Last Sent	Whenever a message is sent out, the "last sent" counter is updated.
Last Heard	Whenever a message is received from a remote node, "last heard" is updated.

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip ports	Displays information about local and remote ports
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.

show dsip ports

To display information about local and remote ports, use the **show dsip ports** command in EXEC mode.

show dsip ports [**local** | **remote** [*slot*]]

Syntax Description

local	(Optional) Displays information for local ports. The local port is the port created at a seat's local end.
remote	(Optional) Displays information for remote ports. The remote port is the port residing on a remote seat to which DSIP IPC based connection is open.
slot	(Optional) Specifies a slot number to display information for a specific card on the dial shelf.

Defaults

If no options are specified, information is displayed for both local and remote ports.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

The DSIP communication going through the IPC stack uses ports. The creation of a port returns a 32-bit port ID which is the endpoint for communication between two IPC clients.

The **show dsip ports** command is used to check clients that are up and running:

- To see the local ports that are created and the activity on them.
- To see the remote ports which are connected and to see the activity on them.

Examples

The following is sample output from the **show dsip ports** command:

```
Router# show dsip ports

Dsip Local Ports:
----------------
Client:Portname             Portid    In-Msgs   Bytes     Last-i/p
Console:Master              10004     0         0         never
Clock:Master                10005     16        1800      00:00:05
Modem:Master                10006     90        70162     00:10:08
Logger:Master               10007     0         0         never
Trunk:Master                10008     792       62640     00:00:03
Async data:Master           10009     0         0         never
TDM:Master                  1000A     7         112       00:10:44
Dial shelf manager:Master   1000B     15        2256      00:00:27
DSIP Test:Master            1000C     1294      1294      00:00:00
```

```
Dsip Remote Ports:
------------------
Client:Portname              Portid    Out-Msgs  Bytes     Last-o/p  Last-act
Clock:Slave1                 101005F   1         24        00:10:46  00:10:46
Trunk:Slave1                 1010061   12        1776      00:10:46  00:10:46
Modem:Slave5                 1050050   96        2148      00:10:21  00:10:44
Modem:Slave6                 1060050   105       2040      00:10:25  00:10:48
Modem:Slave7                 1070050   106       2188      00:10:21  00:10:45
Modem:Slave8                 1080050   112       2212      00:10:25  00:10:47
Modem:Slave9                 1090050   115       2224      00:10:39  00:11:05
Modem:Slave11                10B0050   107       2192      00:10:39  00:11:02
Clock:Slave12                10C000D   1         24        00:11:07  00:11:07
Dial shelf manager:Slave12   10C000E   15        2256      00:00:45  00:11:05
DSIP Test:Slave12            10C000F   0         0         never     00:11:05
```

Table 49 describes the significant fields shown in the display.

Table 49 show dsip ports Field Descriptions

Field	Description
Client:Portname	Client name and port name. Port Name. The port names can be determined because they are based on a uniform naming convention that includes the following elements: • Client name • Master/slave status • Slot number Any client can derive the port name of the other client it wants to talk to once it knows its physical location, using the following formula: Master/Slave Status — Port Name Syntax Master — *Client-Name*:**Master**, for example, **Console:Master** Slave — *Client-Name*:**Slave***Slot*, for example, **Clock:Slave1**
Portid	Port ID. The Port ID is a 32-bit identifier comprised of **seatid** and the **port-number**. The IPC maintains a seat table which contains the seatids of all the seats in the system. A seat is where clients and ports reside. The seat ID is a function of the slot number. Port number is the sequential number of the port that is being created on a particular seat, for example: 0,1, 2, etc.
In-Msgs/	The total number of input messages that were received on a particular port.
Out-Msgs	The total number of output messages that were sent to a particular remote port.
Bytes(in/out)	The total number of bytes that were received on a particular port or sent to a remote port. The number of bytes on this port up to the time of the execution of the **show** command.
Last-i/p	Elapsed time since the last input was received on a local port.
Last-o/p	Elapsed time since the last message was sent to a particular remote port.
Last-act	Elapsed time since the connection to a remote port was opened.

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip queue

To display the number of IPC messages in the transmission queue waiting for acknowledgment, use the **show dsip queue** command in EXEC mode.

show dsip queue

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

IPC is inter-process communication. Processes communicate by exchanging messages held in queue buffers. Use the show dsip queue to display the status of these queue buffers.

Examples

The following is sample output from the **show dsip queue** command when the system is operating correctly:

```
Router# show dsip queue

DSIP ipc queue:
---------------
There are 0 IPC messages waiting for acknowledgment in the transmit queue.
There are 0 messages currently in use by the system.
```

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip ports	Displays information about local and remote ports.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip tracing

To display Distributed System Interconnect Protocol (DSIP) tracing buffer information, use the **show dsip tracing** command in EXEC mode.

show dsip tracing [**control** | **data** | **ipc**] [*slot* | **entries** *entry-number* [*slot*]]

Syntax Description

control	(Optional) Displays the control tracing buffer.
data	(Optional) Displays the data tracing buffer.
ipc	(Optional) Displays the inter-process communication tracing buffer.
slot	(Optional) Specifies a specific slot number on the dial shelf. Slot number can be 0 to 14.
entries *entry-number*	(Optional) Specifies the number of entries to trace. Entries can be 1 to 500.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

This feature allows logging of DSIP media header information. Use the **show dsip tracing** command to obtain important information of the various classes of DSIP packets (Control/Data/IPC) coming in. You must first use the **debug dsip tracing** command then use the **show dsip tracing** command to display the logged contents. To clear the information, use the **clear dsip tracing** command.

Examples

The following is sample output from the **show dsip tracing** command:

```
Router# debug dsip tracing

DSIP tracing debugging is on
Router#

Router# show dsip tracing

Dsip Control Packet Trace:
------------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.5387.4808 Type:200B SrcShelf:1 SrcSlot:1 MsgType:0 MsgLen:82
Timestamp: 00:00:03
------------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.5387.4838 Type:200B SrcShelf:1 SrcSlot:7 MsgType:0 MsgLen:82
Timestamp: 00:00:03
------------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.4b67.8260 Type:200B SrcShelf:1 SrcSlot:12 MsgType:0 MsgLen:82
Timestamp: 00:00:03
------------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.5387.4858 Type:200B SrcShelf:1 SrcSlot:11 MsgType:0 MsgLen:82
Timestamp: 00:00:03
------------------------------------------------------------------------------
```

```
Dest:00e0.b093.2238 Src:0007.5387.4848 Type:200B SrcShelf:1 SrcSlot:9 MsgType:0 MsgLen:82
Timestamp: 00:00:03
```

Table 50 describes the significant fields shown in the display:

Table 50 show dsip tracing Field Descriptions

Field	Description
Dest	The destination MAC address in the DSIP packet.
Src	The source MAC address in the DSIP packet.
Type	There are three types of DSIP packets: • Control—0x200B • IPC—0x200C • Data—0x200D
SrcShelf	The source shelf ID of the DSIP packet.
SrcSlot	The source slot of the DSIP packet.
MsgType	Used to further demultiplex Data packets. Not used for Control and IPC type packets.
MsgLen	Length of the message excluding the DSIP header.
Timestamp	Time elapsed since the packet was received.

Related Commands

Command	Description
clear dsip tracing	Clears DSIP tracing logs.
debug dsip tracing	Enables DSIP trace logging for use with the show dsip tracing commands.

show dsip transport

To display information about the Distributed System Interconnect Protocol (DSIP) transport statistics for the control/data and IPC packets and registered addresses, use the **show dsip transport** command in EXEC mode.

show dsip transport

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Examples

The following is sample output from the **show dsip transport** command:

```
Router# show dsip transport

DSIP Transport Statistics:
 IPC : input msgs=4105, bytes=375628; output msgs=4105, bytes=248324
        total consumed ipc msgs=669;  total freed ipc msgs = 669
        transmit contexts in use = 11, free = 245, zombie = 0, invalid = 0
        ipc getmsg failures = 0, ipc timeouts=0
        core getbuffer failures=0, api getbuffer failures=0
       dsip test msgs rcvd = 1200, sent = 0
 CNTL: input msgs=488, bytes=40104; output msgs=68, bytes=4080
        getbuffer failures=0
 DATA: input msgs=0, bytes=0; output msgs=426, bytes=5112

DSIP Private  Buffer Pool Hits  = 0

DSIP Registered Addresses:
 Shelf0 : Master: 00e0.b093.2238, Status=local
 Shelf1 : Slot1 : 0007.5387.4808, Status=remote
 Shelf1 : Slot5 : 0007.5387.4828, Status=remote
 Shelf1 : Slot6 : 0007.5387.4830, Status=remote
 Shelf1 : Slot7 : 0007.5387.4838, Status=remote
 Shelf1 : Slot8 : 0007.5387.4840, Status=remote
 Shelf1 : Slot9 : 0007.5387.4848, Status=remote
 Shelf1 : Slot11: 0007.5387.4858, Status=remote
 Shelf1 : Slot12: 0007.4b67.8260, Status=remote
Router#
```

Table 51 describes the significant fields shown in the display:

Table 51 show dsip transport Field Descriptions

Field	Description
DSIP Transport Statistics:	There are basically three kinds of communication channels between the DSIP modules running on two processors: 1. IPC: DSIP IPC-based reliable/best-effort channel. 2. CNTL: Control packet channel for DSIP modules to communicate between themselves. For example, keepalive messages and initial handshake messages between two DSIP modules are exchanged over this channel. 3. DATA: DSIP fast data packet channel.
input msgs/output msgs	The number of input/output packets on a particular channel.
bytes	The number of input bytes received or sent on a particular channel.
total consumed ipc msgs	The total number of IPC messages consumed so far from the IPC buffer pool.
total freed ipc msgs	The total number of IPC messages returned to the IPC buffer pool so far.
transmit contexts in use	DSIP for each active reliable connection to a remote port keeps a transmit context. This context holds all the important information pertaining to the remote connection, such as, destination portid, port name, number of message and bytes sent to that port etc. This is created when first time a connection is opened to a remote port and is reused for all subsequent communication to that port.
free	Free transmit context is available.
zombie	When DSIP tears down a connection to a remote slot, all the transmit contexts to that slot should return to the free pool. But instead of immediately returning to the free pool, all such contexts first end up on a zombie queue, spend their last few seconds here and then eventually return to the free queue.
invalid	Each transmit context has a magic number. While returning contexts to the free queue, if any transmit context is found to be corrupted, it is marked as invalid and is not returned to the free queue.
ipc getmsg failures	Number of times we failed to get an ipc message.
ipc timeouts	The retry timeouts of the reliable DSIP transport stack.
core getbuffer failures	The number of times DSIP transport layer has failed to allocate buffers for the IPC transport.
aip getbuffer failures	The number of times DSIP transport has failed to allocate buffers while preparing to transmit data received from the clients.
dsip test msgs received/sent	The DSIP test messages received and sent by invoking received/sent the “DSIP Test” client.

Table 51 show dsip transport Field Descriptions (continued)

Field	Description
DSIP Private Buffer Pool Hits	DSIP by default gets all its buffers from the public buffer pools. If for some reason, it runs out of those buffers, it falls back on a DSIP private pool. This number indicates the number of times DSIP has used this fallback pool.
DSIP Registered Addresses	The MAC addresses of nodes (slots) participating in DSIP communication including the local node. The master sees N slaves whereas slave sees only master (excluding themselves). The information is presented in the following form: Shelf*X*: Master | Slot*Y* : *MAC Address* : Status= local | remote

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip ports	Displays information about local and remote DSIP ports.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip version

To display Distributed System Interconnect Protocol (DSIP) version information, use the **show dsip version** command in EXEC mode.

show dsip version

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Examples

The following is sample output from the **show dsip version** command:

```
Router# show dsip version

DSIP version information:
------------------------
Local DSIP major version = 5,    minor version = 2

All feature boards are running DSIP versions compatible with router shelf

Local Clients Registered Versions:
-----------------------------------
Client Name      Major Version   Minor Version
Console          52
Clock            1               1
Modem            0               0
Logger           No version      No version
Trunk            No version      No version
Async data       No version      No version
TDM              No version      No version
DSIP Test        No version      No version

Mismatched  Remote Client Versions:
---------------------------------
```

DSIP is version-controlled software that should be identified and kept current.

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip ports	Displays information about local and remote DSIP ports.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show interfaces bri

To display information about the BRI D channel or about one or more B channels, use the **show interfaces bri** command in privileged EXEC mode.

show interfaces bri *number*[[**:***bchannel*] | [*first*] [*last*]] [**accounting**]

Cisco 7200 Series Router only

show interfaces bri *slot/port*

Syntax Description

number	Interface number. The value is 0 through 7 if the router has one 8-port BRI NIM or 0 through 15 if the router has two 8-port BRI NIMs. Interface number values will vary, depending on the hardware platform used. The Cisco 3600 series router, for example, can have up to 48 interfaces. Specifying just the number will display the D channel for that BRI interface.
slot/port	On the Cisco 7200 series, slot location and port number of the interface.
:*bchannel*	(Optional) Colon (:) followed by a specific B channel number.
first	(Optional) Specifies the first of the B channels; the value can be either 1 or 2.
last	(Optional) Specifies the last of the B channels; the value can only be 2, indicating B channels 1 and 2.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
11.2 P	This command was enhanced to support the slot/port syntax for the PA-8B-ST and PA-4B-U port adapters on the Cisco 7200 series.

Usage Guidelines

Use either the **:***bchannel* argument or the *first* or *last* arguments to display information about specified B channels.

Use the **show interfaces bri** *number* form of the command (without the optional **:***bchannel*, or *first* and *last* arguments) to obtain D channel information.

Use the command syntax sample combinations in Table 52 to display the associated output.

Table 52 Sample show interfaces bri Command Step Combinations

Command Syntax	Displays
show interfaces	All interfaces in the router
show interfaces bri 2	Channel D for BRI interface 2

Table 52 Sample show interfaces bri Command Step Combinations (continued)

Command Syntax	Displays
show interfaces bri 2:1	Channel B1 on BRI interface 2
show interfaces bri 2:2	Channel B2 on BRI interface 2
show interfaces bri 4 1	Channel B1 on BRI interface 4
show interfaces bri 4 2	Channel B2 on BRI interface 4
show interfaces bri 4 1 2	Channels B1 and B2 on BRI interface 4
show interfaces bri	Error message: "% Incomplete command."

Examples

The following is sample output from the **show interfaces bri** command:

```
Router# show interfaces bri 0:1

BRI0:1 is down, line protocol is down
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  LCP Closed
  Closed: IPCP
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 7 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

The following is sample output from the **show interfaces bri** command on a Cisco 7200 series router:

```
Router# show interfaces bri 2/0

BRI2/0 is up, line protocol is up (spoofing)
  Hardware is BRI
  Internet address is 11.1.1.3/27
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/64/0 (size/threshold/drops)
     Conversations  0/1 (active/max active)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     609 packets input, 2526 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     615 packets output, 2596 bytes, 0 underruns
     0 output errors, 0 collisions, 5 interface resets
     0 output buffer failures, 0 output buffers swapped out
     3 carrier transitions
```

Table 53 describes the significant fields shown in the display.

Table 53 show interfaces bri Field Descriptions

Field	Description
BRI... is {up | down | administratively down}	Indicates whether the interface hardware is currently active (whether line signal is present) and whether it has been taken down by an administrator.
line protocol is {up | down | administratively down}	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful).
Hardware is	Hardware type.
Internet address is	IP address and subnet mask, followed by packet size.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a nonfunctioning interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks (**) are printed.
Output queue, drops Input queue, drops	Number of packets in output and input queues. Each number is followed by a slash (/), the maximum size of the queue, and the number of packets dropped due to a full queue.
Five minute input rate Five minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and media access control (MAC) encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.

Table 53 show interfaces bri Field Descriptions (continued)

Field	Description
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so this sum may not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating station or far-end device does not match the checksum calculated from the data received. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can increase the ignored count.
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
packets output	Total number of messages sent by the system.
bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of collisions. These can occur when you have several devices connected on a multiport line.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system recognizes that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.

Table 53 show interfaces bri Field Descriptions (continued)

Field	Description
restarts	Number of times the controller was restarted because of errors.
carrier transitions	Number of times the carrier detect signal of a serial interface has changed state. Check for modem or line problems if the carrier detect line is changing state often.

show interfaces serial bchannel

To display information about the physical attributes of the ISDN PRI over channelized E1 or channelized T1 B and D channels, use the **show interfaces serial bchannel** command in EXEC mode.

show interfaces serial *slot/port* **bchannel** *channel-number*

show interfaces serial *number* **bchannel** *channel-number*

Syntax Description

slot/port	Backplane slot number and port number on the interface. See your hardware installation manual for the specific slot and port numbers.
number	Network processor module (NPM) number, in the range 0 through 2.
channel-number	E1 channel number ranging from 1 to 31 or T1 channel number ranging from 1 to 23; 1 to 24 if using NFAS.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

show interfaces virtual-access

To display status, traffic data, and configuration information about a specified virtual access interface, use the **show interfaces virtual-access** command in EXEC mode.

show interfaces virtual-access *number* [**configuration**]

Syntax Description

number	Number of the virtual access interface.
configuration	(Optional) Restricts output to configuration information.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
11.3	The **configuration** keyword was added.

Usage Guidelines

To identify the number of the vty on which the virtual access interface was created, enter the **show users** EXEC command.

Notice The output packet byte counts as reported by the L2TP access server (LAC) to the RADIUS server in the accounting record do not match with those of a client. The following paragraphs describe how the accounting is done, and how you can determine the correct packet byte counts.

Packet counts for client packets in the input path are as follows:

- For packets that are process-switched, virtual access input counters are incremented by the coalescing function by the PPP over Ethernet (PPPoE) payload length.
- For packets that are fast-switched, virtual access input counters are incremented by the fast switching function by the formula:

  PPPoE payload length + PPP addr&cntl bytes = = PPPoE payload length + 2

- For packets that are Cisco Express Forwarding (CEF)-switched, virtual access input counters are incremented by the CEF switching function by the formula:

  IP len + PPP encapbytes (4) = = PPPoE payload length + 2

Packet counts for client packets in the output path are as follows:

- For packets that are process-switched by protocols other than PPP, virtual access output counters are incremented in the upper layer protocol by the entire datagram, as follows:

  Size = = PPPoE payload + PPPoE hdr(6) + Eth hdr(14) + SNAP hdr(10) + media hdr (4 for ATM)

- For packets process-switched by PPP Link Control Protocol (LCP) and Network Control Protocol (NCP), virtual access output counters are incremented by PPP, as follows:

PPP payload size + 4 bytes of PPP hdr

- For packets that are CEF fast-switched, virtual access counters are incremented by the PPPoE payload size.

Accounting is done for PPPoE, PPPoA PTA and L2X as follows:

- For PPPoE PPP Termination Aggregation (PTA), the PPPoE payload length is counted for all input and output packets.
- For PPPoE L2X on a LAC, the PPPoE payload length is counted for all input packets. On an L2TP Network Server (LNS), the payload plus the PPP header (addr + control + type) are counted.
- For PPP over ATM (PPPoA) PTA i/p packets, the payload plus the PPP addr plus cntl bytes are counted. For PPPoA PTA o/p packets, the payload plus PPP addr plus cntl plus ATM header are counted.
- For PPPoA L2X on a LAC for i/p packets, the payload plus PPP addr plus cntl bytes are counted. For PPPoA L2X on a LNS, the payload plus PPP header (addr + control + type) are counted.

Examples

The following is sample output from the **show interfaces virtual-access** command:

```
Router# show interfaces virtual-access 2

Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Ethernet0 (10.0.21.14)
  MTU 1500 bytes, BW 9 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  DTR is pulsed for 0 seconds on reset
  LCP Open
  Open: IPCP
  Last input 00:00:06, output 00:00:05, output hang never
  Last clearing of "show interface" counters 00:14:58
  Input queue: 1/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/64/0 (size/threshold/drops)
     Conversations  0/1 (active/max active)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4 packets input, 76 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     8 packets output, 330 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Table 54 describes the significant fields shown in the display.

Table 54 show interfaces virtual-access Field Descriptions

Field	Description
Virtual-Access ... is {up | down | administratively down}	Indicates whether the interface is currently active (whether carrier detect is present), inactive, or has been taken down by an administrator.
line protocol is {up | down | administratively down}	Indicates whether the software processes that handle the line protocol think the line is usable (that is, whether keepalives are successful).
Hardware is Virtual Access interface	Type of interface. In this case, the interface is a dynamically created virtual access interface existing on a VTY line.
Internet address | interface is unnumbered	IP address, or IP unnumbered for the line. If unnumbered, the output lists the interface and IP address to which the line is assigned (Ethernet0 at 10.0.21.14 in this example).
MTU	Maximum transmission unit for packets on the virtual access interface.
BW	Bandwidth of the virtual access interface in kilobits per second.
DLY	Delay of the virtual access interface in microseconds.
rely	Reliability of the virtual access interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over five minutes.
load	Load on the virtual access interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over five minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to the virtual access interface.
loopback	Test in which signals are sent and then directed back toward the source at some point along the communication path. Used to test network interface usability.
keepalive	Interval set for keepalive packets on the interface. If keepalives have not been enabled, the message is “keepalive not set.”
DTR	Data Terminal Ready. An RS232-C circuit that is activated to let the DCE know when the DTE is ready to send and receive data.
LCP open | closed | req sent	Link control protocol (for PPP only; not for SLIP). LCP must come to the open state before any useful traffic can cross the link.

Table 54 show interfaces virtual-access Field Descriptions (continued)

Field	Description
Open IPCP | IPXCP | ATCP	IPCP is IP control protocol for PPP, IPXCP is IPX control protocol for PPP, ATCP is AppleTalk control protocol for PPP. Network control protocols (NCPs) for the PPP suite. The NCP is negotiated after the LCP opens. The NCP must come into the open state before useful traffic can cross the link.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by a virtual access interface. Useful for knowing when a dead interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by a virtual access interface.
output hang	Number of hours, minutes, and seconds (or never) since the virtual access interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2^{31}ms (and less than 2^{32}ms) ago.
Input queue, drops	Number of packets in input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.
Queueing strategy	Type of queueing selected to prioritize network traffic. The options are first-come-first-serve (FCFS) queueing, weighted fair queueing, priority queueing, and custom queueing.
Output queue	Number of packets in output queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.
Conversations	Number of weighted fair queueing conversations.
Reserved Conversations	Number of reserved weighted fair queueing conversations. The example shows the number of allocated conversations divided by the number of maximum allocated conversations. In this case, there have been 0 reserved conversations.
Five minute input rate, Five minute output rate	Average number of bits and packets transmitted per second in the last five minutes.

Table 54 show interfaces virtual-access Field Descriptions (continued)

Field	Description
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the virtual access interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far end device does not match the checksum calculated from data received. On a LAN, this often indicates noise or transmission problems on the LAN interface or the LAN bus. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs often indicate noise, gain hits or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the virtual access interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on a virtual access interface. This usually indicates a clocking problem between the virtual access interface and the data link equipment.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.

Table 54 show interfaces virtual-access Field Descriptions (continued)

Field	Description
underruns	Number of times that the far-end transmitter has been running faster than the near-end communication server's receiver can handle. This might never be reported on some virtual access interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the virtual access interface being examined. Note that this might not balance with the sum of the enumerated output errors, as some datagrams might have more than one error, and others might have errors that do not fall into any of the tabulated categories.
collisions	Number of packets colliding.
interface resets	Number of times a virtual access interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. This can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a virtual access interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when a virtual access interface is looped back or shut down.
restarts	Number of times the controller was restarted because of errors.
carrier transitions	Number of times the carrier detect (CD) signal of a virtual access interface has changed state. Indicates modem or line problems if the CD line changes state often. If data carrier detect (DCD) goes down and comes up, the carrier transition counter increments two times.
output buffer failures	Number of outgoing packets dropped from the output buffer.
output buffers swapped out	Number of times the output buffer was swapped out.

show ip interface virtual-access

To display network layer IP information about a specified virtual access interface, use the **show ip interface virtual-access** command in EXEC mode.

show ip interface virtual-access *number*

Syntax Description

number	Number of the virtual access interface.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Examples

The following is sample output from the **show ip interface virtual-access** command. This virtual access interface has been configured with a virtual template interface that applies the **ip unnumbered ethernet 0** command.

```
Router# show ip interface virtual-access 1

Virtual-Access1 is up, line protocol is up
  Interface is unnumbered. Using address of Ethernet0 (172.21.114.132)
  Broadcast address is 255.255.255.255
  Peer address is 20.0.0.1
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Outgoing access list is not set
  Inbound  access list is Virtual-Access1#0
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
```

Table 55 describes only the output fields that are significant to virtual access interfaces and that are not described in other IP commands.

Table 55 show ip interface virtual-access Field Descriptions

Field	Description
Virtual-Access1 is up, line protocol is up	Virtual access interface is up and the upper layers consider the line usable.
Interface is unnumbered. Using the address of Ethernet0 (172.21.114.132)	The **ip unnumbered ethernet 0** command was included in the virtual template interface cloned on this interface.

show ip local pool

To display statistics for any defined IP address pools, use the **show ip local pool** command in privileged EXEC mode.

show ip local pool [[*named-address-pool*] | [**group** [*group-name*]]]

Syntax Description

named-address-pool	(Optional) Displays statistics of the named IP address pool.
group	(Optional) Displays statistics of all pools in the base system group.
group [*group-name*]	(Optional) Displays statistics of all pools in the named group.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.1(5)DC	This command was enhanced to allow pool group statistics to be displayed.

Usage Guidelines

If you omit the *named-address-pool* argument, the command displays a generic list of all defined address pools and the IP addresses that belong to them. If you specify the *named-address-pool* argument, the command displays detailed information about that pool.

When you supply the **group** keyword without the associated group name, the command displays all pools in the base system group. When you supply the **group** keyword with the associated group name, the command displays all pools in that group.

Examples

The following is sample output from the **show ip local pool** command when pool groups have not been created:

```
Router# show ip local pool

Scope    Begin           End             Free InUse
Dialin   172.30.228.11   172.30.228.26   16   0
Available addresses:
   172.30.228.12
   172.30.228.13
   172.30.228.14
   172.30.228.15
   172.30.228.16
   172.30.228.17
   172.30.228.18
   172.30.228.19
   172.30.228.20
   172.30.228.21
   172.30.228.22
   172.30.228.23
   172.30.228.24
```

```
   172.30.228.25
   172.30.228.26
   172.30.228.11        Async5

Inuse addresses:
     None
```

The following is sample output from the **show ip local pool** command when pool groups have been created:

```
Router# show ip local pool
 Pool                    Begin           End             Free  In use
 ** pool <p1> is in group <g1>
 p1                      10.1.1.1        10.1.1.10         10       0
                         10.1.1.21       10.1.1.30         10       0
 ** pool <p2> is in group <g2>
 p2                      10.1.1.1        10.1.1.10         10       0
 lcl1                    10.2.2.1        10.2.2.10         10       0
                         10.2.2.21       10.2.2.30         10       0
                         10.2.2.41       10.2.2.50         10       0
 ** pool <mypool> is in group <mygroup>
 mypool                  172.18.184.223  172.18.184.224     2       0
                         172.18.184.218  172.18.184.222     5       0
 ** pool <ccc> is in group <grp-c>
 ccc                     172.18.184.218  172.18.184.220     3       0
 ** pool <bbb> is in group <grp-b>
 bbb                     172.18.184.218  172.18.184.220     3       0
 ** pool <ddd> is in group <grp-d>
 ddd                     172.18.184.218  172.18.184.220     3       0
 ** pool <pp1> is in group <grp-pp>
 pp1                     172.18.184.218  172.18.184.220     2       1
```

The following is sample output from the **show ip local pool** command for the pool group named “mygroup”:

```
Router# show ip local pool mygroup

 Pool                    Begin           End             Free  In use
 ** pool <mypool> is in group <mygroup>
 mypool                  172.18.184.223  172.18.184.224     2       0
                         172.18.184.218  172.18.184.222     5       0
```

The following sample output from the **show ip local pool group** command shows the base system group(lcl1):

```
Router# show ip local pool group

 Pool                    Begin           End             Free  In use
 lcl1                    10.2.2.1        10.2.2.10         10       0
                         10.2.2.21       10.2.2.30         10       0
                         10.2.2.41       10.2.2.50         10       0
```

Table 56 describes the significant fields shown in the displays.

Table 56 show ip local pool Field Descriptions

Field	Description
Scope	The type of access.
Pool	Pool and group names and associations, if created.
Begin	The first IP address in the defined range of addresses in this pool.
End	The last IP address in the defined range of addresses in this pool.
Free	The number of addresses available.
InUse	The number of addresses in use.

Related Commands

Command	Description
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial asynchronous, synchronous, or ISDN point-to-point interfaces.
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

show ip nhrp

To display Next Hop Resolution Protocol (NHRP) mapping information, use the **show ip nhrp** command in user EXEC or privileged EXEC mode.

show ip nhrp [**dynamic** | **incomplete** | **static**] [*address* | *interface*] [**brief** | **detail**] [**purge**]

Syntax Description

dynamic	(Optional) Displays dynamic (learned) IP-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See Table 57 for types, number ranges, and descriptions.
incomplete	(Optional) Displays information about NHRP mapping entries for which the IP-to-NBMA is not resolved. See Table 57 for types, number ranges, and descriptions.
static	(Optional) Displays static IP-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the **ip nhrp map** command. See Table 57 for types, number ranges, and descriptions.
address	(Optional) Displays NHRP mapping entries for specified protocol addresses.
interface	(Optional) Displays NHRP mapping entries for the specified interface. See Table 57 for types, number ranges, and descriptions.
brief	(Optional) Displays a short output of the NHRP mapping.
detail	(Optional) Displays detailed information about NHRP mapping.
purge	(Optional) Displays NHRP purge information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Table 57 lists the valid types, number ranges, and descriptions for the optional *interface* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 57 Valid Types, Number Ranges, and Interface Description

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface

Table 57 Valid Types, Number Ranges, and Interface Description (continued)

Valid Types	Number Ranges	Interface Descriptions
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ip nhrp detail** command:

```
Router# show ip nhrp detail

10.1.1.1/8 via 10.2.1.1, Tunnel1 created 00:46:29, never expire
  Type: static, Flags: used
  NBMA address: 10.12.1.1
10.1.1.2/8 via 10.2.1.2, Tunnel1 created 00:00:12, expire 01:59:47
  Type: dynamic, Flags: authoritative unique nat registered used
  NBMA address: 10.12.1.2
10.1.1.4, Tunnel1 created 00:00:07, expire 00:02:57
  Type: incomplete, Flags: negative
  Cache hits: 4
```

Table 58 describes the significant fields shown in the displays.

Table 58 show ip nhrp Field Descriptions

Field	Description
10.1.1.1/8	Target network.
via 10.2.1.1	Next Hop to reach the target network.
Tunnel1	Interface through which the target network is reached.
created 00:00:12	Length of time since the entry was created (hours:minutes:seconds).

Table 58 show ip nhrp Field Descriptions (continued)

Field	Description
expire 01:59:47	Time remaining until the entry expires (hours:minutes:seconds).
never expire	Indicates that static entries never expire.
Type	• dynamic—NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations. • static—NHRP mapping is configured statically. Entries configured by the **ip nhrp map** command are marked static. • incomplete—The NBMA address is not known for the target network.
NBMA address	Nonbroadcast multiaccess address of the next hop. The address format is appropriate for the type of network being used: ATM, Ethernet, Switched Multimegabit Data Service (SMDS), or multipoint tunnel.
Flags	• authoritative—Indicates that the NHRP information was obtained from the Next Hop Server or router that maintains the NBMA-to-IP address mapping for a particular destination. • implicit—Indicates that the local node learned about the NHRP mapping entries through the source NHRP mapping information from an NHRP resolution request or reply. • local—Indicates NHRP mapping entries that are for networks local to this router (that is, serviced by this router). These flag entries are created when this router answers an NHRP resolution request that has this information and is used to store the tunnel IP address of all the other NHRP nodes to which it has sent this information. If for some reason this router loses access to this local network (that is, it can no longer service this network), it sends an NHRP purge message to all remote NHRP nodes that are listed in the "local" entry (in **show ip nhrp detai**l command output) to tell the remote nodes to clear this information from their NHRP mapping tables. This local mapping entry times out of the local NHRP mapping database at the same time that this information (from the NHRP resolution reply) would time out of the NHRP mapping database on the remote NHRP nodes. • nat—Indicates that the remote node (NHS client) supports the new NHRP NAT extension for dynamic spoke-spoke tunnels to/from spokes behind a NAT router. This marking does not indicate that the spoke (NHS client) is behind a NAT router.

Table 58 show ip nhrp Field Descriptions (continued)

Field	Description
Flags (continued)	• negative—For negative caching, indicates that the requested NBMA mapping could not be obtained. • (no socket)—Indicates that the NHRP mapping entries will not trigger IPsec to set up encryption because data traffic does not need to use this tunnel. Later, if data traffic needs to use this tunnel, the flag will change from a "(no socket)" to a "(socket)" entry and IPsec will be triggered to set up the encryption for this tunnel. Local and implicit NHRP mapping entries are always initially marked as "(no socket)." • registered—Indicates that the mapping entry was created in response to an NHRP registration request. Although registered mapping entries are dynamic entries, they may not be refreshed through the "used" mechanism. Instead, these entries are refreshed by another NHRP registration request with the same Tunnel IP to NBMA IP address mapping. The Next Hop Client (NHC) regularly sends NHRP registration requests to keep these mappings from expiring. • router—Indicates that NHRP mapping entries for a remote router (that is accessing a network or host behind the remote router) are marked with the router flag. • unique—Indicates that an NHRP mapping entry cannot be overwritten by a mapping entry that has the same IP address and a different NBMA address. This prohibition is necessary because the spoke'soutside IP (NBMA) address may change at any time. If the unique flag is set, the spoke has to wait for the mapping entry on the hub to time out before it can register its new (NBMA) mapping. The NHRP registration request packet has the unique flag set by default. • used—Indicates that the mapping entry is being used. The mapping database is checked every 60 seconds. If the used flag is set and more than 120 seconds remain until expire time, the used flag is cleared. If fewer than 120 seconds are left, this mapping entry is refreshed by the transmission of another NHRP resolution request.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp nhs	Displays NHRP Next Hop Server information.
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	Displays NHRP traffic statistics.

show ip route

To display all static IP routes or those installed using the authentication, authorization, and accounting (AAA) route download function, use the **show ip route** command in EXEC mode.

show ip route [*address* [*network-mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**static** [**download**]]

Syntax Description

address	(Optional) The IP address about which routing information should be displayed.
network-mask	(Optional) Network mask that lets you mask network and subnetwork bits.
longer-prefixes	(Optional) The *address* and *mask* pair becomes a prefix, and any routes that match that prefix are displayed.
protocol	(Optional) Name of a routing protocol; or the keyword **connected**, **static**, or **summary**. If you specify a routing protocol, use one of the following keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**.
process-id	(Optional) Arbitrary number assigned to identify a process of the specified protocol.
static	(Optional) All static routes.
download	(Optional) The route installed using the AAA route download function.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
10.3	The *process-id* argument was added.
11.0	The **longer-prefixes** keyword was added.
12.0(3)T	The **static** and **download** keywords were added.

Usage Guidelines

The **show ip route static download** command provides a way to display all dynamic static routes with name and distance information, including active and inactive ones. You can display all active dynamic static routes with both the **show ip route** and **show ip route static** commands after these active routes are added in the main routing table.

Examples

The following examples display all downloaded static routes. A P designates which route was installed using AAA route download.

```
Router# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route
```

```
Gateway of last resort is 172.21.17.1 to network 0.0.0.0

        172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1 20.0.0.0/24 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1

Router# show ip route static

     172.27.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.1.1.1/32 is directly connected, BRI0
P       172.27.4.0/8 [1/0] via 103.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.21.114.65, Ethernet0
S    10.0.0.0/8 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
     172.21.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.21.114.201/32 is directly connected, BRI0
S       172.21.114.205/32 is directly connected, BRI0
S       172.21.114.174/32 is directly connected, BRI0
S       172.21.114.12/32 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
P    10.1.0.0/8 is directly connected, BRI0
P    10.2.2.0/8 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.21.114.65, Ethernet0
S    172.29.0.0/16 [1/0] via 172.21.114.65, Ethernet0
```

The following example shows how to use the **show ip route static download** command to see all active and inactive routes installed using the AAA route download feature:

```
Router# show ip route static download

Connectivity: A - Active, I - Inactive

A    10.0.0.0 255.0.0.0 BRI0
A    11.0.0.0 255.0.0.0 BRI0
A    12.0.0.0 255.0.0.0 BRI0
A    20.0.0.0 255.0.0.0 BRI0
I    21.0.0.0 255.0.0.0 172.21.1.1
I    22.0.0.0 255.0.0.0 Serial0
I    30.0.0.0 255.0.0.0 Serial0
I    31.0.0.0 255.0.0.0 Serial1
I    32.0.0.0 255.0.0.0 Serial1
A    103.0.0.0 255.0.0.0 103.1.1.1
A    103.1.1.1 255.255.255.255 BRI0 200 name remote1
I    104.21.69.0 255.255.255.0 104.21.69.1
```

Related Commands

Command	Description
show dialer	Displays general diagnostic information for interfaces configured for DDR.

show ipx compression

To show the current status and statistics of Internetwork Packet Exchange (IPX) header compression during PPP sessions, use the **show ipx compression** command in EXEC mode.

show ipx compression [**detail** *int-spec*]

Syntax Description

detail	(Optional) Displays detailed link-state database information for NLSP.
int-spec	(Optional) Interface type, as listed in Table 59.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Table 59 lists the supported interface types.

Table 59 Interface Types

Keyword	Description
Async	Asynchronous interface.
Ethernet	Ethernet IEEE 802.3 interface.
Null	Null interface.
Serial	WAN serial interface.

Related Commands

Command	Description
ipx compression cipx	Enables compression of IPX packet headers in a PPP session.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

show ipx spx-protocol

To view the status of the Sequenced Packet Exchange (SPX) protocol stack and related counters, use the **show ipx spx-protocol** command in EXEC mode.

show ipx spx-protocol

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Examples

The following is sample output from the **show ipx spx-protocol** command:

```
Router> show ipx spx-protocol

Next wake time:

SPX socket: 1D90
  state: 0  Connections: 2

   SPX Remote: A001500::0000.c047.ed5a:3A80   Local: ACBB::0000.0000.0001:2010
   state 1  flags 1
   Queue counts:  inq 0,  outQ 0,  unackedQ 0
   Sequence: 34,  Ack: 34,  local-alloc: 39,  remote-alloc: 35
   Abort Timer fires in 24 secs
   Verify Watchdog Timer fires in 3 secs

   SPX Remote: A001500::0000.c047.ed5a:C980   Local: ACBB::0000.0000.0001:2900
   state 1  flags 1
   Queue counts:  inq 0,  outQ 0,  unackedQ 0
   Sequence: 111,  Ack: 55,  local-alloc: 60,  remote-alloc: 112
   Abort Timer fires in 27 secs
   Verify Watchdog Timer fires in 0 secs
```

Table 60 describes significant fields shown in the display.

Table 60 show ipx spx-protocol Field Descriptions

Field	Description
SPX socket:	IPX/SPX socket number.
state	Internal state.
connections:	Number of open connections for this IPX/SPX socket.
SPX Remote: *xxxxxxx::yyyy:zzzz*	The SPX client address for each SPX connection on this IPX/SPX socket, where *xxxx* is the client IPX network number, *yyyy* is the client IPX MAC address, and *zzzz* is the client SPX connection number.

Table 60 show ipx spx-protocol Field Descriptions (continued)

Field	Description
SPX Local *xxxxxxx::yyyy:zzzz*	The local SPX address, where *xxxx* is local IPX network number, *yyyy* is the local IPX MAC address, and *zzzz* is the local SPX connection number.
state	Internal state.
flags	A status bit that is used internally to allow and close connections.
Queue counts	inQ, outQ, and unackedQ, as specified in the following three rows.
inq	Number of SPX packets available for the SPX application to read.
outQ	Number of SPX packets that must be sent to the remote client.
unackedQ	Number of SPX packets sent, but no packet was received by the client, so far.
Sequence:	SPX sequence number. Represents the sequence number of next packet of data to be sent by the router.
Ack:	SPX acknowledgment number. Represents the sequence number of the client's packet that the router has received, so far.
local-alloc:	Maximum packet sequence number that is acceptable from the client. This is a method of imposing flow control on the NASI client.
remote-alloc:	Maximum packet sequence number that the NASI client can accept from the router. This is the NASI client's way of imposing flow control on the router.
Purge Timer	Time in seconds until this SPX connection is closed and deleted from the list.
Abort Timer	Time in seconds until this SPX connection is closed and deleted if a watchdog packet is not received.
Verify Watchdog Timer fires in X secs	Indicates the time when you last sent a watchdog packet to the client.

Related Commands

Command	Description
aaa authentication nasi	Specifies AAA authentication for NASI clients connecting through the access server.
ipx nasi-server enable	Enables NASI clients to connect to asynchronous devices attached to a router.
nasi authentication	Enables AAA authentication for NASI clients connecting to a router.
show ipx nasi connections	Displays the status of NASI connections.

show isdn

To display the information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels, use the **show isdn** command in EXEC mode.

show isdn {**active** [*dsl* | *serial number*] | **history** [*dsl* | *serial number*] | **memory** | **service** [*dsl* | *serial number*] | **status** [*dsl* | *serial number*] | **timers** [*dsl* | *serial number*]}

Syntax Description

active [*dsl* | *serial number*]	Displays current call information of all ISDN interfaces or, optionally, a specific digital subscriber line (DSL) or a specific ISDN PRI interface (created and configured as a serial interface). Values of *dsl* range from 0 to 15. Information displayed includes the called number, the remote node name, the seconds of connect time, the seconds of connect time remaining, the seconds idle, and Advice of Charge (AOC) charging time units used during the call.
history [*dsl* | *serial number*]	Displays historic and current call information of all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of *dsl* range from 0 to 15. Information displayed includes the called number, the remote node name, the seconds of connect time, the seconds of connect time remaining, the seconds idle, and AOC charging time units used during the call.
memory	Displays ISDN memory pool statistics. This keyword is for use by technical development staff only.
service [*dsl* | *serial number*]	Displays the service status of all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of *dsl* range 0 to 15.
status [*dsl* | *serial number*]	Displays the status of all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of *dsl* range 0 to 15.
timers [*dsl* | *serial number*]	Displays the values of Layer 2 and Layer 3 timers for all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of *dsl* range from 0 to 15.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Examples

The following is an output example from the **show isdn** command with the **active** keyword:

```
Router# show isdn active

------------------------------------------------------------------------------
                              ISDN ACTIVE CALLS
------------------------------------------------------------------------------
History Table MaxLength = 100 entries
History Retain Timer = 15 Minutes
------------------------------------------------------------------------------
Call Calling and Called  Remote Node  Seconds  Seconds  Seconds Recorded Charges
Type Phone Number        Name         Used     Left     Idle    Units/Currency
------------------------------------------------------------------------------
In +---Not Available----    aerocore   684802  +499598     401
In +---Not Available----         pmg   363578  +499503     496
In +---Not Available----      solpro   253232  +499325     674
In +---Not Available----               194047  +499965      34
In +---Not Available----       taber   189165  +499841     158
In +---Not Available----        newt   110342                0
In +---Not Available----                 2603  +499997       2
In +---Not Available----                 1310  +499798     201


------------------------------------------------------------------------------
```

The following is an output example from the **show isdn** command with the **history** keyword:

```
Router# show isdn history

------------------------------------------------------------------------------
                              ISDN CALL HISTORY
------------------------------------------------------------------------------
History Table MaxLength = 100 entries
History Retain Timer = 15 Minutes
------------------------------------------------------------------------------
Call Calling and Called  Remote Node  Seconds  Seconds  Seconds Recorded Charges
Type Phone Number        Name         Used     Left     Idle    Units/Currency
------------------------------------------------------------------------------
In +---Not Available----    aerocore   684818  +499583     416
In +---Not Available----         pmg   363593  +499488     511
In +---Not Available----      solpro   253248  +499310     689
In +---Not Available----               194062  +499950      49
In +---Not Available----       taber   189180  +499826     173
In +---Not Available----        newt   110357                0
In +---Not Available          a45968     5244
In +---Not Available----                 2619  +499997       0
In +---Not Available----       zetta     1432
In +---Not Available----                 1325  +499783     216
In +---Not Available----         trf      161


------------------------------------------------------------------------------
```

Table 61 describes the fields in the **show isdn active** and **show isdn history** output displays.

Table 61 show isdn active and show isdn history Field Descriptions

Field	Description
History Table MaxLength	Maximum number of entries that can be retained in the Call History table.
History Retain Timer	Maximum amount of time any entry can be retained in Call History table.
Call Type	Type of call: In for incoming, Out for outgoing, or -- when direction of call cannot be determined.
Calling and Called Phone Number	For incoming calls, the number from which the call was received. For outgoing calls, the number to which the call was placed, or +---Not Available---- when a phone number is not available. The phone number display is limited to 20 digits. (+---Not Available---- is the truncated version of ----Not Available----. The + in the field means more data is available than can be displayed. The low-order data is displayed and the overflowing data is replaced by a +.)
Remote Node Name	Name of the host placing the call or the host called. The name display is limited to ten characters.
Seconds Used	Six digits (999999) of seconds showing connect time used, or Failed when the connection attempt fails.
Seconds Left	Six digits (999999) of seconds of connect time remaining (when configured through the **dialer idle-timeout** command. The + in the field means more data is available than can be displayed. The low-order data is displayed and the overflowing data is replaced by a +.)
Seconds Idle	Six digits (999999) of seconds since the last interesting packet.
Recorded Charges Units/Currency	For outgoing calls, number of ISDN AOC charging units used or the currency cost of the call. Currency information display is limited to ten characters.

The following output example shows the output of the **show isdn** command with the **service** keyword when PRI is configured on a T1 controller:

```
Router# show isdn service

PRI Channel Statistics:
ISDN Se0:15, Channel (1-31)
  Activated dsl 8
  State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
  Channel (1-31) Service (0=Inservice 1=Maint 2=Outofservice)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

Table 63 describes the significant fields shown in the display.

Table 62 show isdn service Field Descriptions

Field	Description
ISDN Se1/0:15	ISDN PRI interface corresponding to serial interface 1/0:15.
Channel (1-31)	Channel range “1-31” is a standard format for both T1 and E1 outputs, but the state value shown identifies whether the channel is used.
Activated dsl 8	The digital signal link (DSL) value is 8.
State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint)	Current state of each channel. Channels 24 through 31 are marked as reserved when the output is from T1.
Channel (1-31) Service (0=Inservice 1=Maint 2=Outofservice)	Service state assigned to each channel. Channel 24 is marked as out of service.[1]

1. If channel 24 (marked as out of service) is configured as the NFAS primary D channel, NFAS will roll over to the backup D channel if one is configured. If channel 24 is a B channel, it will not accept calls.

The following is sample output from the **show isdn** command with the **service** keyword when PRI is configured on a T1 controller:

```
Router# show isdn service

PRI Channel Statistics:
ISDN Se0:15, Channel (1-31)
  Activated dsl 8
  State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0
  Channel (1-31) Service (0=Inservice 1=Maint 2=Outofservice)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

Table 63 describes the significant fields shown in the **show isdn service** display.

Table 63 show isdn service Field Descriptions

Field	Description
ISDN Se1/0:15	ISDN PRI interface corresponding to serial interface 1/0:15.
Channel (1-31)	Channel range “1-31” is a standard format for both T1 and E1 outputs, but the state value shown identifies whether the channel is used.
Activated dsl 8	The DSL value.
State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint)	Current state of each channel. Channels 24 through 31 are marked as reserved when the output is from T1.
Channel (1-31) Service (0=Inservice 1=Maint 2=Outofservice)	Service state assigned to each channel. Channel 24 is marked as out of service.[1]

1. If channel 24 (marked as out of service) is configured as the NFAS primary D channel, NFAS will roll over to the backup D channel if one is configured. If channel 24 is a B channel, it will not accept calls.

The following is sample output from the **show isdn** command with the **status** keyword when no calls are active for a Cisco 4500 router with eight BRIs and one E1 PRI:

```
Router# show isdn status

Global ISDN Switchtype = basic-5ess
ISDN BRI0 interface
        dsl 0, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
ISDN BRI1 interface
        dsl 1, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 1 CCBs = 0
ISDN BRI2 interface
        dsl 2, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 2 CCBs = 0
ISDN BRI3 interface
        dsl 3, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 75, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 3 CCBs = 0
ISDN BRI4 interface
        dsl 4, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 4 CCBs = 0
ISDN BRI5 interface
        dsl 5, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 5 CCBs = 0
ISDN BRI6 interface
        dsl 6, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        DEACTIVATED
```

```
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 6 CCBs = 0
ISDN BRI7 interface
        dsl 7, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 7 CCBs = 0
ISDN Serial0:15 interface
        dsl 8, interface ISDN Switchtype = primary-ni
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 8 CCBs = 0
    Total Allocated ISDN CCBs = 0
```

The following is sample output from the **show isdn** command with the **status** keyword, with one active call:

```
Router# show isdn status

The current ISDN Switchtype = ntt
ISDN BRI0 interface
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 64, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        1 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 1
        CCB:callid=8003, callref=0, sapi=0, ces=1, B-chan=1
    Number of active calls = 1
    Number of available B-channels = 1
    Total Allocated ISDN CCBs = 1
```

Table 64 describes the significant fields shown in the **show isdn status** display.

Table 64 show isdn status Field Descriptions

Field	Description
Layer 1 Status	
ACTIVE	Status of ISDN Layer 1.
Layer 2 Status	
TEI = 64, State = MULTIPLE_FRAME_ESTABLISHED	Status of ISDN Layer 2. Terminal endpoint identifier number and multiframe structure state.
Layer 3 Status	
1 Active Layer 3 Call(s)	Number of active calls.

Table 64 show isdn status Field Descriptions (continued)

Field	Description
Activated dsl 0 CCBs =	Number of the DSL activated. Number of call control blocks in use.
CCB:callid=8003, callref=0, sapi=0, ces=1, B-chan=1	Information about the active call.
Number of active calls =	Number of active calls.
Number of available B-channels =	Number of B channels that are not being used.
Total Allocated ISDN CCBs =	Number of ISDN call control blocks that are allocated.

The following is sample output from the **show isdn** command with the **timers** keyword:

```
Router# show isdn timers

ISDN Serial0:23 Timers (dsl 0) Switchtype = primary-5ess
        ISDN Layer 2 values
         K     =   7 outstanding I-frames
         N200  =   3 max number of retransmits
         T200  =   1.000 seconds
         T202  =   2.000 seconds
         T203  =  30.000 seconds
        ISDN Layer 3 values
         T303  =   4.000 seconds
         T304  =  20.000 seconds
         T305  =   4.000 seconds
         T306 =  30.000 seconds
         T307 = 180.000 seconds
         T308  =   4.000 seconds
         T309    Disabled
         T310 =  30.000 seconds
         T313 =   4.000 seconds
         T316  = 120.000 seconds
         T318  =   4.000 seconds
         T319  =   4.000 seconds
         T322  =   4.000 seconds
         T3OOS =   5.000 seconds
         TGUARD=   8.000 seconds, Expiry = REJECT_CALL
    ISDN Serial1:23 Timers (dsl 1) Switchtype = primary-5ess
        ISDN Layer 2 values
         K     =   7 outstanding I-frames
         N200  =   3 max number of retransmits
         T200  =   1.000 seconds
         T202  =   2.000 seconds
         T203  =  30.000 seconds
        ISDN Layer 3 values
         T303  =   4.000 seconds
         T304  =  20.000 seconds
         T305  =   4.000 seconds
         T306 =  30.000 seconds
         T307 = 180.000 seconds
         T308  =   4.000 seconds
         T309    Disabled
         T310 =  30.000 seconds
         T313 =   4.000 seconds
         T316  = 120.000 seconds
         T318  =   4.000 seconds
         T319  =   4.000 seconds
```

```
          T322  =   4.000 seconds
          T3OOS =   5.000 seconds
          TGUARD=   8.000 seconds, Expiry = REJECT_CALL
         *** dsl 2 is not configured
         *** dsl 3 is not configured
         *** dsl 4 is not configured
         *** dsl 5 is not configured
         *** dsl 6 is not configured
         *** dsl 7 is not configured
ISDN BRI0 Timers (dsl 0) Switchtype = basic-net3
         ISDN Layer 2 values
          K    = 1   outstanding I-frames
          N200 = 3   max number of retransmits
          N202 = 2   max number of retransmits of TEI ID Request
          T200 = 1   seconds
          T202 = 2   seconds
          T203 = 10  seconds
         ISDN Layer 3 values
          T303 = 4   seconds
          T305 = 30   seconds
          T308 = 4   seconds
          T310 = 40  seconds
          T313 = 4   seconds
          T316 = 0 seconds
          T318 = 4   seconds
          T319 = 4   seconds
```

Table 65 and Table 66 show typical and default values of the timers shown in the **show isdn timers** display. The values of the timers depend on the switch type. The Cisco routers support the following switch type keywords: **basic-ni**, **basic-net3**, **primary-5ess**, and **basic-qsig** and **primary-qsig**. Refer to the Q.921 specifications for detailed technical definitions of the Layer 2 timers; refer to the Q.931 specifications for detailed technical definitions of the Layer 3 timers.

Table 65 show isdn timers Layer 2 Command Output

Timer Number Field	System Parameter (typical)
K = 7 outstanding I-frames	None
N200 = 3 max number of retransmits	3 seconds
T200 = 1.000 seconds	1 second
T202 = 2.000 seconds	2 seconds
T203 = 30.000 seconds	10 seconds

Table 66 show isdn timers Layer 3 Command Output

Timer Number Field	Network Side ITU Default Value	User Side ITU Default Value
T303 = 4.000 seconds	4 seconds	4 seconds
T304 = 20.000 seconds	20 seconds	30 seconds
T305 = 4.000 seconds	30 seconds	30 seconds
T306 = 30.000 seconds	30 seconds	None
T307 = 180.000 seconds	180 seconds (3 minutes)	None
T308 = 4.000 seconds	4 seconds	4 seconds
T309 Disabled	90 seconds	90 seconds

Table 66 show isdn timers Layer 3 Command Output (continued)

Timer Number Field	Network Side ITU Default Value	User Side ITU Default Value
T310 = 30.000 seconds	10 seconds	30 to 120 seconds
T313 = 4.000 seconds	None	4 seconds
T316 = 120.000 seconds	120 seconds (2 minutes)	120 seconds (2 minutes)
T318 = 4.000 seconds	None	4 seconds
T319 = 4.000 seconds	None	4 seconds
T322 = 4.000 seconds	4 seconds	4 seconds
T3OOS = 5.000 seconds	Time interval after which the software should attempt to recover from a Layer 2 failure. Default is 5 seconds	Time interval after which the software should attempt to recover from a Layer 2 failure. Default is 5 seconds
TGUARD = 8.000 seconds, Expiry = REJECT_CALL	Managed timer for authentication requests configured with the **isdn guard-timer** command. Default is 8 seconds.	Managed timer for authentication requests configured with the **isdn guard-timer** command. Default is 8 seconds.

show isdn nfas group

To display all the members of a specified NFAS group or all Non-Facility Associated Signaling (NFAS) groups, use the **show isdn nfas group** command in privileged EXEC mode.

show isdn nfas group [*id-number*]

Syntax Description

id-number	(Optional) Identifier number in the range from 1 to 24 of a specific NFAS group.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following is sample output from the **show isdn nfas group** command:

```
Router# show isdn nfas group 1

ISDN NFAS GROUP 1 ENTRIES:

The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.

There are 3 total nfas members.
There are 93 total available B channels.
The primary D-channel is DSL 0 in state INITIALIZED.
The backup D-channel is DSL 1 in state INITIALIZED.
The current active layer 2 DSL is 1.
```

The following three examples show the D channel state changes when rollover occurs from the primary NFAS D channel to the backup D channel. The first example shows the output with the primary D channel in service and the backup D channel in standby.

```
Router# show isdn nfas group 0

ISDN NFAS GROUP 0 ENTRIES:

The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.

There are 3 total nfas members.
There are 70 total available B channels.
The primary D-channel is DSL 0 in state IN SERVICE.
The backup D-channel is DSL 1 in state STANDBY.
The current active layer 2 DSL is 0.
```

The following example shows the output during rollover. The configured primary D channel is in maintenance busy state and the backup D channel is waiting.

```
Router# show isdn nfas group 0
```

```
ISDN NFAS GROUP 0 ENTRIES:
The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.

There are 3 total nfas members.
There are 70 total available B channels.
The primary D-channel is DSL 0 in state MAINTENANCE BUSY.
The backup D-channel is DSL 1 in state WAIT.
The current active layer 2 DSL is 1.
```

The following example shows the output when rollover is complete. The configured primary D channel is now in standby and the backup D channel is in service.

```
Router# show isdn nfas group 0

ISDN NFAS GROUP 0 ENTRIES:

The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.

There are 3 total nfas members.
There are 70 total available B channels.
The primary D-channel is DSL 0 in state STANDBY.
The backup D-channel is DSL 1 in state IN SERVICE.
The current active layer 2 DSL is 1.
```

Table 67 describes the significant fields shown in the display.

Table 67 show isdn nfas group Field Descriptions

Field	Description
The primary D is Serial1/0:23.	Identifies the primary D channel.
The backup D is Serial1/1:23.	Identifies the backup D channel.
The NFAS member is Serial2/0:23.	Identifies the NFAS group.
There are 3 total nfas members.	Number of member interfaces in the group.
There are 70 total available B channels.	Number of B channels in this NFAS group.
The primary D-channel is DSL 0 in state STANDBY.	Service state of the NFAS primary D channel; this D channel is in service.
The backup D-channel is DSL 1 in state IN SERVICE.	Service state of the NFAS backup D channel; this D channel is in service. The states are IN SERVICE, STANDBY, OUT OF SERVICE, MAINTENANCE, WAIT, INITIALIZED, and BUSY.
The current active layer 2 DSL is 1.	Digital subscriber loop (DSL) identifier assigned by the service provider. If both D channels are out of service, the value displayed in this line is 1.

Related Commands

Command	Description
show isdn	Displays the information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels.

show isdn service

To display the service status of each ISDN channel, use the **show isdn service** command in privileged EXEC mode.

show isdn service

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following example shows channel statistics on a PRI configured on a T1 controller:

```
Router# show isdn service

PRI Channel Statistics:
ISDN Se0:15, Channel (1-31)
  Activated dsl 8
  State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
  Channel (1-31) Service (0=Inservice 1=Maint 2=Outofservice)
  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

Table 68 describes the significant fields shown in the display.

Table 68 show isdn service Field Descriptions

Field	Description
ISDN Se1/0:23	ISDN PRI interface corresponding to serial interface 1/0:23.
Channel (1-31)	Channel range “1-31” is a standard format for both T1 and E1 outputs, but the state value shown identifies whether the channel is used.
Activated dsl 0	The digital signal link (DSL) value is 0.
State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint)	Current state of each channel. Channels 24 through 31 are marked as reserved when the output is from T1.
Channel (1-31) Service (0=Inservice 1=Maint 2=Outofservice)	Service state assigned to each channel. Channel 24 is marked as out of service. [1]

1. If channel 24 (marked as out of service) is configured as the NFAS primary D channel, NFAS will roll over to the backup D channel if one is configured. If channel 24 is a B channel, calls will not be accepted to it.

Related Commands

Command	Description
show isdn	Displays the information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels.

show line async-queue

To display the status of connections currently waiting in the queue, use the **show line async-queue** command in EXEC mode.

show line async-queue [*rotary-group*]

Syntax Description

rotary-group	(Optional) Specifies a rotary group.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Use this command to display all rotary line queues.

Examples

The following example shows all lines that are currently queued:

```
Router# show line async-queue

Showing async-queue for ALL rotary groups

Queue for Rotary Group 1:
    Pos    Waiting TTY    Dest Port    Source Host   Waiting Time
      1          tty69         7001       10.2.1.3       00:00:09
      2          tty70         7001       10.2.1.3       00:00:06


Queue for Rotary Group 2:
    Pos    Waiting TTY    Dest Port    Source Host   Waiting Time
      1          tty66         7002       10.2.1.3       00:00:36
      2          tty67         7002       10.2.1.3       00:00:29
      3          tty68         7002       10.2.1.3       00:00:26


Lines which have queuing enabled [tty (group)]:
tty33 (1)  tty34 (1)  tty35 (1)  tty36 (1)  tty37 (2)
tty38 (2)  tty39 (2)  tty40 (2)  tty41 (3)  tty42 (3)
tty43 (3)  tty44 (3)  tty45 (4)  tty46 (4)  tty47 (4)
Router#
```

Note that Waiting TTY may also be displayed as Waiting VTY and is equivalent.