show access-expression

To display the defined input and output access list expressions, use the **show access-expression** command in privileged EXEC mode.

show access-expression [**begin** | **include** | **exclude**]

Syntax Description

begin	(Optional) Begin with the access list expression that matches.
include	(Optional) Include access list expressions that match.
exclude	(Optional) Exclude access list expressions that match.

Defaults

Displays all input and output access list expressions.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

```
Router# show access-expression
Router# Interface TokenRing0/0:
        Input:(dmac(701) | ~lsap(202))
```

See the **access-expression** command for a description of the access expressions.

Related Commands

Command	Description
access-expression	Defines an access expression.

show alps ascu

To display the status of the Airline Product Set (ALPS) agent-set control unit (ASCU), use the **show alps ascu** command in user EXEC or privileged EXEC mode.

show alps ascu [*interface* [*id*]] [**detailed**]

Syntax Description

interface	(Optional) Combined interface and ASCU interchange address (IA). • If the interface and ASCU are specified, the status for the ASCU on that interface is displayed. • If the interface is specified, then all ASCUs defined on that interface are displayed. • If the interface and ASCU are not specified, then all ASCUs defined are displayed.
id	(Optional) id number of the interface.
detailed	(Optional) Displays detailed output.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(5)T	The output of this command was modified.
12.1(2)T	The output for the **detailed** version of this command was modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2 SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 The *interface* and *id* arguments are not supported in this release.

Examples

The following is sample output from the **show alps ascu** command:

```
Router# show alps ascu

interface  dlc id a1 a2 circuit        pkt_tx      pkt_rx      state
-------------------------------------------------------------------
Serial1/2  ALC 5F 41 42 MATIP-ALC      0           0           DOWN
Serial1/3  UTS 21 23 4A MATIP          0           0           DOWN
Serial1/6  ALC 5F 41 45 MATIP-ALC      0           0           DOWN
Serial1/6  ALC 6F 41 44 MATIP-ALC      0           0           DOWN
Total number of ASCUs: 4
Total number of up ASCUs: 0
```

The following is sample output from the **show alps ascu detailed** command for ASCUs 4F and 6F on serial interface 1/6:

```
Router# show alps ascu detailed

ascu 4F on i/f Serial1/6, dlc = ALC, state = UP
  default-circuit = MATIP-ALC, a1 = 41, a2 = 45
  max_msg_len = 962, retry_option = none, alias = 6F
  err_disp_terminal = 114, err_disp_line = 102
  pkt_tx = 0, byte_tx = 0, pkt_rx = 0, byte_rx = 0
  bad_CCC = 0, garbledMsgs = 0, T1Timeouts = 0

ascu 6F on i/f Serial1/6, dlc = ALC, state = DOWN
  default-circuit = MATIP-ALC, a1 = 41, a2 = 44
  max_msg_len = 962, retry_option = none
  err_disp_terminal = 114, err_disp_line = 102
  pkt_tx = 0, byte_tx = 0, pkt_rx = 0, byte_rx = 0
  bad_CCC = 0, garbledMsgs = 0, T1Timeouts = 14
```

Table 17 describes the significant fields in the display.

Table 17 show alps ascu Field Descriptions

Field	Description
dlc	Data link control.
state	Status of connection; UP, DOWN, or DISABLED.
default-circuit	Name of the default circuit.
a1	Logical ASCU identification information for A1.
a2	Logical ASCU identification information for A2.
max_msg_len	Maximum input message length. Protocol level count that includes all protocol overhead plus data. The valid range is from 1 to 3840 bytes. The default is 962 bytes. Anything over the maximum is discarded and the interface giant counter is incremented. This does not apply to the GarbledMsg for the ASCU.
retry_option	Retry option. When a message with a bad cycle check character (CCC) is received from an ASCU, a retry option can be configured using the **alps retry-option** command. The retry option configures the customer premises equipment (CPE) to send a message to the ASCU. The following retry options are available: • resend—Indicator LED signals the operator at the ASCU to resend data. • reenter—Service messages signal the operator at the ASCU to reenter data. The default retry option is no retry.
alias	Parent ASCU interchange address to which this nonpolling automatic level control (ALC) ASCU is aliased.
err_disp_terminal	Terminal address to which error service messages are sent.
err_disp_line	Screen line number where error service messages are sent.
pkt_tx	Packets sent.
byte_tx	Bytes sent.
pkt_rx	Packets received.
byte_rx	Bytes received.

Table 17 show alps ascu Field Descriptions (continued)

Field	Description
bad_CCC	Number of bad CCCs. Bad CCCs occurs due to the following reasons: • The proper control characters were received. • The characters did not exceed the maximum length. • The CCC calculation fails.
garbledMsgs	Number of garbled messages. Garbled messages are a result of a range of different errors, including the following: • An unexpected character is received. • The maximum interface buffer size is exceeded. • The maximum message length is exceeded.
T1Timeouts	Number of response timeouts.

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.

show alps circuits

To display the status of the Airline Product Set (ALPS) circuits, use the **show alps circuits** command in user EXEC or privileged EXEC mode.

show alps circuits [**peer** *ip-address*] [**name** *name*] [**detailed**]

Syntax Description

peer *ip-address*	(Optional) Displays the status of the circuits connected to the specified peer.
name *name*	(Optional) Displays the status of the specified circuit.
detailed	(Optional) Displays the detailed output.

Command Default

If a circuit name is specified, then the status of that circuit will be displayed; otherwise, the status of all circuits will be displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3T	This command was introduced.
12.0(5)T	The output was modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2 SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show alps circuits** command:

```
Router# show alps circuits

name         pri_peer        curr_peer       dlc   state  pkt_tx     pkt_rx
------------------------------------------------------------------------------
CKT1         172.18.60.201   0.0.0.0         NONE  DISC   0          0
CKT2         172.18.60.201   0.0.0.0         NONE  DISC   0          0
MATIP        10.100.1.2      0.0.0.0         UTS   DISC   0          0
MATIP-ALC    10.100.1.2      0.0.0.0         ALC   INOP   0          0
Total number of circuits: 4
Total number of connected circuits: 0
```

The following is sample output from the **show alps circuits name detailed** command:

```
Router# show alps circuit name matip-alc detailed

MATIP-ALC: dlc = ALC, conn_type = PERM, state = INOP, uptime = 00:00:00
  down reason = noReason
  pri_peer = 10.100.1.2, sec_peer = 0.0.0.0
```

```
  curr_peer = 0.0.0.0,
  local_hld = 4D02, remote_hld = 7F7F
  emtox: hostlink = 255, x121 = 1234
  lifetime_tmr = 4, idle_tmr = 60, retry_tmr = 30
  pkt_tx = 0, byte_tx = 0, pkt_rx = 0, byte_rx = 0
  src_corr = 0, dst_corr = 0
  drops_q_overflow = 0, drops_ckt_disabled = 0
  drops_lifetime_tmr = 0, drops_invalid_ascu = 0
  ascus: (41,42)U, (41,44)U, (41,45)U
Total number of ASCUs: 3
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.

show alps peers

To display the status of the Airline Product Set (ALPS) partner peers, use the **show alps peers** command in user EXEC or privileged EXEC mode.

show alps peers [**ipaddress** *address*] [**detailed**] [**name** *name*]

Syntax Description

ipaddress *address*	(Optional) Displays the status of the specified agent-set control unit (ASCU).
detailed	(Optional) Displays the detailed output.
name *name*	(Optional) Displays the circuit name.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(5)T	The output was modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2 SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 The **name** keyword *name* argument are not supported in this release

Usage Guidelines

If an IP address is specified, then only the status of that peer will be displayed; otherwise, the status of all peers will be displayed.

Examples

The following is sample output from the **show alps peers detailed** command:

```
Router# show alps peers detailed

TCP:10.227.50.106, conn_id = MATIP_A_CKT-2
   protocol = MATIP_A, fport = 350, lport = 11592
   type = DYN, create = ADMIN, state = OPENED, uptime = 00:00:53
   down reason = unknown
   pkt_tx = 1071, byte_tx = 37264, pkt_rx = 1066, byte_rx = 36010
   Drops:giants = 0, q_overflow = 0, peer_down = 0, ver_mismatch = 0
```

Related Commands

Command	Description
alps primary-peer	Specifies the primary TCP peer and, optionally, a backup TCP peer for this ALPS circuit.
alps remote-peer	Specifies the partner IP address.

show bridge

To display classes of entries in the bridge forwarding database, use the **show bridge** command in privileged EXEC mode.

show bridge [*bridge-group*] [*interface*] [*address* [*mask*]] [**verbose**]

Syntax Description

bridge-group	(Optional) Number that specifies a particular spanning tree.
interface	(Optional) Specific interface, such as Ethernet 0.
address	(Optional) 48-bit canonical (Ethernet ordered) MAC address. This may be entered with an optional mask of bits to be ignored in the address, which is specified with the *mask* argument.
mask	(Optional) Bits to be ignored in the address. You must specify the *address* argument if you want to specify a mask.
verbose	(Optional) Displays additional detail, including any Frame Relay data-link connection identifier (DLCI) associated with a station address.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.0	The **verbose** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The **verbose** keyword first appeared in Cisco IOS Release 11.0.

The following are possible variations of the **show bridge** command:

```
show bridge ethernet 0
show bridge 0000.0c00.0000 0000.00FF.FFFF
show bridge 0000.0c00.0e1a
show bridge
show bridge verbose
```

In the sample output, the first command would display all entries for hosts reachable via Ethernet interface 0, the second command would display all entries with the vendor code of 0000.0c00.0000, and the third command would display the entry for address 0000.0c00.0e1a. In the fourth command, all entries in the forwarding database would be displayed. The fifth command provides additional detail. In all five lines, the bridge group number has been omitted.

Examples

The following is sample output from the **show bridge** command. The second display is output from the **show bridge** command with the **verbose** argument.

```
Router# show bridge

Total of 300 station blocks, 280 free
Codes: P - permanent, S - self

Bridge Group 32:Bridge Group 32:

    Address       Action   Interface       Age   RX count   TX count
0180.c200.0000   receive       -            S           0          0
ffff.ffff.ffff   receive       -            S           0          0
0900.2b01.0001   receive       -            S           0          0
0300.0c00.0001   receive       -            S           0          0
0000.0c05.1000   forward   Ethernet0/1      4           1          0
0000.0c04.4b5b   receive       -            S           0          0
0000.0c04.4b5e   receive       -            S           0          0
0000.0c04.4b5d   receive       -            S           0          0
0000.0c04.4b5c   receive       -            S           0          0
0000.0c05.4a62   forward   Ethernet0/1      4           1          0
aa00.0400.2108   forward   Ethernet0/1      0          42          0
0000.0c12.b888   forward   Ethernet0/2      4           1          0
0000.0c12.b886   forward   Ethernet0/1      4           1          0
aa00.0400.4d09   forward   Ethernet0/1      4           1          0
0000.0c06.fb9a   forward   Ethernet0/1      4           1          0
0000.0c04.b039   forward   Ethernet0/1      4           1          0

Router# show bridge verbose

Total of 300 station blocks, 287 free
Codes: P - permanent, S - self

BG Hash      Address      Action Interface     DLCI   Age RX count   TX count
32 00/0   0180.c200.0000 receive      -           -     S           0          0
32 00/1   ffff.ffff.ffff receive      -           -     S           0          0
32 01/0   0900.2b01.0001 receive      -           -     S           0          0
32 01/1   0300.0c00.0001 receive      -           -     S           0          0
32 10/0   0000.0c04.4b5b receive      -           -     S           0          0
32 15/0   0000.0c04.4b5e receive      -           -     S           0          0
32 16/0   0000.0c04.4b5d receive      -           -     S           0          0
32 17/0   0000.0c04.4b5c receive      -           -     S           0          0
32 29/0   aa00.0400.2108 forward  Ethernet0/1     -     0          48          0
32 30/0   0000.0c12.b888 forward  Ethernet0/2     -     0           1          0
32 A4/0   0800.2002.ff5b forward  Ethernet0/1     -     0           6          0
32 E2/0   aa00.0400.e90b forward  Ethernet0/1     -     0          65          0
32 F2/0   0000.0c04.b042 forward  Ethernet0/2     -     3           2          0
```

Table 18 describes the significant fields shown in the display.

Table 18 show bridge Field Descriptions

Field	Description
Total of 300 station blocks	Total number of forwarding database elements in the system. The memory to hold bridge entries is allocated in blocks of memory sufficient to hold 300 individual entries. When the number of free entries falls below 25, another block of memory sufficient to hold another 300 entries is allocated. Therefore, the size of the bridge forwarding database is limited to the amount of free memory in the router.
295 free	Number in the free list of forwarding database elements in the system. The total number of forwarding elements is expanded dynamically, as needed.
BG	Bridging group to which the address belongs.
Hash	Hash key/relative position in the keyed list.
Address	Canonical (Ethernet ordered) MAC address.
Action	Action to be taken when that address is looked up; choices are to discard or forward the datagram.
Interface	Interface, if any, on which that address was seen.
Age	Number of minutes since a frame was received from or sent to that address. The letter “P” indicates a permanent entry. The letter “S” indicates the system as recorded by the router. On the modular systems, this is typically the broadcast address and the router’s own hardware address; on the IGS, this field will also include certain multicast addresses.
RX count	Number of frames received from that address.
TX count	Number of frames forwarded to that address.

show bridge circuit-group

To display the interfaces configured in each circuit group and show whether they are currently participating in load distribution, use the **show bridge circuit-group** command in user EXEC or privileged EXEC mode.

show bridge [*bridge-group*] **circuit-group** [*circuit-group*] [*src-mac-address*] [*dst-mac-address*]

Syntax Description

bridge-group	(Optional) Number that specifies a particular bridge group.
circuit-group	(Optional) Number that specifies a particular circuit group.
src-mac-address	(Optional) 48-bit canonical (Ethernet ordered) source MAC address.
dst-mac-address	(Optional) 48-bit canonical (Ethernet ordered) destination MAC address.

Command Modes

User EXEC
Prvileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from various **show bridge circuit-group** command strings:

```
Router# show bridge circuit-group

Bridge group 1 Circuit group 1:
    Interface Serial0 : inserted, learning, forwarding
    Interface Serial3 : inserted, learning, forwarding
Bridge group 1 Circuit group 2:
    Interface Serial2 : inserted, learning, forwarding

Router# show bridge 1 circuit-group 1

Bridge group 1 Circuit group 1:
    Interface Serial0 : inserted, learning, forwarding
    Interface Serial3 : inserted, learning, forwarding

Router# show bridge 1 circuit-group 2

Bridge group 1 Circuit group 2:
    Interface Serial2 : inserted, learning, forwarding

Router# show bridge 1 circuit-group 1 0000.6502.23EA 0000.1234.4567

Output circuit group interface is Serial3

Router# show bridge 1 circuit-group 1 0000.6502.23EA
```

```
%Destination MAC address required

Router# show bridge 1 circuit-group 1

Bridge group 1 Circuit group 1:
    Transmission pause interval is 250ms
    Output interface selection is source-based
    Interface Serial0 : inserted, learning, forwarding
    Interface Serial3 : inserted, learning, forwarding
    Interface Serial2 is unavailable

Router# show bridge 1 circuit-group 1 0000.6502.23EA 0000.1234.4567

%Please enter source MAC address only
```

Table 19 describes the significant fields shown in the display.

Table 19 show bridge circuit-group Field Descriptions

Field	Description
inserted	Indicates whether this interface is included or not included in circuit-group operation. If the interface is administratively down, or if line protocol is not up, the interface is not included in the circuit-group operation.
learning	Indicates whether this interface is in Spanning Tree Protocol (IEEE or Digital) learning or not learning state.
forwarding	Indicates whether this port is in Spanning Tree Protocol (IEEE or Digital) forwarding or not forwarding state.

show bridge group

To display the status of each bridge group, use the **show bridge group** command in privileged EXEC mode.

show bridge group [**verbose**]

Syntax Description

verbose	(Optional) Displays detailed information.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

```
Router# show bridge group

Bridge Group 1 is running the DEC compatible Spanning Tree Protocol

   Port 7 (ATM0.1 LANE Ethernet) of bridge group 1 is down
   Port 4 (TokenRing0) of bridge group 1 is forwarding
```

"Forwarding" and "down" indicate the port state as determined by the spanning-tree algorithm or via configuration.

The following examples are for bridge group 30 and bridge group 40 of a PA-12E/2FE port adapter in slot 3:

```
Router# show bridge group

Bridge Group 30 is running the IEEE compatible Spanning Tree Protocol
   Port 19 (Fast Ethernet3/0) of bridge group 30 is forwarding
   Port 20 (Fast Ethernet3/1) of bridge group 30 is forwarding
   Port 21 (Ethernet3/2) of bridge group 30 is forwarding
   Port 22 (Ethernet3/3) of bridge group 30 is forwarding
   Port 23 (Ethernet3/4) of bridge group 30 is forwarding
   Port 24 (Ethernet3/5) of bridge group 30 is forwarding
   Port 25 (Ethernet3/6) of bridge group 30 is forwarding

Bridge Group 40 is running the IEEE compatible Spanning Tree Protocol

   Port 26 (Ethernet3/7) of bridge group 40 is down
   Port 27 (Ethernet3/8) of bridge group 40 is down
   Port 28 (Ethernet3/9) of bridge group 40 is down
```

```
Port 29 (Ethernet3/10) of bridge group 40 is down
Port 30 (Ethernet3/11) of bridge group 40 is down
Port 31 (Ethernet3/12) of bridge group 40 is down
Port 32 (Ethernet3/13) of bridge group 40 is down
```

show bridge multicast

To display transparent bridging multicast state information, use the **show bridge multicast** command in user EXEC or privileged EXEC mode.

show bridge [*bridge-group*] **multicast** [**router-ports** | **groups**] [*group-address*]

Syntax Description

bridge-group	(Optional) Bridge group number specified in the **bridge protocol** command.
router-ports	(Optional) Display information for multicast router ports.
groups	(Optional) Display information for multicast groups.
group-address	(Optional) Multicast IP address associated with a specific multicast group.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show bridge multicast** command:

```
Router# show bridge multicast

 Multicast router ports for bridge group 1:

  2 multicast router ports
   Fddi2/0         R
   Ethernet0/4     R

 Multicast groups for bridge group 1:

  235.145.145.223            RX count     TX count
   Fddi2/0         R                0            2
   Ethernet0/4     R                0            3
   Ethernet0/3     G                1            0

  235.5.5.5                  RX count     TX count
   Fddi2/0         R                0            2
   Ethernet0/4     R                0            3
   Ethernet0/3     G                1            0

  235.4.4.4                  RX count     TX count
   Fddi2/0         R                0            2
   Ethernet0/4     R                0            3
   Ethernet0/3     G                1            0
```

Table 20 describes the significant fields shown in the display.

Table 20 show bridge multicast Field Descriptions

Field	Description
Multicast router ports for…	List of the multicast router ports by bridge group. Within the bridge group cluster, the display lists the number of multicast router ports and then lists the ports by interface.
Multicast groups for…	List of the multicast groups by bridge group. Within each multicast group, identified by a unique address, the display lists each port by interface name and indicates whether that port is a group member (“G”), a multicast router port (“R”), or both. The receive (RX) and transmit (TX) counts show the number of multicast packets that have been constrained to the multicast group by the bridge.

show bridge vlan

To display virtual LAN subinterfaces, use the **show bridge vlan** command in privileged EXEC mode.

show bridge vlan

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show bridge vlan** command:

```
Router# show bridge vlan

Bridge Group: 50

Virtual LAN Trunking Interface(s):  vLAN Protocol:     vLAN ID:  State

Fddi2/0.1000                        IEEE 802.10        1000      forwarding
Fast Ethernet4/0.500                 Inter Switch Link  500       listening

Virtual LAN Native Interface(s):    State

Ethernet0/1                         forwarding
Serial1/1                           down
```

Table 21 describes the fields shown in the display.

Table 21 show bridge vlan Field Descriptions

Field	Description
Bridge Group	Bridge group to which these interfaces belong.
Virtual LAN Trunking Interface(s)	VLAN interface.
vLAN Protocol)	IEEE 802.10 or Cisco Inter-Switch Link (ISL) encapsulation.
vLAN ID	VLAN identifier that maintains VLAN identities between switches.

Table 21 show bridge vlan Field Descriptions (continued)

Field	Description
State	Spanning-tree port state of the interface.
Virtual LAN Native Interface(s):	Interfaces whose transparently bridged traffic will be propagated only to other LAN segments within the same virtual LAN.

show bsc

To display statistics about the interfaces on which Bisync is configured, use the **show bsc** command in privileged EXEC mode.

show bsc [**group** *bstun-group-number*] [**address** *address-list*]

Syntax Description

group *bstun-group-number*	(Optional) block serial tunnel (BSTUN) group number. Valid numbers are decimal integers in the range from 1 to 255.
address *address-list*	(Optional) List of poll addresses.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

```
Router# show bsc

BSC pass-through on Serial4:
HDX enforcement state: IDLE.
Frame sequencing state: IDLE.
Total Tx Counts: 0 frames(total). 0 frames(data). 0 bytes.
Total Rx Counts: 0 frames(total). 0 frames(data). 0 bytes.

BSC local-ack on serial5:
Secondary state is CU_Idle.
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1137 frames(total). 0 frames(data). 1137 bytes.
        Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.

        Poll address: C3. Select address: E3 *CURRENT-CU*
        State is Active.
        Tx Counts: 1136 frames(total). 0 frames(data). 1136 bytes.
        Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.

Total Tx Counts: 2273 frames(total). 0 frames(data). 2273 bytes.
Total Rx Counts: 2284 frames(total). 0 frames(data). 11420 bytes.
```

The following is sample output from the **show bsc** command specifying BSTUN group 50:

```
Router# show bsc group 50

BSC local-ack on serial5:
Secondary state is CU_Idle.
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1217 frames(total). 0 frames(data). 1217 bytes.
        Rx Counts: 1222 frames(total). 0 frames(data). 6110 bytes.

        Poll address: C3. Select address: E3 *CURRENT-CU*
        State is Active.
        Tx Counts: 1214 frames(total). 0 frames(data). 1214 bytes.
        Rx Counts: 1220 frames(total). 0 frames(data). 6100 bytes.

Total Tx Counts: 2431 frames(total). 0 frames(data). 2431 bytes.
Total Rx Counts: 2442 frames(total). 0 frames(data). 12200 bytes.
```

The following is sample output from the **show bsc** command specifying BSTUN group 50 and poll address C2:

```
Router# show bsc group 50 address C2

BSC local-ack on serial5:
Secondary state is CU_Idle.
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1217 frames(total). 0 frames(data). 1217 bytes.
        Rx Counts: 1222 frames(total). 0 frames(data). 6110 bytes.

Total Tx Counts: 1217 frames(total). 0 frames(data). 1217 bytes.
Total Rx Counts: 1222 frames(total). 0 frames(data). 6110 bytes.
```

The following is sample output from the **show bsc** command specifying poll address C2:

```
Router# show bsc address C2

BSC pass-through on Serial4:
HDX enforcement state: IDLE.
Frame sequencing state: IDLE.
Total Tx Counts: 0 frames(total). 0 frames(data). 0 bytes.
Total Rx Counts: 0 frames(total). 0 frames(data). 0 bytes.

BSC local-ack on serial5:
Secondary state is CU_Idle.
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1137 frames(total). 0 frames(data). 1137 bytes.
        Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.

Total Tx Counts: 1137 frames(total). 0 frames(data). 1137 bytes.
Total Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.
```

Table 22 describes the fields shown in the display.

Table 22 show bsc Field Descriptions

Field	Description
BSC *x* on *interface y*	Indicates whether the router is configured for pass-through or local acknowledgment on the indicated interface.
Output queue depth	Packets queued on this interface. This field is displayed only when the value is not zero.
Frame builder state	Current frame building state. This field is displayed only when the state is not IDLE.
HDX enforcement state	Current half-duplex send enforcement state. The values are: • IDLE—Waiting for communication activity. • PND_COMP—Waiting for router to send. • PND_RCV—Waiting for attached device to respond to data sent.
Frame sequencing state	Frame sequencing state to protect against network latencies. When the router is configured as the primary end of the link, the values are: • IDLE—Waiting for a poll. • SEC—In a session with a device. When the router is configured as the secondary end of the link, the values are: • IDLE—Waiting for a poll. • PRI—In a session with a device. When the router is configured for point-to-point contention, the values are: • IDLE—Waiting for a poll. • PEND—Waiting for the first data frame. • PRI—Connected device is acting as a primary device. • SEC—Connected device is acting as a secondary device.
Total Tx Counts	Total transmit frame count for the indicated interface.
Total Rx Count	Total receive frame count for the indicated interface.

Table 22 show bsc Field Descriptions (continued)

Field	Description
Primary state is …	The current state when the router is configured as the primary end of the link. The possible values are: • TCU_Down—Waiting for the line to become active. • TCU_EOFile—A valid block ending in ETX has been received. • TCU_Idle—Waiting for work or notification of completion of the sending of end of transmission (EOT). • TCU_InFile—A valid block ending in ETB has been received. • TCU_Polled—A general poll has been issued. • TCU_Selected—A select has been issued. • TCU_SpecPolled—A specific poll has been sent. • TCU_TtdDelay—An ETB block was acknowledged, but the next block to be sent has not yet been received. • TCU_TtdSent—A TTD has been sent because no data was received by the time the timeout for sending Ttd expired. • TCU_TxEOFile—A block of data ending in ETX has been sent. • TCU_TxInFile—A block of data ending in ETB has been sent. • TCU_TxRetry—Trying to send a frame again.
Secondary state is …	The current state when the router is configured as the secondary end of the link. The possible values are: • CU_DevBusy—A select has been refused with WACK or RVI. • CU_Down—Waiting for the line to become active. • CU_EOFile—A valid block ending in ETX has been received. • CU_Idle—Waiting for a poll or select action. • CU_InFile—A valid block ending in ETB has been received. • CU_Selected—A select has been acknowledged. • CU_TtdDelay—An ETB block was acknowledged, but the next block to be sent has not yet been received. • CU_TtdSent—A TTD has been sent because no data was received by the time the timeout for sending Ttd expired. • CU_TxEOFile—A block of data ending in ETX has been sent. • CU_TxInFile—A block of data ending in ETB has been sent. • CU_TxRetry—Trying to send a frame again. • CU_TxSpecPollData—A data frame (typically S/S) has been used to answer a specific poll. • CU_TxStatus—Host has polled for device-specific status.
Poll address	Address used when the host wants to get device information.
Select address	Address used when the host wants to send data to the device.

Table 22 show bsc Field Descriptions (continued)

Field	Description
State is …	Current initialization state of this control unit. The values are: • Active—The remote device is active. • Inactive—The remote device is dead. • Initializing—No response from remote device yet.
Tx Counts	Transmit frame count for this control unit.
Rx Counts	Receive frame count for this control unit.
Total Tx Counts	Total transmit frame count for the indicated interface.
Total Rx Counts	Total receive frame count for the indicated interface.

show bstun

To display the current status of serial tunnel (STUN) connections, use the **show bstun** command in privileged EXEC mode.

show bstun [**group** *bstun-group-number*] [**address** *address-list*]

Syntax Description

group *bstun-group-number*	(Optional) Block Serial Tunneling (BSTUN) group number. Valid numbers are decimal integers in the range from 1 to 255.
address *address-list*	(Optional) List of poll addresses.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(4)T	This command was modified for the Bisync-to-IP Conversion for Automated Teller Machines feature. The display was modified to include Bisync-to-IP (BIP) as a transport protocol, and to show both the foreign and local port numbers.
12.3(2)T	This command was modified for the Asynchronous Point of Sale-to-IP Conversion (APIP) feature to include APIP as a transport protocol.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show bstun** command with no options:

```
Router# show bstun

This peer: 10.26.54.111
 *Serial0/0 (group 201 [bsc-local-ack])
route  transport  address         dlci  lsap     state     rx_pkts   tx_pkts   drops
C1     TCP        10.26.54.2                    closed    0         0         0
C2     TCP        10.26.54.2                    closed    0         0         0
C3     TCP        10.26.54.2                    closed    0         0         0
```

The following is sample output from the **show bstun** command using the new BIP configuration:

```
Router# show bstun

This peer: 10.26.54.111
 *Serial0/0 (group 201 [bsc-local-ack])
route  transport  address       fport  lport     state     rx_pkts   tx_pkts   drops
C1     BIP        10.26.54.2    2002   1963      closed    0         0         0
C2     BIP        10.26.54.2    2001   1963      closed    0         0         0
C3     BIP        10.26.54.2    2000   1963      closed    0         0         0
```

```
Router# show bstun

 Serial1/7  (group 10 [apos])
route  transport  address       fport  lport     state     rx_pkts   tx_pkts   drops
all     APIP      10.26.54.2    10550  0         closed    0         0         0
```

Table 23 describes the significant fields shown in the output.

Table 23 show bstun Field Descriptions

Field	Description
This peer	Lists the peer name or address. The interface name (as defined by the **description** command), its block serial tunnel (BSTUN) group number, and the protocol associated with the group are shown on the next header line.
route	Bisync control unit address or all.
transport	Description of link, either a serial interface using serial transport (indicated by IF followed by interface name), a TCP connection to a remote router (TCP followed by IP address), a BIP connection to a host, or APIP connection to a host (APIP followed by an IP address).
address	The IP address or serial interface that packets are being forwarded to.
fport	The foreign port number.
lport	The local port number.
state	State of the link. The following are possible values for the state of the link: • open: A connection is active. • open pending: Indicates the router will be attempting to connect to the remote device. • open wait: An active open message has been sent to the remote device, and the router is waiting for a response. • direct: A direct link to another line is active. • dead: The connection has been aborted. • closed: A normal close operation has disconnected the connection.
open	A connection is active.
open pending	Indicates the router will be attempting to connect to the remote device.
open wait	An active open message has been sent to the remote device, and the router is waiting for a response.
direct	A direct link to another line is active.
dead	The connection has been aborted.
closed	A normal close operation has disconnected the connection.
rx_pkts	Number of received packets.
tx_pkts	Number of sent packets.
drops	Number of packets that had to be dropped for whatever reason.

show controllers channel

To display Channel Port Adapter (CPA)-specific information, including the loaded microcode, use the **show controllers channel** command in user EXEC or privileged EXEC mode.

show controllers channel [*slot*/*port*]

Syntax Description

slot	(Optional) Slot number.
port	(Optional) Interface number.

Command Modes

User EXEC
Prvileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show controllers channel** command:

```
Router# show controllers channel 5/0

ECPA 5, hardware version 1.0, microcode version 26.0
    Mailbox commands: 0 forevers, 0 max elapsed usecs
    Microcode loaded from flash slot0:xcpa26-0_kernel_xcpa
    Loaded:seg_eca         Rev. 0    Compiled by cip-release on 01-Apr-98
    EPROM version 1.0, VPLD version 1.1
    ECA0: hw version 255, microcode version C50602D1
    Load metrics:
      Memory    sram 2964552/4096K, dram 11552952/16M
      CPU       1m   0%, 5m   0%, 60m   0%
      DMA       1m   0%, 5m   0%, 60m   0%
      ECA0      1m   0%, 5m   0%, 60m   0%
 Interface Channel5/0
 Hardware is Escon Channel
  HW Registers control status=0x0001EC07  LED control=0x00045DD5
  HW Poll Register 4B05D4E0:[00000001]
  Free buffer queues
    queue=0 max_entries=128 size=600 head=39 ring=4B095F00
    queue=1 max_entries=32 size=4520 head=31 ring=4B095E40
    queue=2 max_entries=64 size=4520 head=63 ring=4B096140
  Tx Queues
    queue=0 head=0 tail=0 tx_cnt=0 tx_pakcnt=0
    max_entries=128 type=1 poll_index=0 ring=4B0963C0
    fspak buffers swapped out=0
    queue=1 head=31 tail=31 tx_cnt=0 tx_pakcnt=0
    max_entries=32 type=2 poll_index=1 ring=4B096280
    fspak buffers swapped out=0
```

```
Rx Queues
  max_entries=221 poll_index=3 head=57 ring=4B096800
  max packets per interrupt count = 0
```

show controllers token (IBM)

To display information about memory management, error counters, and the board itself, use the **show controllers token** command in privileged EXEC mode.

show controllers token

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Depending on the board being used, the output from the **show controllers token** command can vary. The **show controllers token** command also displays proprietary information. Thus, the information that the **show controllers token** command displays is of primary use to Cisco Systems technical personnel. Information that is useful to users can be obtained with the **show interfaces tokenring** command, described later.

Examples

The following is sample output from the **show controllers token** command of a CSC-IR or CSC-2R card:

```
Router# show controllers token

TR Unit 0 is board 0 - ring 0

 state 3, dev blk: 0x1D2EBC, mailbox: 0x2100010, sca: 0x2010000
   current address: 0000.3080.6f40, burned in address: 0000.3080.6f40
   current TX ptr: 0xBA8, current RX ptr: 0x800

   Last Ring Status: none

 Stats: soft:0/0, hard:0/0, sig loss:0/0
        tx beacon: 0/0, wire fault 0/0, recovery: 0/0
        only station: 0/0, remote removal: 0/0
   Bridge: local 3330, bnum 1, target 3583
     max_hops 7, target idb: 0x0, not local
   Interface failures: 0 -- Bkgnd Ints: 0
   TX shorts 0, TX giants 0

   Monitor state: (active)
     flags 0xC0, state 0x0, test 0x0, code 0x0, reason 0x0
 f/w ver: 1.0, chip f/w: '000000.ME31100', [bridge capable]
```

```
     SMT form of this command s: 1.01 kernel, 4.02 fastmac
     ring mode: F00, internal enables: SRB REM RPS CRS/NetMgr
     internal functional: 0000011A (0000011A), group: 00000000 (00000000)
     if_state: 1, ints: 0/0, ghosts: 0/0, bad_states: 0/0
     t2m fifo purges: 0/0
     t2m fifo current: 0, t2m fifo max: 0/0, proto_errs: 0/0
     ring: 3330, bridge num: 1, target: 3583, max hops: 7

Packet counts:
       receive total: 298/6197, small: 298/6197, large 0/0
               runts: 0/0, giants: 0/0
               local: 298/6197, bridged: 0/0, promis: 0/0
             bad rif: 0/0, multiframe: 0/0
       ring num mismatch 0/0, spanning violations 0
       transmit total: 1/25, small: 1/25, large 0/0
                runts: 0/0, giants: 0/0, errors 0/0
bad fs: 0/0, bad ac: 0
congested: 0/0, not present: 0/0
     Unexpected interrupts: 0/0, last unexp. int: 0

     Internal controller counts:
    line errors:  0/0, internal errors: 0/0
    burst errors: 0/0, ari/fci errors:  0/0
    abort errors: 0/0, lost frame: 0/0
    copy errors:  0/0, rcvr congestion: 0/0
    token errors: 0/0, frequency errors: 0/0
    dma bus errors: -/-, dma parity errors: -/-
     Internal controller smt state:
    Adapter MAC:     0000.3080.6f40, Physical drop:     00000000
    NAUN Address:    0000.a6e0.11a6, NAUN drop:         00000000
    Last source:     0000.a6e0.11a6, Last poll:         0000.3080.6f40
    Last MVID:       0006,           Last attn code:    0006
    Txmit priority:  0006,           Auth Class:        7FFF
    Monitor Error:   0000,           Interface Errors:  FFFF
    Correlator:      0000,           Soft Error Timer:  00C8
    Local Ring:      0000,           Ring Status:       0000
    Beacon rcv type: 0000,           Beacon txmit type: 0000
    Beacon type:     0000,           Beacon NAUN:       0000.a6e0.11a6
```

Table 24, Part 1 describes the fields shown in the first line of sample output.

Table 24, Part 1 show controllers token Field Descriptions

Field	Description
TR Unit 0	Unit number assigned to the Token Ring interface associated with this output.
is board 0	Board number assigned to the Token Ring controller board associated with this interface.
ring 0	Number of the Token Ring associated with this board.

In the following line, state 3 indicates the state of the board. The rest of this output line displays memory mapping that is of primary use to Cisco engineers.

```
state 3, dev blk: 0x1D2EBC, mailbox: 0x2100010, sca: 0x2010000
```

The following line also appears in **show interface token** output as the address and burned-in address (bia), respectively:

```
current address: 0000.3080.6f40, burned in address: 0000.3080.6f40
```

The following line displays buffer management pointers that change by board:

```
current TX ptr: 0xBA8, current RX ptr: 0x800
```

The following line indicates the ring status from the controller chipset. This information is used by LAN Network Manager:

```
Last Ring Status: none
```

The following line displays Token Ring statistics. See the Token Ring specification for more information:

```
Stats: soft:0/0, hard:0/0, sig loss:0/0
        tx beacon: 0/0, wire fault 0/0, recovery: 0/0
        only station: 0/0, remote removal: 0/0
```

The following line indicates that Token Ring communication has been enabled on the interface. If this line of output appears, the message "Source Route Bridge capable" should appear in the **show interfaces tokenring** display.

```
Bridge: local 3330, bnum 1, target 3583
```

Table 24, Part 2 describes the fields shown in the following line of sample output:

```
max_hops 7, target idb: 0x0, not local
```

Table 24, Part 2 show controllers token Field Descriptions

Field	Description
max_hops 7	Maximum number of bridges.
target idb: 0x0	Destination interface definition.
not local	Interface has been defined as a remote bridge.

The following line is specific to the hardware:

```
Interface failures: 0 -- Bkgnd Ints: 0
```

In the following line, transmit (TX) shorts are the number of packets the interface sends that are discarded because they are smaller than the medium's minimum packet size. TX giants are the number of packets the interface sends that are discarded because they exceed the medium's maximum packet size.

```
TX shorts 0, TX giants 0
```

The following line indicates the state of the controller. Possible values are active, failure, inactive, and reset.

```
Monitor state: (active)
```

The following line displays detailed information relating to the monitor state shown in the previous line of output. This information relates to the firmware on the controller. This information is relevant to Cisco engineers only if the monitor state is something other than active.

```
flags 0xC0, state 0x0, test 0x0, code 0x0, reason 0x0
```

Table 24, Part 3 describes the fields in the following line of output:

```
f/w ver: 1.0 expr 0, chip f/w: '000000.ME31100', [bridge capable]
```

Table 24, Part 3 show controllers token Field Descriptions

Field	Description
f/w ver: 1.0	Version of Cisco firmware on the board.
chip f/w: '000000.ME31100'	Firmware on the chipset.
[bridge capable]	Interface has not been configured for bridging, but it has that capability.

The following line displays the version numbers for the kernel and the accelerator microcode of the Madge firmware on the board; this firmware is the Logical Link Control (LLC) interface to the chipset:

```
SMT form of this command s: 1.01 kernel, 4.02 fastmac
```

The following line displays LAN Network Manager information that relates to ring status:

```
ring mode: F00, internal enables: SRB REM RPS CRS/NetMgr
```

The following line corresponds to the functional address and the group address shown in **show interfaces tokenring** output:

```
internal functional: 0000011A (0000011A), group: 00000000 (00000000)
```

The following line displays interface board state information that is proprietary:

```
if_state: 1, ints: 0/0, ghosts: 0/0, bad_states: 0/0
```

The following lines display information that is proprietary. Our engineers use this information for debugging purposes:

```
t2m fifo purges: 0/0
t2m fifo current: 0, t2m fifo max: 0/0, proto_errs: 0/0
```

Each of the fields in the following line maps to a field in the **show source bridge** display, as follows: ring maps to srn; bridge num maps to bn; target maps to trn; and max hops maps to max:

```
ring: 3330, bridge num: 1, target: 3583, max hops: 7
```

In the following lines of output, the number preceding the slash (/) indicates the count since the value was last displayed; the number following the slash (/) indicates the count since the system was last booted:

```
Packet counts:
       receive total: 298/6197, small: 298/6197, large 0/0
```

In the following line, the number preceding the slash (/) indicates the count since the value was last displayed; the number following the slash (/) indicates the count since the system was last booted. The runts and giants values that appear here correspond to the runts and giants values that appear in **show interfaces tokenring** output:

```
runts: 0/0, giants: 0/0
```

The following lines are receiver-specific information that Cisco engineers can use for debugging purposes:

```
local: 298/6197, bridged: 0/0, promis: 0/0
bad rif: 0/0, multiframe: 0/0
ring num mismatch 0/0, spanning violations 0
transmit total: 1/25, small: 1/25, large 0/0
runts: 0/0, giants: 0/0, errors 0/0
```

The following lines include very specific statistics that are not relevant in most cases, but exist for historical purposes. In particular, the internal errors, burst errors, ari/fci, abort errors, copy errors, frequency errors, dma bus errors, and dma parity errors fields are not relevant.

```
Internal controller counts:
 line errors: 0/0, internal errors: 0/0
 burst errors: 0/0, ari/fci errors: 0/0
 abort errors: 0/0, lost frame: 0/0
 copy errors: 0/0, rcvr congestion: 0/0
 token errors: 0/0, frequency errors: 0/0
 dma bus errors: -/-, dma parity errors: -/-
```

The following lines are low-level Token Ring interface statistics relating to the state and status of the Token Ring with respect to all other Token Rings on the line:

```
Internal controller smt state:
 Adapter MAC:     0000.3080.6f40, Physical drop:     00000000
 NAUN Address:    0000.a6e0.11a6, NAUN drop:         00000000
 Last source:     0000.a6e0.11a6, Last poll:         0000.3080.6f40
 Last MVID:       0006,           Last attn code:    0006
 Txmit priority:  0006,           Auth Class:        7FFF
 Monitor Error:   0000,           Interface Errors:  FFFF
 Correlator:      0000,           Soft Error Timer:  00C8
 Local Ring:      0000,           Ring Status:       0000
 Beacon rcv type: 0000,           Beacon txmit type: 0000
```

show dlsw capabilities

To display the configuration of a specific peer or all peers, use the **show dlsw capabilities** command in privileged EXEC mode.

show dlsw capabilities [**interface** *type number* | **ip-address** *ip-address* | **local**]

Syntax Description

interface *type number*	(Optional) Specifies the interface type and number for which the data-link switching plus (DLSw+) capabilities are to be displayed.
ip-address *ip-address*	(Optional) Specifies a peer by its IP address.
local	(Optional) Specifies the local DLSw+ peer.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw capabilities** command:

```
Router# show dlsw capabilities

DLSw: Capabilities for peer 10.1.1.6(2065)
   vendor id (OUI)         : '00C' (cisco)
   version number          : 1
   release number          : 0
   init pacing window      : 20
   unsupported saps        : none
   num of tcp sessions     : 1
   loop prevent support    : no
   icanreach mac-exclusive : no
   icanreach netbios-excl. : no
   reachable mac addresses : none
   reachable netbios names : none
   cisco version number    : 1
   peer group number       : 0
   border peer capable     : no
   peer cost               : 3
   biu-segment configured  : no
   UDP Unicast support     : yes
   local-ack configured    : yes
   priority configured     : no
   configured ip address   : 1.1.1.6
```

```
   peer type               : conf
   version string          :
Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-JSV-M), Version 11.3(4), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Tue 16-Jun-98 04:29 by phanguye
```

Table 25 describes the fields shown in the display.

Table 25 show dlsw capabilities Field Descriptions

Field	Description
vendor id (OUI)	Vendor ID.
version number	RFC 1795 version of the Sequenced Packet Protocol (SSP) protocol.
release number	RFC 1795 release of the SSP protocol
init pacing window	Initial pacing window.
unsupported saps	Unsupported service access point (SAP)s.
num of tcp sessions	Number of TCP sessions.
loop prevent support	No loop prevent support.
icanreach mac-exclusive	Configured MAC addresses that the router can reach.
icanreach netbios-excl.	Configured NetBIOS names that the router can reach.
reachable mac addresses	Reachable MAC addresses.
reachable netbios name	Reachable NetBIOS names.
cisco version number	Cisco version number.
peer group number	Peer group member number.
border peer capable	Border peer capability.
peer cost	Peer cost.
biu-segment configured	Basic information unit (BIU) segment configured.
UDP Unicast support	User Datagram Protocol (UDP) unicast support.
local-ack configured	Local acknowledgment capable.
priority configured	Priority capability.
configured ip address	Configured IP address.
peer type	Peer type can be peer-on-demand or promiscuous.
version string	Cisco IOS software version information.

show dlsw circuits

To display the state of all circuits involving this MAC address as a source and destination, use the **show dlsw circuits** command in privileged EXEC mode.

show dlsw circuits [**detail**] [**mac-address** *address* | **sap-value** *value* | **circuit id**]

Syntax Description

detail	(Optional) Display circuit state information in expanded format.
mac-address *address*	(Optional) Specifies the MAC address to be used in the circuit search.
sap-value *value*	(Optional) Specifies the service access point (SAP) to be used in the circuit search.
circuit id	(Optional) Specifies the circuit ID of the circuit index.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw circuits** command:

```
Router# show dlsw circuits

Index           local addr(lsap)    remote addr(dsap)  state          uptime
4060086272      4000.0000.0056(F0)  4001.0000.0049(F0) CONNECTED      00:00:13
Total number of circuits connected: 1
```

The following is sample output from the **show dlsw circuits** command with the **detail** argument:

```
Router# show dlsw circuits detail

Index   local addr(lsap)    remote addr(dsap)   state uptime
194 0800.5a9b.b3b2(F0)  800.5ac1.302d(F0)  CONNECTED 00:00:13
        PCEP: 995AA4     UCEP: A52274
        Port: To0/0      peer 172.18.15.166(2065)
        Flow-Control-Tx SQ CW:20, Permitted:28; Rx CW:22, Granted:25 Op:
IWO
        Congestion: LOW(02), Flow Op: Half: 12/5 Reset 1/0
        RIF = 0680.0011.0640
```

Table 26 describes the fields shown in the display.

Table 26 show dlsw circuits Field Descriptions

Field	Description
Index	Number the software uses to reference an individual circuit.
local addr(lsap)	MAC address and SAP value used by end station closest to this data-link switching plus (DLSw+) peer.
remote addr(dsap)	MAC address and SAP value used by end station that is across the peer connection (remote).
state	Indicates whether circuit has completed establishment.
uptime	Length of time a circuit has been connected.
Total number of circuits connected	Number of total connected circuits. If a circuit has not completed connection, it will not show a value.
PCEP, UCEP	Internal correlators used as labels for communication internal to the router between DLSw+ and Logical Link Control, type 2 (LLC2), Synchronous Data Link Control (SDLC), or Qualified Logical Link Control (QLLC).
Port	Local port over which this circuit has been established or DLSw interface to the bridge group.
Flow Control (Tx and Rx)	Reports DSLw+ flow control windows as described in Section 8 of RFC 1795.
SQ	Two flags indicating congestion toward the remote peer. These flags are displayed only when the circuit is congested.
S	Data flow from the local station has been stopped. This results in LLC2 or SDLC sending Receiver Not Ready (RNR) frames.
Q	Data frames are being queued for transport to the remote peer.
CW	Current pacing window. See RFC 1795.
Permitted	Packet counter for tx. See RFC 1795.
Granted	Packet counter for rx. See RFC 1795.
Op	Next flow indicator (FCI) that will be sent to the remote peer. See RFC 1795.
Congestion	Data flow indicator from router to station is congested. Values are Low, Medium, High, and Max.
Flow Op	Amount of Reset Window Operator and Half Window Operator being sent or received. See RFC 1795.
RIF	Routing Information Field used over the local port for data traversing this circuit (if appropriate).

show dlsw circuits history

To display the details of the last status of all DLSW circuits either currently active or not active, use the **show dlsw circuits history** command in privileged EXEC mode.

show dlsw circuits history [**detail**] [**mac-address** *address* | **sap-value** *value* | **circuit id**]

Syntax Description

detail	(Optional) Displays details for all remote circuits in the connected state.
mac-address *address*	(Optional) Specifies the MAC address to be used for all remote circuits.
sap-value *value*	(Optional) Specifies the service access point (SAP) to be used for all remote circuits.
circuit id	(Optional) Specifies the circuit ID of a specific remote circuit.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show dlsw circuits history** command keeps the history for the last 32 circuits. For every circuit, the command stores a maximum of 16 entries.

Examples

The following is sample output from the **show dlsw circuits history** command:

```
Router# show dlsw circuits history

Circuit history kept for last 32 circuits using 4096 bytes:
Index           local addr(lsap)    remote addr(dsap)  remote peer
1761607680      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198
3657433089      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198 Ckt Active
```

The following is sample output from the **show dlsw circuits history** command with the **detail** keyword:

```
Router# show dlsw circuits history detail

Circuit history kept for last 32 circuits, using 4096 bytes
Index           local addr(lsap)    remote addr(dsap)  remote peer
1761607680      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198
        Created at   : 08:19:14.440 EDT Wed Sep 21 2005
        Connected at : 08:19:14.476 EDT Wed Sep 21 2005
        Destroyed at : 08:20:21.159 EDT Wed Sep 21 2005
        Local Corr   : 1761607680   Remote Corr: 1962934272
        Bytes:             633/731        Info-frames:           7/7
        XID-frames:          4/5          UInfo-frames:          0/0
        Flags: Remote created, Local connected
        Last events:
```

```
        Current State        Event              Add. Info  Next State
        ---------------------------------------------------------------------
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN halt-noack       0x0      HALT_NOACK_PEND
        HALT_NOACK_PEND      DLC DiscCnf          0x0      CLOSE_PEND
        CLOSE_PEND           DLC DiscInd          0x0      CLOSE_PEND
        CLOSE_PEND           DLC CloseStnCnf      0x0      DISCONNECTED

3657433089      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198 Ckt Active
        Created at   : 08:20:51.146 EDT Wed Sep 21 2005
        Connected at : 08:20:51.182 EDT Wed Sep 21 2005
        Local Corr   : 3657433089   Remote Corr: 3137339393
        Bytes:             633/731        Info-frames:           7/7
        XID-frames:          4/5          UInfo-frames:          0/0
        Flags: Remote created, Local connected
        Last events:
        Current State        Event              Add. Info  Next State
        ---------------------------------------------------------------------
        CONNECT_PENDING      WAN contacted        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC ConnectCnf       0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
```

The following is sample output from the **show dlsw circuits history** command for specific circuits only:

```
Router# show dlsw circuits history mac-address 0000.6666.4242

Circuit history kept for last 32 circuits, using 4096 bytes
Index           local addr(lsap)    remote addr(dsap)  remote peer
1761607680      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198
3657433089      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198 Ckt Active
Router# show dlsw circuits history detail mac-address 4000.1000.2000
Circuit history kept for last 32 circuits, using 4096 bytes
Index           local addr(lsap)    remote addr(dsap)  remote peer
1761607680      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198
3657433089      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198 Ckt Active
```

Table 27 show dlsw circuits history Field Descriptions

Field	Description
Index	Number the software uses to reference an individual circuit.
local addr(lsap)	MAC address and SAP value used by the end station that is closest to this data-link switching plus (DLSw+) peer.
remote addr(dsap)	MAC address and SAP value used by the end station that is across the peer connection (remote).
Ckt Active	Indicates a circuit that is Active.
remote peer	IP address of the peer that is used by the individual circuit.
Ckt Active	Indicates a circuit that is Active.
Local Corr	Circuit ID of the local router.
Remote Corr	Circuit ID of the peer.
Bytes	Bytes that are transmitted and bytes that are received.
Info-frames	Transmitted frames/received frames. Info-frames carry the actual information that you want to transmit or received.
XID-frames	Transmitted XID's/received XID's. XIDs are exchange ids.
Uinfo-frames	Unnumbered information frames that use the Logical Link Control 1(llc1) mode with no guaranteed delivery and no retransmission of the information frame.
Flags	Flags that are created can be either local or remote: • local = This router has started the circuit. • remote = Partner DLSw peer has started the circuit. Connected can be either local or remote: • local = This router has received the Set Asynchronous Balanced Mode Extended (SABME) from the end system. The router transmits a UA back in response. • remote = This router has received a DLSw contacted primitive from the DLSw partner and is sending out a SABME to the end system, receiving a UA back in response.
Current State	Current state of the finite state machine.
Next State	The state to which the transition occurs is based on the event.
CONNECTED	The DLSw+ circuit is fully established and connected end to end.
HALT_NOACK_PEND	Indicates a state for which the DLSw peer is lost and the local router is awaits the Disc.Cnf or Close_Stn.Cnf signal.
CLOSE_PEND	DLSw is awaiting Close_Stn.Cnf with a disc confirmation from the end station and also from the DLSw partner.
DISCONNECTED	A state where no DLSw circuit exists.
LOCAL_RESOLVE	DLSw is awaiting the Req_Opn_Stn_confirm signal.
REMOTE_RESOLVE	Successful circuit end point (CEP) creation, which receives a Canureach_Ex.
CKT_ESTABLISHED	The two end stations are exchanging Exchange Ids (XID).

Table 27 show dlsw circuits history Field Descriptions (continued)

Field	Description
CKT_PENDING	DLSw is awaiting CONTACTED, having received a SABME and sending a CONTACT to the partner. The partner must send out the SABME, get the UA and respond with CONTACTED
CONTACT_PENDING	DLSw is awaiting DLC_CONTACTED, having received the CONTACT from the partner.
CKT_RESTART	The data link switch (DLS) that originated the reset is awaiting the restart of the data link and the DL_RESTARTED response to a RESTART_DL_message.
RESTART_PENDING	The remote DLS is awaiting the DLC_DL_HALTED indication following the DLC_HALT_DL request.
DISC_PENDING	DLSw is awaiting Ssp dl_Halted.
HALT_PENDING	DLSw is awaiting Disc.dnf.
HALT_NOACK_PEND	Indicates a state in which the DLSw peer is lost and the local router is awaits the Disc.Cnf or Close_Stn.Cnf signal.
CLOSE_PEND	DLSw is awaiting Close_Stn.Cnf having received a Disc.Cnf from the end station and also from the DLSw partner.
Event	An incident or occurrence corresponding to a state.
ADM Stop	A clear DLSw circuit or the DLSw peer goes down.
ADM RingStop	DLSw configuration gets removed.
ADM WANFailure	The peer is down. See RFC1795.
WAN contact	The WAN connection is fully established. See RFC1795.
WAN contacted	A UA received in response to a SABME. See RFC1795.
WAN infoframe	An infoframe (data containing a valid payload) is received on the WAN.See RFC1795.
DLC DataInd	An infoframe is received from the local media. See RFC1795.
DLC ConnectCnf	A UA is going out on the local interface. See RFC1795.

Related Commands

Command	Description
show dlsw circuits	Displays the state of all circuits involving a common MAC address as a source and destination.

show dlsw fastcache

To display the fast cache for Fast Sequenced Transport (FST) and direct-encapsulated peers, use the **show dlsw fastcache** command in privileged EXEC mode.

show dlsw fastcache

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw fastcache** command with an FST peer:

```
Router# show dlsw fastcache

    peer              local-mac      remote-mac   l/r sap rif
FST 10.2.32.1       0800.5a8f.881c 0800.5a8f.8822 04/04 0680.02D5.1360
```

The following is sample output from the **show dlsw fastcache** command:

```
Router# show dlsw fastcache

    peer              local-mac      remote-mac   l/r sap rif

IF Se1  0800.5a8f.881c  0800.5a8f.8822 F0/F0 0680.02D5.1360
```

Table 28 describes the fields shown in the display.

Table 28 show dlsw fastcache Field Descriptions

Field	Description
peer	Peer in which the router is connected. Could represent either an IP address or interface.
local-mac	Local MAC address.
remote-mac	Remote MAC address.
l/r sap	Local or remote service access point (SAP) value.
rif	Routing Information Field (RIF) value.

show dlsw local-circuit

To display the state of all locally-switched DLSw+ circuits, use the **show dlsw local-circuit** privileged EXEC command.

show dlsw local-circuit [**mac-address** *address* | **sap-value** *value* | *circuit-id*]

Syntax Description

mac-address *address*	(Optional) Specifies the MAC address to be used in the circuit search.
sap-value *value*	(Optional) Specifies the SAP to be used in the circuit search.
circuit-id	(Optional) Specifies the circuit ID of the circuit index. The valid range is 0 to 4294967295.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw local-circuit** command:

```
Router# show dlsw local-circuit

~ key         mac-addr    sap    state        port       rif
34886696   4000.1111.22c1 04  CONNECTED      Se2/0      --no rif--
~                PCEP: 2145198  UCEP: 2145428
~          4000.3745.0001 04  CONNECTED      DL0         --no rif--
~                PCEP: 2176C90  UCEP: 2145428
```

Table 29 describes significant fields shown in the display

Table 29 show dlsw local-circuit Field Descriptions

Field	Description
mac-addr	MAC address of the remote peer connection.
SAP	SAP value used by the remote peer.
state	Indicates whether circuit has completed establishment.
Port	Local port over which this circuit has been established or DLSw interface to the bridge group.

Table 29 show dlsw local-circuit Field Descriptions (continued)

Field	Description
RIF	Routing Information Field used over the local port for data traversing this circuit (if appropriate).
PCEP, UCEP	Internal correlators used as labels for communication internal to the router between DLSw+ and LLC2, SDLC, or QLLC.

show dlsw peers

To display data-link switching plus (DLSw) peer information, use the **show dlsw peers** command in privileged EXEC mode.

show dlsw peers [**interface** *type number* | **ip-address** *ip-address* | **ssp-dlx** [**interface** *type number* | **ip-address** *ip-address*] | **udp**]

Syntax Description

interface *type number*	(Optional) Specifies a remote peer by a direct interface.
ip-address *ip-address*	(Optional) Specifies a remote peer by its IP address.
ssp-dlx	(Optional) Details Sequenced Packet Protocol (SSP) and Data Link Exchange (DLX) primitive frames received and sent by a TCP or Logical Link Control, type 2 (LLC2) peer.
udp	(Optional) Displays User Datagram Protocol (UDP) frame forwarding statistics for specified peers.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	The **ssp-dlx** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw peers** command:

```
Router# show dlsw peers udp

Peers:   tot-Q'd     total-rx  total-tx    tot-retx  tot-drop curr-Q'd TCP uptime
1.1.1.      0                                                 23
0                                            0                                     0
                  0                          0       00:01:02
Total number of connected peers: 2
Total number of connections:     8
```

The following is sample output from the **show dlsw peers** command with a TCP connection:

```
Router# show dlsw peers

Peers:                 state     pkts_rx   pkts_tx  type  drops ckts TCP   uptime
 TCP 10.1.91.1
     High priority   CONNECT         43        40   conf      0    1   0 00:01:02
```

```
   Medium priority   CONNECT          0          0  conf      0    -   0 00:01:02
   Normal priority   CONNECT          4         41  conf      0    -   5 00:01:02
      Low priority   CONNECT          1          0  conf      0    -   0 00:01:02
 TCP 10.1.93.1
     High priority   CONNECT          3          3  conf      0    0   0 00:00:58
   Medium priority   CONNECT          0          0  conf      0    -   0 00:00:58
   Normal priority   CONNECT          0          0  conf      0    -   0 00:00:58
      Low priority   CONNECT          0         39  conf      0    -   0 00:00:58
Total number of connected peers: 2
Total number of connections:     8
```

The following is sample output from the **show dlsw peers** command with a Direct Frame Relay connection:

```
Router # show dlsw peers

Peers:                state    pkts_rx pkts_tx  type  drops ckts TCP    uptime
IF         SE1 16
        connect                  53                                              2597
        conf                                      0
-                   -             00:04:09
Total number of connected peers: 2
Total number of connections:     8
```

The following is sample output from the **show dlsw peers** command with a Direct Frame Relay with local acknowledgment (LLC2) connection:

```
Router # show dlsw peers

Peers:                state     pkts_rx pkts_tx  type  drops ckts TCP    uptime
LLC2 SE116                                    connect
1179                                                 108              conf
0   1               -                  -                                       00:04:09
Total number of connected peers: 2
Total number of connections:     8
```

The following is sample output from the **show dlsw peers ssp-dlx** command:

```
Router # show dlsw peers ssp-dlx

Peer:10.1.1.6                              received transmitted
    CUR_ex Can U Reach Explorers                5           2
    CUR_cs Can U Reach Circuit Start            2           5
    ICR_ex I Can Reach Explorers                4           5
    ICR_cs I Can Reach Circuit Start            4           1
    ACK Reach Acknowledgement                   1           4
    XID Frame                                  22          20
    CONQ Contact Remote Station                 4           0
    CONR Remote Station Contacted               0           4
    INFO Information (I) Frame                 39          39
    HLTQ Halt Data Link                         0           1
    HLTR Data Link Halted                       1           0
    HLTN Halt Data Link (no ack)                1           2
    CAPX Capabilities Exchange                  2           2
    Total SSP Primitives                       85          85

    DLX Peer Test Request                     122         146
    DLX Peer Test Response                    146         122
    DLX Border to Border Message               53           9
    --> SSP:CUR Can U Reach                    53           2
    --> SSP:DATA Data Frames                    0           7

    Last SSP Received: INFO
```

```
    Last SSP Sent: ICR

Total number of connected peers:1
Total number of connections:    1
```

Table 30 describes the significant fields shown in the display.

Table 30 show dlsw peers Field Descriptions

Field	Description
Peers	Information related to the remote peer, including encapsulation type, IP address (if using Fast Sequenced Transport [FST] or TCP)and interface number (if using direct encapsulation).
tot-Q'd	Number of UDP packets that have been queued because of TCP congestion.
total-rx	Number UDP packets received from the peer.
total-tx	Number of UDP packets sent to the peer.
tot-retx	Number of reachability resends (for example, DLSw+ retries NQ_ex and CUR_ex) when originally sent via UDP.
tot-drop	Number of queued UDP packets that were dropped because of persistent TCP congestion.
curr-Q'd	Number of current UDP packets queued because of TCP congestion.
TCP	Number of packets on the TCP output queue.
state	State of the peer: • CONNECT—normal working peer. • DISCONN—peer is not connected. • CAP_EXG—capabilities exchange mode. Waiting for capabilities response. • WAIT_RD—TCP write pipe (local port 2065) is open and peer is waiting for remote peer to open the read port (local port 2067). This field applies only to TCP peers. • WAN_BUSY—TCP outbound queue is full. This field applies only to TCP peers.
pkts_rx	Number of received packets.
pkts_tx	Number of sent packets.
type	Type of remote peer: • conf—configured • prom—promiscuous • pod—peer on demand

Table 30 show dlsw peers Field Descriptions (continued)

Field	Description
drops	Number of drops done by this peer. Reasons for the counter to increment: • WAN interface not up for a direct peer. • DLS tries to send a packet before the peer is fully connected (waiting for TCP event or capabilities event). • Outbound TCP queue full. • FST sequence number count mismatch. • Cannot get buffer to "slow switch" FST packet. • CiscoBus controller failure on high end (cannot move packet from receive buffer to send buffer, or vice versa). • Destination IP address of FST packet does not match local peer ID. • WAN interface not up for an FST peer. • No source-route bridging (SRB) route cache command configured. • Madge ring buffer is full on low-end systems (WAN feeding LAN too fast).
ckts	Number of active circuits through this peer. This field applies only to TCP and LLC2 transport peer types.
uptime	How long the connection has been established to this peer.
total number of connected peers	Total number of connected peers.
total number of connections	Total number of active circuit connections.

show dlsw reachability

To display data-link switching plus (DLSw+) reachability information, use the **show dlsw reachability** command in privileged EXEC mode.

show dlsw reachability [**group** [*value*] | **local** | **remote** | **mac-address** [*address*] | **netbios-names** [*name*]]

Syntax Description

group	(Optional) Displays contents of group reachability cache only.
value	(Optional) Specifies the group number for the reachability check. Only displays group cache entries for the specified group. The valid range is from 1 to 255.
local	(Optional) Displays contents of local reachability cache only.
remote	(Optional) Displays contents of remote reachability cache only.
mac-address	(Optional) Displays DLSw reachability for MAC addresses only.
address	(Optional) Specifies the MAC address for which to search in the reachability cache.
netbios-names	(Optional) Displays DLSw reachability for NetBIOS names only.
name	(Optional) Specifies the NetBIOS name for which to search in the reachability cache.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If none of the group, local, or remote options is specified, then the caches will be displayed in the following order: local, remote, and group.

Examples

The following is sample output from the **show dlsw reachability group** command:

```
Router# show dlsw reachability group

DLSw Group MAC address reachability cache list
Mac Addr Group
0000.3072.1070     10
DLSW Group NetBIOS Name reachability cache list
```

```
NetBIOS Name    Group
```

The following is sample output from the **show dlsw reachability** command:

```
Router# show dlsw reachability

DLSw MAC address reachability cache list
Mac Addr        status     Loc.    peer/port          rif
0000.f641.91e8  SEARCHING  LOCAL
0006.7c9a.7a48  FOUND      LOCAL   TokenRing0/0   0CB0.0011.3E71.A041.0DE5.0640
0800.5a4b.1cbc  SEARCHING  LOCAL
0800.5a54.ee59  SEARCHING  LOCAL
0800.5a8f.9c3f  FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
4000.0000.0050  FOUND      LOCAL   TokenRing0/0   0CB0.0011.3E71.A041.0DE5.0640
4000.0000.0306  FOUND      LOCAL   TokenRing0/0   0CB0.0011.3E71.A041.0DE5.0640
4000.0000.0307  SEARCHING  LOCAL
4000.0000.0308  SEARCHING  LOCAL
4000.1234.56c1  FOUND      LOCAL   Serial3/7      --no rif--
4000.1234.56c2  FOUND      LOCAL   Serial3/7      --no rif--
4000.3000.0100  FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
4000.4000.ff40  SEARCHING  LOCAL
4000.7470.00e7  SEARCHING  LOCAL
4000.ac0b.0001  FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
4001.0000.0064  FOUND      LOCAL   TokenRing0/0   0CB0.0011.3E71.A041.0DE5.0640
4001.3745.1088  FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
4100.0131.1030  FOUND      LOCAL   TokenRing0/0
10B0.FFF1.4041.0041.3E71.A041.0DE5.0640

DLSw NetBIOS Name reachability cache list
NetBIOS Name    status     Loc.    peer/port          rif
APPNCLT2        FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
```

The following is sample output from the **show dlsw reachability** command with the **mac-address** keyword:

```
Router# show dlsw reachability mac-address 4000.00000306

DLSw MAC address reachability cache list
Mac Addr        status     Loc.    peer/port          rif
4000.0000.0306  FOUND      LOCAL   TokenRing0/0   0CB0.0011.3E71.A041.0DE5.0640
```

The following is sample output from the **show dlsw reachability** command with the **netbios-names** keyword:

```
Router# show dlsw reachability netbios-names

DLSw NetBIOS Name reachability cache list
NetBIOS Name    status     Loc.    peer/port          rif
APPNCLT2        FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
```

Table 31 describes the significant fields shown in the display.

Table 31 show dlsw reachability Field Descriptions

Field	Description
Mac Addr	MAC address of station being sought (destination MAC address of canureach_ex packet).
NetBIOS Name	NetBIOS name of station being sought (destination MAC address of NQ_ex packet).

Table 31 show dlsw reachability Field Descriptions (continued)

Field	Description
status	Result of station search. The status can be one of the following: • FOUND—Station has recently sent a broadcast or responded to a broadcast. • SEARCHING—Router has sent a broadcast to this station and is waiting for a response. • NOT_FOUND—Negative caching is on, and the station has not responded to queries. • UNCONFIRMED—Station is configured, but DLSw has not verified it. • VERIFY—Cache information is being verified because cache is going stale, or the user configuration is being verified.
Loc.	Location of station. LOCAL indicates that the station is on the local network. REMOTE indicates that the station is on the remote network.
peer/port	Peer/port number. If the Loc. field lists a REMOTE station, the peer/port field indicates the peer through which the remote station is reachable. If the Loc. field lists a LOCAL station, the peer/port field indicates the port through which the local station is reachable. For ports, the port number and slot number are given. Pxxx-Syyy denotes port xxx slot yyy. If the station is reachable through a bridge group, that is shown by TBridge-xxx.
rif	Displays the Routing Information Field (RIF) in the cache. This column applies only to LOCAL stations. If the station was reached through a medium that does not support RIFs (such as Synchronous Data Link Control [SDLC] or Ethernet) then "--no rif--" is shown.

show dlsw statistics

To display the number of frames that have been processed in the local, remote, and group cache, use the **show dlsw statistics** command in privileged EXEC mode.

show dlsw statistics [**border-peers**]

Syntax Description

border-peers	(Optional) Displays the number of frames processed in the local, remote, and group caches.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw statistics** command. The output displays the number of frames processed in the local, remote, and group cache.

```
Router# show dlsw statistics border-peers

100 Border Peer Frames processed
10 Border frames found Local
20 Border frames found Remote
17 Border frames found Group Cache
```

show dlsw transparent cache

To display the master circuit cache for each transparent bridged domain, use the **show dlsw transparent cache** command in privileged EXEC mode.

show dlsw transparent cache

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Issue the **show dlsw transparent cache** command on the master router of the transparent bridged domain.

Examples

The following is sample output from the **show dlsw transparent cache** command:

```
Router# show dlsw transparent cache

Interface Ethernet0/1
 Circuit Cache
local addr(lsap)    remote addr(dsap)  state          Owner
0000.3028.92b6(08)  0007.0db1.238c(08) POSITIVE        SELF
0000.3028.92b6(08)  0008.dec3.609e(12) NEGATIVE        0009.fa50.0b1c
Total number of circuits in the Cache:2
```

show dlsw transparent map

To display MAC address mappings on the local router and any mappings for which the local router is acting as backup for a neighbor peer, use the **show dlsw transparent map** command in privileged EXEC mode.

show dlsw transparent map

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Issue the **show dlsw transparent map** command to ensure that the local MAC address is the address created in the **dlsw transparent map** command. The command should be issued on all the routers configured for the Ethernet Redundancy feature to ensure the local MAC addresses match.

Examples

The following is sample output from the **show dlsw transparent map** command on two routers configured for the Ethernet Redundancy feature:

```
Router6# show dlsw transparent map

Interface Ethernet6/2
      LOCAL Mac          REMOTE MAC      BACKUP
      ---------          ----------      ------
    0008.dec3.0080     0008.dec3.609e    0007.7fb0.1080     STATIC
    0008.dec3.0040     0008.dec3.609e    0007.7fb0.1080     DYNAMIC(Passive)

Router7# show dlsw transparent map

Interface Ethernet0/1
      LOCAL Mac          REMOTE MAC      BACKUP
      ---------          ----------      ------
    0008.dec3.0080     0008.dec3.609e    0006.3a0a.1a55     DYNAMIC(Passive)
    0008.dec3.0040     0008.dec3.609e    0006.3a0a.1a55     STATIC
```

The output from Router 6 and Router 7 shows the created MAC addresses are 0008.dec3.0080 and 0008.dec3.0040.

show dlsw transparent neighbor

To display data-link switching plus (DLSw) neighbors in a transparent bridged domain, use the **show dlsw transparent neighbor** command in privileged EXEC mode.

show dlsw transparent neighbor

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw transparent neighbor** command:

```
Router# show dlsw transparent neighbor

Interface ATM0.1
0006.e278.6c0e  SELF                    Master
0009.fa50.0b1c  Rcvd Master-Accepted     VALID
```

The output shows that Router 7 is the master router whose MAC address is 0006.e278.6c0e. The other router, with a MAC address of 0009.fa50.0b1c, is a slave router on the common domain. The master router received a packet from the slave and notes the router is VALID.

show drip

To display the status of the duplicate ring protocol (DRiP) database for a router or an Route Switch Module (RSM), use the **show drip** command in privileged EXEC mode.

show drip

Syntax Descriptions

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

```
Router# show drip

DRIP Database for Mgmt Domain Fast Ethernet4/0
---------------------------------------------------
Mac Address 0010-A6AE-B440
Vlan     100    Status    30 : l-active, l-config,

Mac Address 0010-2F72-C800
Vlan      20    Status    0C : r-active, r-config,
Vlan    1003    Status    0C : r-active, r-config,

Statistics:
Advertisements received            126
Advertisements processed           1
Advertisements transmitted         131
Last revision transmitted          0x84
Last changed revision transmitted  0x2
```

Related Commands

Command	Description
clear drip counters	Clears DRiP counters.
interface vlan	Configures a Token Ring or Ethernet interface on the RSM.
show vlans	Displays virtual LAN subinterfaces.

show dspu

To display the status of the downstream physical unit (DSPU) feature, use the **show dspu** command in privileged EXEC mode.

show dspu [**pool** *pool-name* | **pu** {*host-name* | *pu-name*}] [**all**]

Syntax Description

pool *pool-name*	(Optional) Name of a pool of logical unit (LU)s (as defined by the **dspu pool** command).
pu	(Optional) Name of defined physical unit (PU) (as defined by either the **dspu pu** or the **dspu host** command).
host-name	Name of a host defined in a **dspu host** command.
pu-name	Name of a PU defined in a **dspu pu** command.
all	(Optional) Displays a detailed status.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dspu** command. It shows a summary of the DSPU status.

```
Router# show dspu

dspu host HOST_NAMEA interface PU STATUS ssssssss
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
dspu host HOST_NAMEB interface PU STATUS ssssssss
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
dspu pu PU_NAMEE interface PU STATUS ssssssss
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
dspu pu PU_NAMEF interface PU STATUS ssssssss
```

```
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
```

The following is sample output from the **show dspu** command with the **pu** keyword:

```
Router# show dspu pu putest

dspu pu PUTEST interface PU STATUS ssssssss
RMAC remote_mac RSAP remote_sap LSAP local_sap
XID xid RETRIES retry_count RETRY_TIMEOUT retry_timeout
WINDOW window_size MAXIFRAME max_iframe
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
```

The following is sample output from the **show dspu** command with the **all** keyword:

```
Router# show dspu pu putest all

dspu pu PUTEST interface PU STATUS ssssssss
RMAC remote_mac RSAP remote_sap LSAP local_sap
XID xid RETRIES retry_count RETRY_TIMEOUT retry_timeout
WINDOW window_size MAXIFRAME max_iframe
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LU nnn PEER PU HOST_NAMEA PEER LU nnn STATUS tttttttt
       FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LU nnn PEER PU HOST_NAMEA PEER LU nnn STATUS tttttttt
       FRAMES RECEIVED nnnnnn, FRAMES SENT nnnnnn
LU nnn PEER PU HOST_NAMEB PEER LU nnn STATUS tttttttt
       FRAMES RECEIVED nnnnnn, FRAMES SENT nnnnnn
```

The following example shows a summary of the LUs in a pool:

```
Router# show dspu pool poolname

dspu pool poolname host HOST_NAMEA lu start-lu end-lu
```

The following example shows the details of all the LUs in a pool:

```
Router# show dspu pool poolname all

dspu pool poolname host HOST_NAMEA lu start-lu end-lu
DSPU POOL poolname INACTIVITY_TIMEOUT timeout-value
lu nnn host HOST_NAMEA peer lu nnn pu PU_NAMEF status tttttttt
lu nnn host HOST_NAMEA peer lu nnn pu PU_NAMEF status tttttttt
lu nnn host HOST_NAMEA peer lu nnn pu PU_NAMEF status tttttttt
```

show extended channel backup

To display information about the Common Link Access for Workstations (CLAW) and offload commands for each backup group configured on Cisco Mainframe Channel Connection (CMCC) channel interfaces, use the **show extended channel backup** command in privileged EXEC mode.

show extended channel *slot*/*port* **backup** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
backup	Displays all **claw** or **offload** commands associated with the backup group.
ip-address	(Optional) Displays information about all devices in the backup group defined by the *ip-address* argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel backup** command:

```
Router# show extended channel 0/1 backup

Mode     Path Device IP Address: 10.11.198.2
OFFLOAD  E200   50  CISCOVM  RISPIX   TCPIP    TCPIP    TCPIP    API
OFFLOAD  E300   50  CISCOVM  RISPIX   TCPIP    TCPIP    TCPIP    API
Last statistics 4 seconds old, next in 6 seconds
```

Related Commands

Command	Description
claw (backup)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (backup)	Configures a backup group of Offload devices.

show extended channel cmgr

To display information about the Cisco Multipath Channel (CMPC+) transmission group (TG) connection manager, use the **show extended channel cmgr** command in privileged EXEC mode.

show extended channel *slot*/*port* **cmgr** [*tg-name*]

Syntax Description

slot	Slot number.
port	Physical channel interface port number.
tg-name	(Optional) Name of the TG.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid on the Channel Interface Processor (CIP)'s virtual channel interface or the Channel Port Adapter (CPA)'s physical channel interface.

Examples

The following is sample output from the **show extended channel cmgr** command:

```
Router# show extended channel 3/2 cmgr

CMGR:MPCPTG2  Type=PTP
  Local Group Token:0500128933                  Remote Group Token :0500993355
  Local VC Token   :0500109002                  Local Conn. Token  :0500109003
  Remote VC Token  :0500201002                  Remote Conn. Token :0500201002
  VC Status        :Active                      Connection Status  :Active

CMGR:MPCPTG3   Type=PTP
  Local Group Token:050014573                 Remote Group Token :05008984300
  Local VC Token   :0500109044                Local Conn. Token  :0500109066
  Remote VC Token  :0500201095                Remote Conn. Token :0500201088
  VC Status        :Active                    Connection Status  :Active
```

Table 32 describes the significant fields shown in the display.

Table 32 show extended channel cmgr Field Descriptions

Field	Description
Local Group Token	Cisco Mainframe Channel Connection (CMCC)'s Multi-Path Channel plus (MPC+) group token for this TG.
Remote Group Token	Host's MPC+ group token for this TG.
Type	Connection manager type supported is point-to-point (PTP).
Local VC Token	CMCC adapter's token for the connection manager's virtual circuit.
Remote VC Token	Host's token for the connection manager's virtual circuit.
VC Status	Valid states for a VC are: • Reset—Awaiting a connection manager virtual circuit activate indication from the host. • Active—Connection manager virtual circuit active indication was received from the host and CMCC adapter has sent a virtual circuit active indication to the host. The virtual circuit is now ready to send receive connection requests.
Local Conn.Token	CMCC's token for the connection manager's connection.
Remote Conn.Token	Host's token for the connection manager's connection.
Connection Status	Valid states for a connection manager's connection are: • Reset—Awaiting a connection manager connection request from the host. • Active—Connection is active. The host has sent a connection request and the CMCC adapter has responded with a confirmation of the connection.

Related Commands

Command	Description
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.

show extended channel cmpc

To display information about each Cisco Multipath Channel (CMPC) or CMPC+ subchannel configured on the specified channel interface, use the **show extended channel cmpc** command in privileged EXEC mode.

show extended channel *slot*/*port* **cmpc** [*path* [*device*]]

Syntax Description

slot	Slot number.
port	Physical channel interface port number.
path	(Optional) Logical channel path.
device	(Optional) Two-digit hexadecimal value that specifies a device address of the CPMC or CMPC+ subchannel. If specified, only status for that CMPC or CMPC+ device is displayed. If not specified, status for all CMPC or CMPC+ devices for the specified path is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.0(3)T	Support was added for the CMPC+ feature.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the Cisco Mainframe Channel Connection (CMCC) adapter physical interfaces.

Examples

The following is sample output on a Cisco 7500 router from the **show extended channel cmpc** command:

```
Router# show extended channel 3/0 cmpc c020

     Path Dv  TGName    Dir    Bfrs  Status
CMPC C020 46  MVS2ISRA  READ   10    Active
CMPC C020 47  MVS2ISRA  WRITE  16    Active
CMPC C020 4A  MVS2ISR1  READ   7     Active
CMPC C020 4B  MVS2ISR1  WRITE  16    Active
CMPC C020 4C  MVS2ISR2  READ   7     Active
CMPC C020 4D  MVS2ISR2  WRITE  16    Active
CMPC C020 4E  MVS2TN    READ   0     Inactive
CMPC C020 4F  MVS2TN    WRITE  0     Inactive
```

Table 33 describes the specified fields shown in the display.

Table 33 show extended channel cmpc Field Descriptions

Field	Description
Path	CMPC or CMPC+ channel path configured.
Dv	CMPC or CMPC+ subchannel device configured.
TGName	TG name configured for the CMPC or CMPC+ subchannel.
Dir	Identifies this CMPC or CMPC+ subchannel as READ or WRITE.
Bfrs	On the read subchannel, this is the number of 4 KB-size pages that virtual telecommunications access method (VTAM) has allocated for each Read. This will match the MAXBFRU value configured in the VTAM Transport Resource List (TRL) major node. On the write subchannel, this is the maximum number of 4-KB pages VTAM can write to the CMCC adapter for a single channel I/O. The value will always be 16 for the write subchannel because the Channel Interface Processor (CIP)always allows VTAM to write up to 64 KB per channel I/O.
Status	State of the CMPC or CMPC+ subchannel. Valid values are: • Shutdown—CMCC adapter interface for this CMPC or CMPC+ subchannel is shut down. In this state, the Bfrs value is not available and will be displayed as zeros. • Inactive—CMPC or CMPC+ subchannel is not active. • XID2 Pending—exchange identification (XID)2 handshaking in progress. • Active—XID2 exchange completed; CMPC or CMPC+ subchannel is active. • Active**+**—XID2 exchange is complete; subchannel is active in High-Performance Data Transfer (HPDT) mode.

Related Commands

Command	Description
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.
tg (CMPC)	Defines LLC connection parameters for the CMPC transmission group.
tg (CMPC+)	Defines IP connection parameters for the CMPC+ transmission group.
show extended channel cmgr	Displays information about the MPC+ transmission group connection manager.

show extended channel connection-map llc2

To display the number of active Logical Link Control, type 2 (LLC2) connections for each service access point (SAP) and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP, use the **show extended channel connection-map llc2** command in privileged EXEC mode.

show extended channel *slot*/*port* **connection-map llc2**

Syntax Description

slot	Slot number.
port	Port number.
connection-map llc2	Displays a connection map of LLC2 connections.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0(3)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel connection-map llc2** command is valid only on the virtual channel interfaces.

Examples

The following is sample output from the **show extended channel connection-map llc2** command:

```
Router# show extended channel 1/2 connection-map llc2

LAN Token  0 Adapter   0 4000.7000.0747
 Local SAP=08 LLC2 Connections=4   CSNA Port=1 Path=C200 Device=60
 Local SAP=0C LLC2 Connections=4   CSNA Port=1 Path=C200 Device=60
 Local SAP=10 LLC2 Connections=2   CSNA Port=1 Path=C200 Device=60
 Local SAP=14 LLC2 Connections=0   CSNA Port=1 Path=C200 Device=60

LAN Token  1 Adapter   1 4000.7000.0767
 Local SAP=08 LLC2 Connections=3   CSNA Port=1 Path=C200 Device=61
 Local SAP=0C LLC2 Connections=3   CSNA Port=1 Path=C200 Device=61
 Local SAP=10 LLC2 Connections=2   CSNA Port=1 Path=C200 Device=61
 Local SAP=14 LLC2 Connections=2   CSNA Port=1 Path=C200 Device=61

LAN Token  2 Adapter   2 4000.7000.0737
 No SAPs open on this interface

 Total : SAPs opened = 8      Connections active = 20
```

show extended channel csna

To display information about the cisco systems network architecture (CSNA) subchannels configured on the specified Cisco Mainframe Channel Connection (CMCC) interface, use the **show extended channel csna** command in privileged EXEC mode.

show extended channel *slot/port* **csna** [*path* [*device*]] [**admin** | **oper** | **stats**]

Syntax Description

slot	Slot number.
port	Port number.
path	(Optional) A hexadecimal value in the range from 0000 to FFFF. This specifies the data path and consists of two digits for the physical connection (either on the host or on the ESCON Director switch), one digit for the control unit address, and one digit for the channel logical address. If not specified, information is displayed for all CSNA subchannels configured on the selected interface.
device	(Optional) A hexadecimal value in the range from 00 to FE. This is the unit address associated with the control unit number and path as specified in the host input/output configuration program (IOCP) file. If not specified, information is displayed for all CSNA subchannels configured with the specified path on the selected interface.
admin	(Optional) Displays configured values for CSNA channel devices. If neither **admin**, **oper**, nor **stats** is specified, **admin** is the default.
oper	(Optional) Displays operational values for CSNA channel devices.
stats	(Optional) Displays statistics for CSNA channel devices.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0(3)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The information that is displayed by this command is generally useful for diagnostic tasks performed by technical support personnel only.

Examples

The following is sample output from the **show extended channel csna** command. Three examples are provided, one for each type of output as specified by the **admin**, **oper**, and **stats** keywords.

The following example displays the configured values for all CSNA devices on interface channel 1/0:

```
Router# show extended channel 1/0 csna admin

     Path Dv  maxpiu       time-delay   length-delay
```

```
CSNA C200 60  64000        100          64000
CSNA C200 61  64000        100          64000
CSNA C200 62  64000        100          64000
```

The following example displays operational data for all CSNA devices configured on interface channel 1/0. The channel interface must be up (no shut) for this information to be displayed.

```
Router# show extended channel 1/0 csna oper

     Path Dv Status       SlowDown  maxpiu       time-delay   length-delay
CSNA C200 60 setupComplet off       64000        100          64000
CSNA C200 61 setupComplet off       64000        100          64000
CSNA C200 62 setupComplet off       64000        100          64000
```

The following example displays CSNA statistics for subchannel path c200, device 60. The channel interface must be up (no shut) for this information to be displayed. If the maxpiu value is reconfigured while the CSNA subchannel is active (setupComplete) then the maxpiu value displayed by the **oper** keyword is the old, operational value.

```
Router# show extended channel 1/0 csna c200 60 stats

CSNA     C200 60
Blocks Transmitted =   38979079  Received =   38979075
Bytes  Transmitted =  79251477K  Received =      13554
Slow downs Sent =           0  Received =          0
Txd by maxpiu      : Blocks =          0   Bytes =         0
Txd by time-delay  : Blocks =        222   Bytes =     12522
Txd by length-delay: Blocks =          0   Bytes =         0
```

Table 34 describes the specified fields shown in the displays.

Table 34 show extended channel csna Field Descriptions

Field	Description
Path	Path from the CSNA configuration.
Dev	Device address from the CSNA configuration.
Status	State of the CSNA device. One of the following values: • closed—Subchannel is closed. • pendingOpen—An Open Subchannel command has been received from virtual telecommunications access method (VTAM). • open—Subchannel is open. • pendingSetup—VTAM has queried Channel Interface Processor (CIP) for all configured MAC adapters. • setupComplete—All internal MAC adapter information has been collected from the CIP. The CSNA subchannel is operational. • pendingClose—A Close Subchannel command has been received from VTAM. • unknown—Current state of the CSNA subchannel cannot be determined.

Table 34 show extended channel csna Field Descriptions (continued)

Field	Description
SlowDown	Status of flow control for the CSNA device. • off—Subchannel is normal (both CSNA and VTAM are able to send data. • sent— CSNA has put VTAM into a slow down state for this CSNA subchannel. • received—VTAM has put the CSNA subchannel into a slow down state. • both—Both VTAM and the CSNA subchannel are in a slow down state. • unknown—Current state of flow control on this CSNA subchannel cannot be determined.
maxpiu	Maximum size of a channel I/O block that the CSNA subchannel can send to the host. This value may differ from the configured maxpiu value if the value is reconfigured while the CSNA subchannel is active (setupComplete). CSNA blocks Systems Network Architecture (SNA) frames into channel I/O blocks which must not exceed the maxpiu value. A length-delay value less than the maxpiu value can cause the channel I/O blocks to be limited to the lower value. The maxpiu value may be reconfigured while the subchannel is operational but the new maxpiu value does not take effect until the subchannel is reinitialized (in other words, until the XCA major node is recycled). In this case, the maxpiu value displayed with the **admin** keyword will be the new, configured value while the maxpiu displayed by the **oper** keyword will be the old, operational value.
time-delay	CSNA blocks SNA frames destined for VTAM for time-delay milliseconds from the time the first SNA frame within a channel I/O block is blocked from sending. This can increase the overall throughput of CSNA by minimizing the number of channel I/O operations. However, blocking can induce response time latency of a transaction by up to the time-delay value. If time-delay=0, CSNA ignores length-delay and puts each frame into the channel I/O block for sending to the host. Even with a time-delay=0, CSNA may still block frames while waiting for a previous channel I/O to complete.
length-delay	CSNA blocks SNA frames destined for VTAM when the current block reaches the length-delay value in size (bytes). This will increase the chance of using larger block sizes for CSNA channel I/O. SNA frames are blocked up to either time-delay milliseconds or until the block reaches the length-delay size, at which time CSNA starts the channel I/O. The length-delay is ignored if larger than the maxpiu value. It can be used to force CSNA blocking to generate smaller I/O blocks than specified by maxpiu. In general, however, larger blocks result in better channel throughput and efficiency. A value of zero causes the length-delay value to be ignored; blocking is then controlled by the maxpiu and time-delay parameters.

Table 34 show extended channel csna Field Descriptions (continued)

Field	Description
Blocks Transmitted	Number of channel I/O blocks sent to VTAM from this CSNA subchannel. The Blocks Transmitted value may be higher than the total blocks for the Txd by maxpiu, Txd by time-delay, and Txd by length-delay counters. This is due to NULL blocks (8 bytes each with no data) that CSNA sends. The channel program used for link-state advertisement (LSA) traffic consists of a write/read CCW chain. When VTAM has data for CSNA it sends it with the write CCW. When the chained read CCW is executed CSNA will respond with any pending inbound data. If CSNA has no pending inbound data the read CCW is satisfied with an 8-byte header indicating no data.
Blocks Received	Number of channel I/O blocks received from VTAM by this CSNA subchannel.
Slow downs Sent	Number of times CSNA put VTAM into a slowdown (flow control) for this subchannel device.
Slow downs Received	Number of times VTAM put CSNA into a slowdown (flow control) for this subchannel.
Txd by maxpiu Blocks/Bytes	Number of channel I/O blocks and bytes sent to VTAM by this CSNA subchannel because the size of the channel I/O block reached the maxpiu value configured for this subchannel.
Txd by time-delay Blocks/Bytes	Number of channel I/O blocks and bytes sent to VTAM by this CSNA subchannel because the blocking time delay configured for this subchannel expired.
Txd by length-delay Blocks/Bytes	Number of channel I/O blocks and bytes sent to VTAM by this CSNA subchannel because the blocking length delay configured for this subchannel was reached.

Related Commands

Command	Description
csna	Configures SNA support on a CMCC physical channel interface and specifies the path and device/subchannel on a physical channel of the router to communicate with an attached mainframe.

show extended channel icmp-stack

To display information about the Internet Control Message Protocol (ICMP) stack running on the Cisco Mainframe Channel Connection (CMCC) channel interfaces, use the **show extended channel icmp-stack** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **icmp-stack** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
ip-address	(Optional) IP address specified by the **offload** interface configuration command or the **tn3270-server pu** command.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	The Alias addresses field was added to the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel icmp-stack** command is valid on both physical and virtual channel interfaces.

Examples

The following is sample output from the **show extended channel icmp-stack** command:

```
Router# show extended channel 0/1 icmp-stack

ICMP Statistics for IP Address 10.11.198.2
  InMsgs         : 3            InErrors        : 0            InDestUnreachs: 0
  InTimeExcds    : 0            InParmProbs     : 0            InSrcQuenchs  : 0
  InRedirects    : 0            InEchos         : 3            OutEchoReps   : 3
  OutTimestamps  : 0            OutTimestampReps: 0            OutAddrMasks  : 0
  OutAddrMaskReps: 0
ICMP Statistics for IP Address 10.11.198.3
  InMsgs         : 1            InErrors        : 0            InDestUnreachs: 0
  InTimeExcds    : 0            InParmProbs     : 0            InSrcQuenchs  : 0
  InRedirects    : 0            InEchos         : 1            OutEchoReps   : 1
  OutTimestamps  : 0            OutTimestampReps: 0            OutAddrMasks  : 0
  OutAddrMaskReps: 0
```

The following is sample output from the **show extended channel icmp-stack** for an offload device at real IP address 10.10.21.3 and alias IP address 10.2.33.88:

```
Router# show extended channel 3/1 icmp-stack

ICMP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  InMsgs         : 0            InErrors        : 0            InDestUnreachs: 0
  InTimeExcds    : 0            InParmProbs     : 0            InSrcQuenchs  : 0
  InRedirects    : 0            InEchos         : 0            OutEchoReps   : 0
  OutTimestamps  : 0            OutTimestampReps: 0            OutAddrMasks  : 0
  OutAddrMaskReps: 0
```

Table 35 describes the specified fields shown in the display.

Table 35 show extended channel icmp-stack Field Descriptions

Field	Description
Alias addresses	Virtual IP addresses assigned to the real IP address of an offload device.
InMsgs	Total number of Internet Control Message Protocol (ICMP) messages that the entity received. Note that this counter includes all those counted by icmpInErrors.
InErrors	Number of ICMP messages that the entity received but determined as having ICMP-specific errors (for example, bad ICMP checksums, bad length).
InDestUnreachs	Number of ICMP Destination Unreachable messages received.
InTimeExcds	Number of ICMP Time Exceeded messages received.
InParmPrbs	Number of ICMP Parameter Problem messages received.
InSrcQuenchs	Number of ICMP Source Quench messages received.
InRedirects	Number of ICMP Redirect messages received.
InEchos	Number of ICMP Echo (request) messages received.
OutEchoReps	Number of ICMP Echo Reply messages sent.
OutTimestamps	Number of ICMP Timestamp (request) messages sent.
OutTimestampReps	Number of ICMP Timestamp Reply messages sent.
OutAddrMasks	Number of ICMP Address Mask Request messages sent.
OutAddrMaskReps	Number of ICMP Address Mask Reply messages sent.

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
pu (TN3270)	Creates a physical unit (PU) entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.

show extended channel ip-stack

To display information about the IP stack running on Cisco Mainframe Channel Connection (CMCC) channel interfaces, use the **show extended channel ip-stack** command in user EXEC or privileged EXEC mode.

show extended channel *slot/port* **ip-stack** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
ip-address	(Optional) IP address specified by the **offload** interface configuration command or the **tn327-server pu** command.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	The Alias addresses field was added to the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel ip-stack** command is valid on both physical and virtual channel interfaces.

Examples

The following is sample output from the **show extended channel ip-stack** command:

```
Router# show extended channel 0/1 ip-stack

IP Statistics for IP Address 10.11.198.2
  Forwarding     : no           DefaultTTL     : 64          InReceives   : 165
  InHdrErrors    : 0            InAddrErrors   : 0           ForwDatagrams: 0
  InUnknownProtos: 0            InDiscards     : 0           InDelivers   : 165
  OutRequests    : 157          OutDiscards    : 0           OutNoRoutes  : 0
  ReasmTimeout   : 60           ReasmReqds     : 0           ReasmOKs     : 0
  ReasmFails     : 0            FragOKs        : 0           FragFails    : 0
  FragCreates    : 0            RoutingDiscards: 0
IP Statistics for IP Address 10.11.198.3
  Forwarding     : no           DefaultTTL     : 64          InReceives   : 77
  InHdrErrors    : 0            InAddrErrors   : 0           ForwDatagrams: 0
  InUnknownProtos: 0            InDiscards     : 0           InDelivers   : 77
  OutRequests    : 78           OutDiscards    : 0           OutNoRoutes  : 0
  ReasmTimeout   : 60           ReasmReqds     : 0           ReasmOKs     : 0
  ReasmFails     : 0            FragOKs        : 0           FragFails    : 0
  FragCreates    : 0            RoutingDiscards: 0
```

The following is sample output from the **show extended channel ip-stack** for an offload device at real IP address 10.10.21.3 and alias IP address 10.2.33.88:

```
Router# show extended channel 3/1 ip-stack

IP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  Forwarding     : no           DefaultTTL     : 64           InReceives   : 16
  InHdrErrors    : 0            InAddrErrors   : 0            ForwDatagrams: 0
  InUnknownProtos: 0            InDiscards     : 0            InDelivers   : 16
  OutRequests    : 7            OutDiscards    : 0            OutNoRoutes  : 0
  ReasmTimeout   : 60           ReasmReqds     : 0            ReasmOKs     : 0
  ReasmFails     : 0            FragOKs        : 0            FragFails    : 0
  FragCreates    : 0            RoutingDiscards: 0
```

The following is sample output from the **show extended channel ip-stack** when you specify the alias IP address for an offload device at real IP address 10.10.21.3:

```
Router# show extended channel 3/1 ip-stack 10.2.33.88

IP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  Forwarding     : no           DefaultTTL     : 64           InReceives   : 16
  InHdrErrors    : 0            InAddrErrors   : 0            ForwDatagrams: 0
  InUnknownProtos: 0            InDiscards     : 0            InDelivers   : 16
  OutRequests    : 7            OutDiscards    : 0            OutNoRoutes  : 0
  ReasmTimeout   : 60           ReasmReqds     : 0            ReasmOKs     : 0
  ReasmFails     : 0            FragOKs        : 0            FragFails    : 0
  FragCreates    : 0            RoutingDiscards: 0
```

Table 36 describes the specified fields shown in the display.

Table 36 show extended channel ip-stack Field Descriptions

Field	Description
Alias addresses	Virtual IP addresses assigned to the real IP address of an offload device.
Forwarding	Indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host). Note that for some managed nodes this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a "badValue" response if a management station attempts to change this object to an inappropriate value.
DefaultTTL	The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity whenever a TTL value is not supplied by the transport layer protocol.
InReceives	Total number of input datagrams received from interfaces, including those received in error, for this IP address instance.
InHdrErrors	Number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.

Table 36 show extended channel ip-stack Field Descriptions (continued)

Field	Description
InAddrErrors	Number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ForwDatagrams	Number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities that do not act as IP Gateways, this counter will include only those packets that were source-routed through this entity, and the source-route option processing was successful.
InUnknownProtos	Number of locally-addressed datagrams received but discarded because of an unknown or unsupported protocol.
InDiscards	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but that were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting reassembly.
InDelivers	Total number of input datagrams delivered to IP user protocols (including Internet Control Message Protocol (ICMP)).
OutRequests	Total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for sending. Note that this counter does not include any datagrams counted in ipForwDatagrams.
OutDiscards	Number of output IP datagrams for which no problem was encountered to prevent sending them to their destination, but that were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutNoRoutes	Number of IP datagrams discarded because no route could be found to send them to their destination. Note that this counter includes any packets counted in ipForwDatagrams that meet this no-route criterion. Note that this includes any datagrams that a host cannot route because all of its default gateways are down.
ReasmTimeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
ReasmReqds	Number of IP fragments received that needed to be reassembled at this entity.
ReasmOKs	Number of IP datagrams reassembled.
ReasmFails	Number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so on). Note that this is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
FragOKs	Number of IP datagrams that have been fragmented at this entity.
FragFails	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their Don't Fragment flag was set.

Table 36 show extended channel ip-stack Field Descriptions (continued)

Field	Description
FragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
RoutingDiscards	Number of routing entries that were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free buffer space for other routing entries.

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
pu (TN3270)	Creates a physical unit (PU) entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.

show extended channel lan

To display the internal LANs and adapters configured on a Cisco Mainframe Channel Connection (CMCC) adapter, use the **show extended channel lan** command in user EXEC or privileged EXEC mode.

show extended channel *slot/port* **lan** [*tokenring* [*lan-id* [*adapno*]]]

Syntax Description

slot	Slot number.
port	Port number.
tokenring	(Optional) Specify the CMCC internal LAN type to be displayed.
lan-id	(Optional) Specify the CMCC internal LAN number to be displayed.
adapno	(Optional) Specify the CMCC internal adapter number on the selected internal LAN to be displayed.

Defaults

Display all internal LANs and adapters on the selected channel interface.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel lan** command:

```
Router# show extended channel 3/2 lan

Lan TokenRing 0
        Adapno Mac Address    Name     Vcnum
             0 4000.1111.1112            544
            20 4000.1111.2200            564
            30 4000.3030.0101            574
Lan TokenRing 1
        source-bridge 207 1 2002
        Adapno Mac Address    Name     Vcnum
             1 4000.2222.2222            545
Lan TokenRing 2
        source-bridge 50 1 1500
```

```
        Adapno Mac Address    Name     Vcnum
             2 4000.3333.2222           546
Lan TokenRing 5
        source-bridge 112 1 3000
        Adapno Mac Address    Name     Vcnum
             5 4000.1234.5656           549
Lan TokenRing 9
        source-bridge 111 1 3000
        Adapno Mac Address    Name     Vcnum
             9 4000.9999.1111           553
Lan TokenRing 10
        source-bridge 110 1 3000
        Adapno Mac Address    Name     Vcnum
            10 4000.aaaa.1111           554
Lan TokenRing 20
        source-bridge 20 1 2002
        Adapno Mac Address    Name     Vcnum
            21 4000.2020.2020           565
```

Related Commands

Command	Description
adapter	Configures internal adapters.
lan	Configures an internal LAN on a CMCC adapter interface and enters internal LAN configuration mode.

show extended channel llc2

To display information about the Logical Link Control, type 2 (LLC2) sessions running on the Cisco Mainframe Channel Connection (CMCC) adapter interfaces, use the **show extended channel llc2** command in user EXEC or privileged EXEC mode.

show extended channel *slot/port* **llc2** [**admin** | **oper** | **stats**] [*lmac* [*lsap* [*rmac* [*rsap*]]]]

Syntax Description

slot	Slot number.
port	Port number.
admin	(Optional) Displys Shows configured values. This is the default.
oper	(Optional) Displays operational values for: • Internal adapters • Service access point (SAP)s opened on the internal adapters • LLC2 connections on the internal adapters
stats	(Optional) Displays statistics for: • Internal adapters • SAPs opened on the internal adapters • LLC connections on the internal adapters
lmac	(Optional) Local MAC address.
lsap	(Optional) Local SAP address, in the range from 0 to 256.
rmac	(Optional) Remote MAC address.
rsap	(Optional) Remote SAP address, in the range from 0 to 256.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0(3)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel llc2** command is valid on virtual channel interfaces.

To specify LLC information for internal adapters, perform the following asks:

- Specify a value for the *lmac* argument to get information for a specific internal adapter.
- Omit the *lmac* argument to display information for all internal adapters on the specified channel interface.

To display LLC information for SAPs opened on an internal adapter, perform the following tasks:

- Specify values for the *lmac* and *lsap* arguments to display information for a particular SAP.
- Specify a value for the *lmac* argument and "*' to display information for all SAPs opened on the specified channel adapter.

To display information for LLC2 connections on a channel interface, perform the following tasks:

- Specify values for the *lmac*, *lsap*, *rmac*, and *rsap* arguments to display information for a particular active LLC2 connection.
- Specify values for the *lmac*, *lsap*, and *rmac* arguments to display information for all LLC2 connections active between the specified remote MAC address and the specified local SAP opened on the specified internal adapter.
- Specify values for the *lmac* and *lsap* arguments and "*" to display information for all LLC2 connections active on the specified local SAP and the specified internal adapter and any remote MAC address the connections are active with.
- Specify a value for the *lmac* argument, "*" for the local SAP, and a value for the *rmac* argument to display information for all LLC2 connections active between the specified internal adapter and the remote MAC address.
- Specify a value for the *lmac* argument, "*" for the local SAP, and "*"' for the remote MAC address to display information for all active LLC2 connections on the specified internal adapter.

Examples

The following is sample output from the **show extended channel llc2** command. Three examples are provided, one for each type of output as specified by the **admin**, **oper**, and **stats** keywords.

The following sample displays the configured values for all LLC2 connections on channel 2/2:

```
Router# show extended channel 2/2 llc2 admin

    Lan Token adapter   0 0004.0004.0004
  t1-time   = 1000  tpf-time  = 1000  trej-time = 3200  tbusy-tim = 9600
  idle-time =60000  local-win =    7  recv-wind =    7  N2        =    8
  N1        = 1033  ack-delay =  100  ack-max   =    3  nw        =    0
```

Table 37 describes the specified fields shown in the display.

Table 37 show extended channel llc2 admin Field Descriptions—All LLC2 Connections

Field	Description
t1-time	Length of time in milliseconds the CMCC LLC2 link station waits for an acknowledgment to a sent I-frame before polling the remote LLC2 station.
tpf-time	Length of time in milliseconds the CMCC LLC2 link station waits for a final response to a poll before resending the original poll frame.
trej-time	Length of time in milliseconds the CMCC LLC2 link station waits for a correct frame after sending a reject command to a remote LLC2 station.
tbusy-time	Length of time in milliseconds the CMCC LLC2 link station waits before repolling a busy LLC2 station.
idle-time	Frequency of polls during periods of idle traffic.
local-win	Maximum number of I-frames that the CMCC LLC2 link station connection can send to the remote LLC2 station without receiving an acknowledgment.

Table 37 show extended channel llc2 admin Field Descriptions—All LLC2 Connections

Field	Description
recv-wind	Maximum number of I-frames that the CMCC LLC2 link station connection can receive without receiving an acknowledgment.
N2	Number of times the CMCC LLC2 link station connection will resend an unacknowledged I-frame.
N1	Maximum size of LLC frames supported by the CMCC LLC2 link station. The maximum size LLC frame supported on the CMCC is controlled by other factors including the largest interface MTU between the CMCC and the remote network device, and configured values at virtual telecommunications access method (VTAM) and at the end station.
ack-delay	Maximum amount of time the CMCC LLC2 link station allows received I-frames to remain unacknowledged. The CMCC LLC2 connection will acknowledge received I-frames within the ack-delay time.
ack-max	Maximum number of I-frames the Channel Interface Processor (CIP) LLC2 link station receives before sending an acknowledgment.
Nw	Working send window size. When I-frames sent by the CMCC are rejected by the remote LLC2 station, the CMCC LLC2 connection reduces its working send window size to 1. Then, for every subsequent I-frame sent by the CMCC LLC2 connection that is positively acknowledged by the remote LLC2 station, the CMCC LLC2 connection increases its working send window by the Nw value until the working send window reaches the configured local-window value.

The following sample displays the operational values for all LLC2 connections on channel 2/2:

```
Router# show extended channel 5/2 llc oper

  LAN Token  0 Adapter   0 4000.1010.2020
      Open SAPs=1
      Max SAPs Opened=1
```

Open SAPS is the number of SAPs opened on this internal MAC adapter. *Max SAPs Opened* is the number of SAPs concurrently opened on this internal MAC adapter since the last reset of the channel adapter of channel interface.

The following sample displays operational information for the specified SAP opened on a CMCC internal adapter:

```
Router# show extended channel 5/2 llc stats

LAN Token  0 Adapter   0 4000.1010.2020
      PDUsIn     =     223339    PDUsOut     =       9564
      OctetsIn   =    6949875    OctetsOut   =     307448
      TESTCmdsIn =     213293    TESTRspsOut =          2
      LocalBusies=          0    UnknownSAPs =          0
```

Table 38 describes the specified fields shown in the display. These statistics are available on the adapter because when LLC2 connections are deactivated, users can no longer retrieve the information per LLC2 connection.

Table 38 show extended channel llc2 stats Field Descriptions—All LLC2 Connections

Field	Description
PDUsIn	Protocol data units received by the internal adapter.
PDUsOut	Protocol data Units sent by the internal adapter.
OctetsIn	PDU bytes received by the internal adapter.
OctetsOut	PDU bytes sent by the internal adapter.
TESTCmdsIn	Number of TEST commands received destined for this MAC address.
TESTRspsOut	Number of TEST responses sent by this MAC address responding to TEST commands received.
Local Busies	Number of times LLC2 connection stations on this adapter entered a busy state, sent Receiver Not Ready (RNR)s to the remote LLC2 station.
UnknownSAPs	Number of frames received that are destined for a SAP that does not exist on this adapter.

The following sample displays operational information for the specified SAP opened on the internal adapter, 4000.1010.2020, configured on channel interface 5/2:

```
Router# show extended channel 5/2 llc2 oper 4000.1010.2020 04

  LAN Token  0 Adapter   0 4000.1010.2020
    Local SAP=04
      Open Connections=2
      Max Connections Opened=2
```

Table 39 describes the specified fields shown in the display.

Table 39 show extended channel llc2 oper Field Descriptions for Specified Interface

Field	Description
Open Connections	Number of LLC2 connections active on the SAP.
Max Connections	Highest number of LLC2 connections concurrently active on that SAP since the SAP has been active.

The following sample displays statistics for the specified SAP on the internal adapter, 4000.1010.2020 configured on channel interface 5/2:

```
Router# show extended channel 5/2 llc2 stats 4000.1010.2020 04

  LAN Token  0 Adapter   0 4000.1010.2020
    Local SAP=04
      TESTRspsIn     =          0  TESTCmdsOut    =          0
      XIDCmdsIn      =         14  XIDCmdsOut     =         16
      XIDRspsIn      =          4  XIDRspsOut     =          0
      UIFramesIn     =          0  UIFramesOut    =          0
      UIOctetsIn     =          0  UIOctetsOut    =          0
      ConnectOk      =          2  ConnectFail    =          0
      DiscNorm       =          0  DiscByTmr      =          0
      DiscByFRMRSent =          0  DiscByFRMRRcvd =          0
```

```
DMsInABM        =           0   SABMEsInABM     =           0
```

Table 40 describes the specified fields shown in the display. All statistics for SAPs are based on the time the SAP was last opened.

Table 40 show extended channel llc2 stats Field Descriptions for Specified Interface

Field	Description
TESTRspsIn	Number of TEST responses received on this SAP for TEST commands sent by VTAM (connect out).
TESTCmdsOut	Number of TEST commands sent by this SAP to explore for a remote MAC address (VTAM connect out).
XIDCmdsIN	Number of exchange identification (XID) commands received by this SAP from a remote link station.
XIDCmdsOut	Number of XID commands sent by this SAP to a remote link station.
XIDRspsIN	Number of XID responses received by this SAP from a remote link station.
XIDRspsOut	Number of XID responses sent by this SAP to a remote link station.
UIFramesIn	Number of Unnumbered I-frames received by this SAP from a remote link station.
UIFramesOut	Number of Unnumbered I-frames sent by this SAP to a remote link station.
UIOctetsIn	Number of Unnumbered I-frame bytes received by this SAP from a remote link station.
UIOctetsOut	Number of Unnumbered I-frame bytes sent by this SAP to a remote link station.
ConnectOk	Number of successful LLC2 connection attempts on this SAP.
ConnectFail	Number of LLC2 connections that failed.
DiscNorm	Number of normal LLC2 connection disconnections.
DisByTmr	Number of LLC2 connections disconnected due to the CMCC LLC2 link station not getting responses to polls from the remote LLC2 station, typically due to the remote station being powered off or a severe network failure or congestion. The CMCC LLC2 stack generates an event each time it detects this condition. The event can be configured to generate a NetView alert, SNMP trap, and a router console message.
DiscByFRMRSent	Number of times a CMCC LLC2 connection disconnected after detecting a protocol violation and sending a FRNR to the remote LLC2 station. The CMCC LLC2 link station generates an event each time it detects this condition. The event can be configured to generate a NetView alert, an SNMP trap, and a router console message.
DiscByFRMRRcvd	Number of times the CMCC LLC2 connection disconnected after the remote LLC2 station detected a protocol violation and sent an FRMR to the CMCC LLC2 link station. The CMCC LLC2 stack generates an event each time it detects this condition. The event can be configured to generate a NetView alert, an SNMP trap, and a router console message.

Table 40 show extended channel llc2 stats Field Descriptions for Specified Interface

Field	Description
DMsInABM	Number of times the CMCC LLC2 link station went into disconnect mode after receiving a disconnect mode (DM). The CMCC LLC2 stack generates an event each time it detects this condition. The event can be configured to generate a NetView alert, an SNMP trap, and a router console message.
SABMEDsInABM	Number of times the CMCC LLC2 link station went into disconnect mode after receiving a Set Asynchronous Balanced Mode Extended (SABME) from the LLC2 station. The CMCC LLC2 stack generates an event each time it detects this condition. The event can be configured to generate a NetView alert, an SNMP trap, and a router console message.

The following sample displays operation information for the specified CMCC link station:

```
Router# show extended channel 5/2 llc2 oper 4000.1010.2020 04 4000.1234.1030 18

  LAN Token  0 Adapter   0 4000.1010.2020
    Local SAP=04 Remote MAC=4000.1234.1030 Remote SAP=18 State=normal
      t1-time   = 1000  tpf-time  = 1000  trej-time = 3200  tbusy-tim = 9600
      idle-time =60000  local-win =    7  recv-wind =    7  N2        =    8
        N1-Send   = 4105  N1-Rcv    = 4105  ack-delay =  100  ack-max   =    3
Nw        =    0  Ww        =    7
      Last Ww Cause = neverInvoked
      Connection Time: 17:50:11
      Last modified: never
```

Table 41 explains parameters in use by the LLC2 connection. These parameters are the ones configured on the internal adapter 4000.0000.0001 at the time the LLC2 connection was established. If the LLC2 parameters on the internal adapter are changed while this connection is active, the connection will not reflect the changes to the adapter.

Table 41 show extended channel llc2 Field Descriptions for Internal LAN Adapter

Field	Description
State	• ADM (Asynchronous Disconnect Mode) • setup • conn • normal • busy • reject • await • awaitBusy

Table 41 show extended channel llc2 Field Descriptions for Internal LAN Adapter (continued)

Field	Description
State (continued)	• awaitReject • discConn • reset • error • pendDiscRsp The descriptions for each state can be found in Section 7.8.3, IOS 8802-2: 1989, ANSI/IEEE Std 802.2 - 1989.
t1-time	Length of time in milliseconds the CMCC LLC2 link station waits for an acknowledgment to a sent I-frame before polling the remote LLC2 station.
tpf-time	Length of time in milliseconds the CMCC LLC2 link station waits for a final response to a poll before resending the original poll frame.
trej-time	Length of time in milliseconds the CMCC LLC2 link station waits for a correct frame after sending a reject command to a remote LLC2 station.
tbusy-tim	Length of time in milliseconds the CMCC LLC2 link station waits before repolling a busy LLC2 station.
idle-time	Frequency of polls during periods of idle traffic.
local-win	Maximum number of I-frames that the CMCC LLC2 link station can send to the remote LLC2 station without receiving an acknowledgment.
recv-wind	Maximum number of I-frames that a CMCC LLC2 link station can receive without receiving an acknowledgment.
N2	Number of times a CMCC LLC2 link station will resend an unacknowledged I-frame.
N1-Send	Largest frame size this CMCC LLC2 link station is allowed to send.
N1-Rcv	Largest frame size this CMCC LLC2 link station can receive.
ack-delay	Maximum length of time in milliseconds the CMCC LLC2 link station allows received I-frames to remain unacknowledged. The Channel Interface Processor (CIP)LLC2 connection will acknowledge received I-frames within the ack-delay time.
ack-max	Maximum number of I-frames a CMCC LLC2 link station receives before sending an acknowledgment.
Nw	Working send window size. When I-frames sent by a CMCC LLC2 link station are rejected by the remote LLC2 station, the CMCC LLC2 link station reduces its working send window size to 1. Then, for every subsequent I-frame sent by the CMCC LLC2 connection that is positively acknowledged by the remote LLC2 station, the CMCC LLC2 link station increases its working send window by the Nw value until the working send window reaches the configured local-window value.
Ww	Current working window size for this LLC2 link station. This is the current number of unacknowledged I-frames that this LLC2 link station will send.

Table 41 show extended channel llc2 Field Descriptions for Internal LAN Adapter (continued)

Field	Description
Last Ww Cause	Last event that caused the working window to change values. Valid values are: • neverInvoked—This LLC2 station has not detected a condition to change the working window from the initial value at activation time. • lostData—The current working window value was changed due to loss of data by the remote LLC2 link station. • macLayerCongestion—The current working window value was changed due to the remote end station sending this LLC2 link station a Receiver Not Ready (RNR) frame.
Connection Time	Length of time this LLC2 connection has been active.
Last modified	Length of time since one of the LLC2 parameters for this connection was last modified.

The following sample displays statistics for the CMCC LLC2 link station connection between LMAC 4000.1010.2020 LSAP 04 and RMAC 4000.1234.1030 RSAP 18:

```
Router# show extended channel 5/2 llc2 stats 4000.1010.2020 04 4000.1234.1030 18

  LAN Token  0 Adapter   0 4000.1010.2020
    Local SAP=04 Remote MAC=4000.1234.1030 Remote SAP=18
      LocalBusies    =          0  RemoteBusies   =          0
      IFramesIn      =          1  IFramesOut     =          1
      IOctetsIn      =         19  IOctetsOut     =         21
      SFramesIn      =          0  SFramesOut     =          0
      REJsIn         =          0  REJsOut        =          0
      RetransmitsOut =          0  WwCountChanges =          0
```

Table 42 describes the specified fields shown in the display.

Table 42 show extended channel llc2 stats Field Descriptions

Field	Description
LocalBusies	Number of times the CMCC LLC2 link station entered the busy state. This state occurs for a CMCC LLC2 link station when there are *x* I-frames received from the remote LLC2 station on the CMCC queued to be sent over the channel to VTAM; Where *x* is two times the recv-wind value. The CMCC LLC2 link station will also enter into busy state whenever it receives a flow control command from VTAM.
RemoteBusies	Number of times the remote LLC2 link station entered into busy state.
IFramesIn	Number of LLC2 information frames received by the CMCC LLC2 link station from the remote link station.
IFramesOut	Number of LLC2 information frames sent by the CMCC link station to the remote link station.
IOctetsIn	Number of LLC2 information frame bytes received by the CMCC LLC2 link station from the remote link station.
IOctetsOut	Number of LLC2 information frame bytes sent by the CMCC link station to the remote link station.

Table 42 show extended channel llc2 stats Field Descriptions (continued)

Field	Description
SFramesIn	Number of LLC2 supervisory frames received by the CMCC link station from the remote link station. These include RRs, RNRs, and REJs.
SFramesOut	Number of LLC2 supervisory frames sent by the CMCC link station to the remote link station. These include RRs, RNRs and REJs.
REJsIn	Number of LLC2 REJ frames received by the CMCC link station from the remote link station. This field indicates the number of times the remote link station detected dropped I-frames sent from the CMCC LLC2 station.
REJsOut	Number of LLC2 REJ frames sent by the CMCC link station to the remote link station. This indicates the number of times the CMCC link station detected dropped I-frames sent by the remote link station.
RetransmitsOut	Number of I-frames the CMCC link station was required to resend.
WwCountChanges	Number of times the CMCC LLC2 link station changed its working send window (local-win). See the Nw field description in Table 40 for a description of when the LLC2 link stations working send window is changed.

Related Commands

Command	Description
adapter	Configures internal adapters.

show extended channel max-llc2-sessions

To display information about the number of Logical Link Control, type 2 (LLC2) sessions supported on the Cisco Mainframe Channel Connection (CMCC) adapter, use the **show extended channel max-llc2-sessions** command in privileged EXEC mode.

show extended channel *slot*/*port* **max-llc2-sessions**

Syntax Description

slot	Slot number.
port	Port number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0(3)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel max-llc2-sessions** command:

```
Router# show extended channel 1/2 max-llc2-sessions

Administrative max-llc2-sessions = 1000
Operational max-llc2_sessions = 1000
Highest concurrent LLC2 sessions = 30
LLC2 session allocation failures = 0
```

Table 43 describes the specified fields shown in the display.

Table 43 show extended channel max-llc2-sessions Field Descriptions

Field	Description
Administrative max-llc2-sessions	Maximum number of LLC2 sessions configured.
Operational max-llc2-sessions	Maximum number of LLC2 sessions configured on the CMCC adapter. This value differs from the value for the administrative max-llc2-sessions if the maximum number of LLC2 sessions is decreased by configuring a new value while the CMCC adapter's virtual interface is up. If the CMCC adapter's virtual interface is reset **shut** and **no shut** command, both the administrative and operational max-llc2-sessions numbers will match.

Table 43 show extended channel max-llc2-sessions Field Descriptions (continued)

Field	Description
Highest concurrent LLC2 sessions	Highest number of LLC2 sessions active concurrently since the CMCC adapter LLC2 was started. When the CMCC adapter llc2 is initiated, the following message displays: `%CIP1-6-MSG: %MSG802-6-LLC_START: Starting LLC-2 with a session capacity of 1000`
LLC2 session allocation failures	Number of times network devices tried to establish an LLC2 connection with the CMCC adapter and failed because the operational max-llc2-sessions limit was reached when the connection was attempted.

Related Commands

Command	Description
adapter	Configures internal adapters.
show extended channel connection-map llc2	Displays the number of active LLC2 connections for each service access point (SAP) and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP.

show extended channel packing names

To display Common Link Access for Workstations (CLAW) packing names and their connection state, use the **show extended channel packing names** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **packing names** [*path* [*device-address*]]

Syntax Description

slot	Slot number.
port	Port number.
path	(Optional) Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
device-address	(Optional) Hexadecimal value in the range from 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even numbered value.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel packing names** command:

```
Router# show extended channel 3/0 packing names

Path: C010  Devices: F2,F3 CLAW Link: 1

    Sublink            Link Names
       0                 CONTROL
       1               IP        IP
       2               CKSUM     CKSUM

Path: C030  Devices: F6,F7 CLAW Link: N

    Sublink            Link Names
  DISCONNECTED          CONTROL
  DISCONNECTED        IP        IP
  DISCONNECTED        CKSUM     CKSUM
```

Table 44 describes the specified fields shown in the display.

Table 44 show extended channel packing names Field Descriptions

Field	Description
Path	Path from the CLAW configuration. It indicates which port on the switch is used by the channel side of the configuration.
Devices	Device address for each device. One CLAW connection requires two devices. You need only specify the even numbered address.
CLAW Link	Established CLAW link number used for all CLAW packing messages. A number value indicates that a CONTROL sublink is connected. "N" indicates that a control sublink is disconnected.
Sublink	DISCONNECTED indicates that a sublink connection for a particular link name is not established. 0 indicates that the CONTROL sublink is established. 1 to 15 indicates the negotiated sublink number for each application pair.
Link Names	Name used to represent the type of traffic that flows over a particular sublink: • CONTROL indicates the sublink used to transport CLAW packing control messages. • IP indicates the sublink used to send IP datagrams whose TCP checksum is handled by the host. CKSUM indicates the sublink used to send IP datagrams that use the CMCC checksum assist feature.

Related Commands

Command	Description
claw (primary) (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (primary) (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.

show extended channel packing stats

To display Common Link Access for Workstations (CLAW) packing statistics, use the **show extended channel packing stats** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **packing stats** [*path* [*device-address*]]

Syntax Description

slot	Slot number.
port	Port number.
path	(Optional) Hexadecimal value in the range from 0000 to FFFF. This specifies the data path and consists of two digits for the physical connection (either on the host or on the ESCON Director switch): one digit for the control unit address, and one digit for the channel logical address. If not specified, the control unit address and channel logical address default to 0.
device-address	(Optional) Hexadecimal value in the range from 00 to FE. This value is the unit address associated with the control unit number and path as specified in the host input/output configuration program (IOCP) file. For CLAW and offload support, the device address must have an even numbered value.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel packing stats** command:

```
Router# show extended channel 3/0 packing stats

Path: C010 Devs: F2,F3 CLAW Link: 1  Read Blks: 4584       Wrt Blks: 15054
                 Packets               Bytes                 Drops
Linkname       Read      Write      Read     Write       Read      Write   Err C
CONTROL           4          2       128        64          0          0     0 Y
IP                5          5       500       500          0          0     0 Y
CKSUM          4694      93584    187854  53889648          0          0     0 Y
  Total:       4703      93591    188482  53890212          0          0     0

Path: C030 Devs: F6,F7 CLAW Link: N  Read Blks: UNKNOWN    Wrt Blks: UNKNOWN
                 Packets               Bytes                 Drops
Linkname       Read      Write      Read     Write       Read      Write   Err C
CONTROL           0          0         0         0          0          0     0 N
IP                0          0         0         0          0          0     0 N
CKSUM             0          0         0         0          0          0     0 N
  Total:          0          0         0         0          0          0     0
```

Table 45 describes the specified fields shown in the display

Table 45 show extended channel packing stats Field Descriptions

Field	Description
Path	Path from the CLAW, offload, or Cisco Systems Network Architecture (CSNA) configuration.
Devs	Device address for each device. One CLAW connection requires two devices. You need only specify the even numbered address.
CLAW Link	Established CLAW link number used for all CLAW packing messages. A number value indicates that a CONTROL sublink is connected. "N" indicates that a control sublink is disconnected.
Read Blks	Number of CLAW channel blocks read.
Write Blks	Number of CLAW channel blocks written.
Linkname	Name used to represent the type of traffic that flows over a particular sublink. • CONTROL indicates the sublink used to transport CLAW packing control messages. • IP indicates the sublink used to send IP datagrams whose TCP checksum is handled by the host. CKSUM indicates the sublink used to send IP datagrams that use the CMCC checksum assist feature.
Packets Read Write	Total number of packets read and written for each sublink.
Bytes Read Write	Total number of bytes read and written for each sublink.
Drops Read Write	Total number of dropped read and write packets for each sublink.
Err	Number of errors. Each error produces an error message at the router console.
C	Connection state of a sublink. "Y" indicates connected. "N" indicates not connected.
Total	Total for each of the recorded statistics.

Related Commands

Command	Description
claw (primary) (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (primary) (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.

show extended channel statistics

To display statistical information about subchannels on the physical interface of a Cisco Mainframe Channel Connection (CMCC) adapter, use the **show extended channel statistics** command in user EXEC or privileged EXEC mode. This command displays information that is specific to the interface channel devices. The information is generally useful only for diagnostic tasks performed by technical support personnel.

show extended channel *slot*/*port* **statistics** [*path* [*device-address*]] [**connected**]

Syntax Description

slot	Slot number.
port	Port number.
path	(Optional) Hexadecimal value in the range from 0x0000 to 0xFFFF. This value specifies the data path and consists of two digits for the physical connection (either on the host or on the ESCON Director switch): one digit for the control unit address, and one digit for the channel logical address.
device-address	(Optional) Hexadecimal value in the range from 0x00 to 0xFE. This value is the unit address associated with the control unit number and path as specified in the host input/output configuration program (IOCP) file. For Common Link Access for Workstations (CLAW) and offload support, the device address must have an even numbered value.
connected	(Optional) For each backup group, displays information only about the active subchannel or the first subchannel defined in the group if none are active.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.0(3)T	Support was added for the CMPC+ feature.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel statistics** command from a CMCC adapter configured with Common Link Access for Workstations (CLAW), offload, cisco systems network architecture (CSNA), and Cisco Multipath Channel (CMPC):

```
Router# show extended channel 0/1 statistics E010

Path: E010  -- ESTABLISHED
                    Command              Selective      System      Device         CU
Dev    Connects     Retries     Cancels      Reset       Reset       Errors       Busy
 D0        4459        4459           0          0           0            0          0
 D1        4950           0           0          0           0            0          0
```

```
 D2       2529       2526          0          0          0          0          0
 D3       2600          0          0          0          0          0          0
 D9       2211          0          0          0          0          0          0
 DA       4048       2024          0          0          0          0          0
                Blocks               Bytes              Dropped Blk    Memd
Dev-Lnk      Read      Write      Read     Write       Read      Write  wait Con
 D0-00          0          0         0         0          0          0     0   Y
 D0-01       5017          0   1215457         0          0          0     0   Y
Total:       5017          0   1215457         0          0          0     0
 D1-00          0          0         0         0          0          0     0   Y
 D1-01          0       5039         0   1247307          0          0     0   Y
Total:          0       5039         0   1247307          0          0     0
 D2-00          0          0         0         0          0          0     0   Y
 D2-01          0          0         0         0          0          0     0   Y
 D2-02       2671          0    661621         0          0          0     0   Y
Total:       2671          0    661621         0          0          0     0
 D3-00          0          0         0         0          0          0     0   Y
 D3-01          0          0         0         0          0          0     0   Y
 D3-02          0       2680         0    653285          0          0     0   Y
Total:          0       2680         0    653285          0          0     0
 D9-00          0       2214         0    223418          0          0     0   Y
 DA-00       2024          0    124587         0          0          0     0   Y
Path E010
Total:       9712       9933   2001665   2124010          0          0     0
  Last statistics 5 seconds old, next in 5 seconds
```

The following is sample output from the **show extended channel statistics** command from a CMCC adapter configured with CLAW, offload, cisco systems network architecture (CSNA), and CMPC+:

```
Router# show extended channel 0/1 statistics

Path:C020  -- ESTABLISHED
                Command              Selective     System     Device         CU
Dev   Connects    Retries    Cancels      Reset      Reset     Errors       Busy
 30          5          0          0          0          3          0          0
 31          5          0          0          0          3          0          0
 36         27         15          1          0          3          0          0
 37         29          6          1          0          3          0          0

                Blocks               Bytes              Dropped Blk    Memd
Dev-Lnk      Read      Write      Read     Write       Read      Write  wait Con
 30-00          0          0         0         0          0          0     0   N
 31-00          0          0         0         0          0          0     0   N
 36-00         19          6     54236       789          0          0     0   Y
 37-00          9         17       801     63302          0          0     0   Y

Path C020
Total:         28         23     55037     64091          0          0     0

Path:C190  -- ESTABLISHED
                Command              Selective     System     Device         CU
Dev   Connects    Retries    Cancels      Reset      Reset     Errors       Busy
 34         12          0          0          0          5          0          0
 35         12          0          0          0          5          0          0
 36        251        226          6          0          5          0          0
 37        258         14          8          0          5          0          0
 3E         12          0          0          0          5          0          0
 3F         12          0          0          0          5          0          0

                Blocks               Bytes              Dropped Blk    Memd
Dev-Lnk      Read      Write      Read     Write       Read      Write  wait Con
 34-00          0          0         0         0          0          0     0   N
 35-00          0          0         0         0          0          0     0   N
 36-00        236         12   3604441      1578          0          0     0   Y
```

```
 37-00          18         236       1602    4217913           0           0      0   Y
 3E-00           0           0          0          0           0           0      0   N
 3F-00           0           0          0          0           0           0      0   N

Path C190
Total:        254         248    3606043    4219491           0           0      0

Adapter Card
Total:        282         271    3661080    4283582           0           0      0

  Last statistics 8 seconds old, next in 2 seconds
```

Table 46 describes the specified fields shown in the display.

Table 46 show extended channel statistics Field Descriptions

Field	Description
Path	Path from the CLAW, offload, CMPC, CMPC+, or CSNA configuration.
Dev	Address for each device. For CLAW and offload, there are two device addresses. In the configuration statement, you specify only the even numbered address. Both CSNA, CMPC, and CMPC+ have one device.
Connects	Number of times the channel started a channel program on the device.
Command Retries	Number of times the CMCC adapter either had no data to send to the channel (for the read subchannel) or the number of times the CMCC adapter had no buffers to hold data from the channel (for the write subchannel). Every command retry that is resumed results in a connect. A command retry can be ended via a cancel.
Cancels	Host requested any outstanding operation to be terminated. It is a measure of the number of times the host program was started.
Selective Reset	Resets only one device. On the virtual machine (VM), selective reset occurs when a device is attached and a CP Initial Program Load (IPL) command is issued.
System Reset	Number of times the system IPL command was issued. A system reset affects all devices on the given channel. The command is always issued when the ESCON Channel Adapter (ECA) is initialized, and when the channel is taken off line.
Device Errors	Errors detected by the ESCON or parallel interface because of problems on the link. This value should always be 0.
CU Busy	Number of times the adapter returned a control unit busy indication to the host. This indication occurs after a cancel or reset if the host requests an operation before the CMCC adapter has finished processing the cancel or reset.
Dev-Lnk	First number is the device address. The second number is the logical link. Link 0 is always used for CLAW control messages. For IP datagram mode, link 1 is for actual datagram traffic. For offload, link 2 is for application program interface (API) traffic. For CSNA, CMPC, and CMPC+, the Dev-Lnk is not relevant.
Blocks Read/Write	Count of channel blocks that are read and written from the mainframe.
Bytes Read/Write	Sum of the bytes in the blocks.

Table 46 show extended channel statistics Field Descriptions (continued)

Field	Description
Dropped Blk Read/Write	If the Route Processor sends data to the CMCC adapter faster than it can send it to the channel, then the block is dropped. High values mean the host is not running fast enough. A write drop occurs if the CMCC adapter fails to get a router processor buffer *x* times for a given block. See the Memd wait counter.
Memd wait	Number of times the CMCC adapter could not obtain a buffer.
Con	For link 0, a connection of Y means the system validation is complete. For all other links, Con means the connection request sequence is completed. For CSNA devices, a value of Y is displayed when the CSNA device status is complete. For all other states, the Con shows a value of N. **Note** If you halt the host or terminate virtual telecommunications access method (VTAM) using the Z NET, CANCEL command, VTAM does not halt the subchannels, and CON shows a value of Y until the subchannels time out (approximately 180 seconds).

The following is sample output from the CSNA path, using the **show extended channel statistics** command:

```
Router# show extended channel 0/1 statistics E200

Path: E200  -- ESTABLISHED
                  Command              Selective     System     Device         CU
Dev   Connects    Retries    Cancels      Reset      Reset     Errors       Busy
 D0     217440     108293          1          0          0          0          0
 D1      59530      19800          1          0          0          0          0
 D2       1065        252          2          0          0          0          0
 D3       1329         16          2          0          0          0          0
 D4       1066        251          2          0          0          0          0
 D5        887         29          2          0          0          0          0
 DA       1073         17          2          0          0          0        373
 DB        410        174          2          0          0          0          0
 DC       1154         14          2          0          0          0        459
 DD        254         17          2          0          0          0          0
                Blocks              Bytes             Dropped Blk    Memd
Dev-Lnk      Read      Write       Read      Write       Read      Write  wait Con
 D0-00     109096     109095 237799616     880468          0          0     0   Y
 D1-00      19877      19875    160688 237876362          0          0     0   Y
 D2-00          9      12842       801  52554701          0          0     0   Y
 D3-00       1315          8  30378114      1052          0          0     0   Y
 D4-00          9      12842       801  52554701          0          0     0   Y
 D5-00        860          8  17003956      1052          0          0     0   Y
 DA-00        687          8  14617852      1052          0          0     0   Y
 DB-00          9       3578       801  14613989          0          0     0   Y
 DC-00        682          8  14513604      1052          0          0     0   Y
 DD-00          9       3594       801  14679517          0          0     0   Y
Path E200
Total:     132553     161858 314477034 373163946          0          0     0
  Last statistics 3 seconds old, next in 7 seconds
```

Related Commands

Command	Description
claw (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.
csna	Configures Systems Network Architecture (SNA) support on a CMCC physical channel interface and specifies the path and device/subchannel on a physical channel of the router to communicate with an attached mainframe.
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.

show extended channel subchannel

To display information about the Cisco Mainframe Channel Connection (CMCC) adapter physical interfaces, use the **show extended channel subchannel** command in user EXEC or privileged EXEC mode. This command displays information that is specific to the interface channel connection. The information displayed is generally useful only for diagnostic tasks performed by technical support personnel.

show extended channel *slot*/*port* **subchannel** [**connected**]

Syntax Description

slot	Slot number.
port	Port number.
connected	(Optional) For each backup group, displays information about the active subchannel or the first subchannel defined in the group if none are active.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.0(3)T	Support was added for the CMPC+ feature.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel subchannel connected** command used on a CMCC adapter configured for Common Link Access for Workstations (CLAW), offload, and cisco systems network architecture (CSNA):

```
Router# show extended channel 1/0 subchannel

Channel1/0:state up
  Flags:VALID ESCON LOADED ENABLED SIGNAL
  Link:E9, Buffers 0, CRC errors 1, Load count 1
  Link Incident Reports
    implicit 0, bit-error 0, link failed 1,
    NOS 0, sequence timeout 0, invalid sequence 0
  Neighbor Node - VALID
    Class:Switch          Type Number :009032        Tag:E9
    Model:002             Manufacturer:IBM
    Plant:02              Sequence    :000000010685
  Local Node - VALID
    Class:CTCA-standalone Type Number :C7200         Tag:10
    Model:6               Manufacturer:CSC
    Plant:A               Sequence    :8083599
                                                                 Last
   Mode    Path Device                                           Sense
```

```
CLAW    E020 90 172.18.55.12  CISCOMVS TRAILMIX TCPIP  TCPIP    0000  Flags:RESET_EVENT
CLAW    E020 91 172.18.55.12  CISCOMVS TRAILMIX TCPIP  TCPIP    0000  Flags:RESET_EVENT
CSNA    E020 94 maxpiu 20470 time-delay  10 length-delay 20470  0000  Flags:RESET_EVENT
OFFLOAD E140 90 172.18.55.11  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  TCPIP  API   Flags:CMD_RETRY
OFFLOAD E140 91 172.18.55.11  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  TCPIP  API   Flags:CMD_RETRY
CLAW    E150 90 172.18.55.13  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
CLAW    E150 91 172.18.55.13  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
CLAW    E150 96 172.18.55.22  CISCOMVS TRAILMIX TCPIP  TCPIP    0080
CLAW    E150 97 172.18.55.22  CISCOMVS TRAILMIX TCPIP  TCPIP    0080
CLAW    E160 90 172.18.55.14  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
CLAW    E160 91 172.18.55.14  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
CLAW    E170 90 172.18.55.15  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
CLAW    E170 91 172.18.55.15  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
CLAW    E180 90 172.18.55.20  VMV2R3   TRAILMIX TCPIP  TCPIP    0000  Flags:CMD_RETRY
CLAW    E180 91 172.18.55.20  VMV2R3   TRAILMIX TCPIP  TCPIP    0000  Flags:CMD_RETRY
CLAW    E180 92 172.18.55.21  TSOMAIN  TRAILMIX TCPIP  TCPIP    0000  Flags:CMD_RETRY
CLAW    E180 93 172.18.55.21  TSOMAIN  TRAILMIX TCPIP  TCPIP    0000  Flags:CMD_RETRY
CLAW    E190 90 172.18.55.17  CISCOMVS TRAILMIX TCPIP  TCPIP    0000  Flags:RESET_EVENT
CLAW    E190 91 172.18.55.17  CISCOMVS TRAILMIX TCPIP  TCPIP    0000  Flags:RESET_EVENT
CLAW    E1E0 90 172.18.55.18  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
CLAW    E1E0 91 172.18.55.18  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
CLAW    E1F0 90 172.18.55.19  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
CLAW    E1F0 91 172.18.55.19  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY

Last statistics 6 seconds old, next in 4 seconds
```

Table 47 describes the specified fields shown in the display.

Table 47 show extended channel subchannel Field Descriptions

Field	Description
Channel1/0: state	State can be up, down, or administratively down.
Flags	• GO-OFF—CMCC adapter is trying to shut down the channel interface. This state should not persist for more than a few seconds. This flag is not applicable to the virtual channel interface. • INVALID—All displays for virtual channel interfaces should contain this flag. On physical channel interfaces, it indicates a problem with the CMCC adapter microcode. • LOADED—Channel firmware for the physical channel interface is loaded. The channel firmware is loaded only if the interface configuration contains at least one device configuration statement and is not shut down. This flag matches the state of the “loaded” LED. This flag is not applicable to the virtual channel interface. • LOVE—Note indicating an interface state change (up-down or down-up) is pending on this interface. This state should not persist for more than a few seconds. • OFFLINE—For an ESCON channel interface, this flag indicates that no mainframe has established an ESCON logical path corresponding to the paths specified in any device configuration statement (claw, offload, csna, or cmpc). For a parallel channel interface, this flag indicates that the x'0100' path is not defined in any device configuration statement or SIGNAL is not present.

Table 47 show extended channel subchannel Field Descriptions (continued)

Field	Description
Flags (continued)	• ONLINE—For an ESCON channel interface, this flag indicates that at least one mainframe has established an ESCON logical path corresponding to the paths specified in one of the device configuration statements (CLAW, offload, CSNA, CMPC, or CMPC+). For a parallel channel interface, this flag indicates that the x'0100' path is defined in at least one device configuration statement and SIGNAL is present. • RQC_PEND—CMCC adapter is attempting to send status to the channel on this interface. This state should not persist for more than a few seconds. This flag is not applicable to the virtual channel interface. • RESET_EVENT—Indicates that a reset event has been received. • SIGNAL—For an ESCON channel interface, this flag indicates that light is detected. For a parallel channel interface, this flag indicates that the "operational out" signal is detected. This flag matches the state of the "signal" LED. It will be set only if the LOADED flag is also set. This flag is not applicable to the virtual channel interface. • STAT_PEND—CMCC adapter has status to present for this device. The indication is cleared when the mainframe accepts the status.
Flags (continued)	• SUSPEND—Indicates that the CMCC device task has decided to suspend data transfer for a particular device. • VALID—A physical interface is installed. All displays for physical channel interfaces should contain this. This flag matches the state of the "present" LED.
Link: xx	Director port number to which the physical channel is connected. If the physical channel is directly connected, then this value is host dependent.
Buffers	Number of times the CMCC adapter has dropped a packet bound for the Route Processor because no packet switching buffer was available on the Route Processor.
CRC errors	Number of cyclic redundancy check (CRC) errors detected on the channel for ESCON. Number of parity errors detected on the channel for parallel.
Load count	For a CMCC physical channel interface, the number of times the channel adapter microcode has been loaded.

Table 47 show extended channel subchannel Field Descriptions (continued)

Field	Description
Link Incident Reports	Link incidents are errors on an ESCON channel. These errors are reported to the host operating system and are recorded here for additional information. • Implicit incidents—Recoverable error occurred in the ESCON Channel Adapter (ECA). • Bit errors—Bit error rate threshold was reached. The bit error rate threshold is 15 error bursts within 5 minutes. An error burst is defined as a time period of 1.5 +/– 0.5 seconds during which one or more code violations occurred. A code violation error is caused by an incorrect sequence of 10 bit characters. • Link failed—Loss of synchronization or light has occurred. • NOS—Channel or switch sent the Not Operational Sequence. • Sequence timeout—Connection recovery timeout has occurred or the router is waiting for the appropriate response while in the send offline sequence (OLS) state. • Invalid Sequence—Unconditional disconnect (UD) or unconditional disconnect response (UDR) is recognized in the wait for offline sequence state.
Neighbor node	Describes the channel or switch. Valid values are: • VALID—Information has been exchanged between the router and channel or switch. • Class—Switch or channel depending on whether the connection is a switched point-to-point connection or a point-to-point connection. • Type number—Model of switch or processor. • TAG—Physical location of the connector. • Model—A further classification of type. • Manufacturer—Identifies who made switch or processor. • Plant and sequence—Manufacturer-specific information to uniquely define this one device.

Related Commands

Command	Description
claw (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.

Command	Description
csna	Configures Systems Network Architecture (SNA) support on a CMCC physical channel interface and specifies the path and device/subchannel on a physical channel of the router to communicate with an attached mainframe.
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.

show extended channel tcp-connections

To display information about the TCP sockets on a channel interface, use the **show extended channel tcp-connections** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tcp-connections** [*loc-ip-addr* [*loc-port* [*rem-ip-addr* [*rem-port*]]]] [**detail** | **summary**]

Syntax Description

slot	Slot number.
port	Port number.
tcp-connections	Specifies TCP connections display.
loc-ip-addr	(Optional) Local IP address. IP address of the local connection endpoint. Restricts the output to those connections with a matching local IP address.
loc-port	(Optional) Local TCP port. This is the TCP port of the local connection endpoint. Restricts the output to those connections with a matching local TCP port. An asterisk (*) is a wildcard that matches every port.
rem-ip-addr	(Optional) Remote IP address. IP address of the remote connection endpoint. Restricts the output to those connections with a matching remote IP address.
rem-port	(Optional) Remote TCP port. TCP port of the remote connection endpoint. Restricts the output to those connections with a matching remote TCP port.
detail	(Optional) Prints detailed information about every matching connection.
summary	(Optional) This is the default. Prints a summary of all matching connections.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	The stack address field was added to the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tcp-connections** command is valid on both physical and virtual channel interfaces. If no IP addresses or TCP ports are specified, all TCP connections are displayed in a summary for the specified interface.

The command displays detailed information about a large number of sessions that can take a long time. Consider restricting the output by IP address and TCP port to connections of interest.

Examples

The following is sample output from the **show extended channel tcp-connections detail** command:

```
Router# show extended channel 0/1 tcp-connections detail

Local IP Addr    Port  Remote IP Addr  Port   State        In Bytes   Out Bytes
10.11.198.2      21    0.0.0.0         0      listen             0           0
10.11.198.2      21    172.18.48.194   38668  establish         62         298
10.11.198.2      23    0.0.0.0         0      listen             0           0
10.11.198.2      23    172.18.48.194   38666  establish        124       11966
10.11.198.2      1025  0.0.0.0         0      listen             0           0
10.11.198.2      1025  172.18.48.194   38705  closeWait         24           1
10.11.198.3      7     0.0.0.0         0      listen             0           0
10.11.198.3      9     0.0.0.0         0      listen             0           0
10.11.198.3      19    0.0.0.0         0      listen             0           0
10.11.198.3      21    0.0.0.0         0      listen             0           0
10.11.198.3      23    0.0.0.0         0      listen             0           0
10.11.198.3      23    172.18.48.194   38667  establish         85         446
```

The following is sample output from the **show extended channel tcp-connections** command when you specify the **detail** keyword for an offload device at real IP address 10.10.21.3 with an alias address of 10.2.33.88:

```
Router# show extended channel 3/1 tcp-connections 10.10.21.3 detail

Stack Address 10.10.21.3:
Local IP Addr    Port  Remote IP Addr  Port   State        In Bytes   Out Bytes Addr
0.0.0.0          23    0.0.0.0         0      listen             0           0
10.2.33.88       23    10.70.5.140     61954  establish         59         105
```

Table 48 describes the specified fields shown in the display.

Table 48 show extended channel tcp-connections Field Descriptions

Field	Description
Stack Address	Real IP address of the TCP/IP stack or offload device.
Local IP Addr	Local IP address on the connection.
State	The state of this TCP connection. The only value that may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a “badValue” response if a management station attempts to set this object to any other value. If a management station sets this object to the value deleteTCB(12), then this has the effect of deleting the Transmission Control Block (TCB) (as defined in RFC 793) of the corresponding connection on the managed node, resulting in immediate termination of the connection. As an implementation-specific option, a reset (RST) segment may be sent from the managed node to the other TCP endpoint. (Note, however, that RST segments are not sent reliably.)

Table 48 show extended channel tcp-connections Field Descriptions (continued)

Field	Description
In Bytes	Number of bytes sent for this TCP connection. **Note** To support Simple Network Management Protocol (SNMP) Version 1 Managers, this variable is supplied as a 32-bit value that can wrap frequently.
Out Bytes	Number of bytes received for this TCP connection. **Note** To support SNMP Version 1 Managers, this variable is supplied as a 32-bit value that can wrap frequently.

The following is sample output from the **show extended channel tcp-connections summary** command:

```
Router# show extended channel 0/1 tcp-connections summary

TCP Connections=12  Input Bytes=      294  Output Bytes=    13049
```

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
pu (TN3270)	Creates a physical unit (PU) entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.
show extended channel tcp-stack	Displays information about the TCP stack running on CMCC adapter interfaces.

show extended channel tcp-stack

To display information about the TCP stack running on Cisco Mainframe Channel Connection (CMCC) adapter interfaces, use the **show extended channel tcp-stack** command in user EXEC or privileged EXEC mode.

show extended channel *slot/port* **tcp-stack** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
tcp-stack	Specifies **tcp stack** display.
ip-address	(Optional) IP address specified by the **offload** interface configuration command or the **tn327-server pu** command.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	The Alias addresses field was added to the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tcp-stack** command is valid on both physical and virtual channel interfaces. If no *ip-address* argument is specified, then information is displayed for all IP addresses configured on the specified interface.

Examples

The following is sample output from the **show extended channel tcp-stack** command:

```
Router# show extended channel 0/1 tcp-stack

TCP Statistics for IP Address 10.11.198.2
  RtoAlgorithm: vanj         RtoMin      : 1000         RtoMax      : 64000
  MaxConn     : -1           ActiveOpens : 1            PassiveOpens: 17
  AttemptFails: 0            EstabResets : 0            CurrEstab   : 5
  InSegs      : 181          OutSegs     : 147          RetransSegs : 0
  InErrs      : 0            OutRsts     : 0
TCP Statistics for IP Address 10.11.198.3
  RtoAlgorithm: vanj         RtoMin      : 1000         RtoMax      : 64000
  MaxConn     : -1           ActiveOpens : 0            PassiveOpens: 1
  AttemptFails: 0            EstabResets : 0            CurrEstab   : 6
  InSegs      : 25           OutSegs     : 23           RetransSegs : 0
  InErrs      : 0            OutRsts     : 0
```

The following is sample output from the **show extended channel tcp-stack** command when you specify the real IP address for an offload device at 10.10.21.3:

```
Router# show extended channel 3/1 tcp-stack 10.10.21.3

TCP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  RtoAlgorithm: vanj         RtoMin      : 1000         RtoMax      : 64000
  MaxConn     : -1           ActiveOpens : 0            PassiveOpens: 1
  AttemptFails: 0            EstabResets : 0            CurrEstab   : 2
  InSegs      : 16           OutSegs     : 7            RetransSegs : 0
  InErrs      : 0            OutRsts     : 0
```

The following is sample output from the **show extended channel tcp-stack** command when you specify the alias IP address for an offload device at 10.2.33.88:

```
Router# show extended channel 3/1 tcp-stack 10.2.33.88

TCP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  RtoAlgorithm: vanj         RtoMin      : 1000         RtoMax      : 64000
  MaxConn     : -1           ActiveOpens : 0            PassiveOpens: 1
  AttemptFails: 0            EstabResets : 0            CurrEstab   : 2
  InSegs      : 16           OutSegs     : 7            RetransSegs : 0
  InErrs      : 0            OutRsts     : 0
```

Table 49 describes the specified fields shown in the display.

Table 49 show extended channel tcp-stack Field Descriptions

Field	Description
Alias addresses	Virtual IP addresses assigned to the real IP address of an offload device.
RtoAlgorithm	The algorithm used to determine the timeout value used for resending unacknowledged octets.
RtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
RtoMax	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
MaxConn	The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value –1.
ActiveOpens	Number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
PassiveOpens	Number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

Table 49 show extended channel tcp-stack Field Descriptions (continued)

Field	Description
AttemptFails	Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
EstabResets	Number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
CurrEstab	Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
InSegs	Total number of segments received, including those received in error. This count includes segments received on established connections.
OutSegs	Total number of segments sent, including those on current connections but excluding those containing only re-sent octets.
RetransSegs	Total number of segments re-sent—that is, the number of TCP segments sent containing one or more previously sent octets.
InErrs	Total number of segments received in error (for example, bad TCP checksums).
OutRsts	Number of TCP segments sent containing the reset (RST) flag.

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
pu (TN3270)	Creates a physical unit (PU) entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.
show extended channel tcp-connections	Displays information about the TCP sockets on a channel interface.

show extended channel tg

To display configuration, operational information, and statistics information for Cisco Multipath Channel (CMPC) or CMPC+ transmission groups configured on the specified Cisco Mainframe Channel Connection (CMCC) adapter's virtual interface, use the **show extended channel tg** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tg** [**oper** | **stats**] [**detailed**] [*tg-name*]

Syntax Description

slot	Slot number.
port	Port number.
oper	(Optional) Operational parameters for the CMPC or CMPC+ Transmission Group (TG) values.
stats	(Optional) Statistical values for the CMPC or CMPC+ TG.
detailed	(Optional) Additional information about the CMPC or CMPC+ TG.
tg-name	(Optional) Name of the TG.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.0(3)T	Support was added for the CMPC+ feature.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tg** command is valid only on the virtual channel interface. If the *tg-name* argument is not specified, information about all TGs configured on the specified interface is displayed.

If neither the **oper** or **stats** keyword is specified, operational values are displayed.

Examples

The following is sample output from the **show extended channel tg oper** command for a CMPC TG:

```
Router# show extended channel 3/2 tg oper detailed MVS2-TG1

CMPC-TG: MVS2-TG1 Status: ACTIVE
   Adapter:token    1  RMAC:4000.4040.1996         LSAP:04         RSAP:04
   TGN    :21          Local CP: NETA.MVS2         Remote CP: NETA.CALEB
   MaxIn  :4105        MaxOut  :4105
   HPR    :NO          HPR LSAP:04                 HPR RSAP :00
   RIF    :0830.1FF1.0041.00A0
Connection LLC2 Information:
   t1-time   = 1000  tpf-time  = 1000  trej-time = 3200  tbusy-tim = 9600
```

```
idle-time =60000  local-win =    7  recv-wind =    7  N2         =    8
N1-Send   = 1033  N1-Rcv    = 1033  ack-delay =  100  ack-max    =    3
Nw        =    0  Ww        =    7
Last Ww Cause = other
Connection Time: 00:00:00 UTC Jan 1 1970
Last modified: 00:00:00 UTC Jan 1 1970
```

Table 50 describes the specified fields shown in the display.

Table 50 show extended channel tg oper Field Descriptions

Field	Description
Status	Connection status of the CMPC TG. Valid values are: • Shutdown—CMCC virtual interface is shut down. In this state, all nonconfigurable values will not be displayed and the Logical Link Control (LLC) connection operational values displayed when the **detailed** keyword is specified also are not displayed. • Inactive—CMPC TG is reset ready to activate. • LocatingRemoteLinkStation—Exploring network for configured CMPC TG peer. • RemoteLinkStationLocated—CMPC TG network peer found. Waiting for connection negotiation to start. • XID3Negotiation—exchange identification (XID) negotiation in progress. • PendingActive—Connect station pending. • ACTIVE—CMPC TG connection active.
Adapter	Identifies the CMCC adapter's internal MAC adapter configured for this CMPC TG. The MAC address configured for this adapter is the local MAC address for the CMPC or CMPC+ TG LLC connection.
RMAC	Remote MAC address configured for the CMPC TG LLC connection.
LSAP	Local service access point (SAP) configured for the CMPC TG LLC connection.
RSAP	Remote SAP configured for the CMPC TG LLC connection.
TGN	TG number for this CMPC TG LLC connection. This value is extracted from the XID3 negotiation exchange.
Local CP	Control point name for virtual telecommunications access method (VTAM). The name is extracted from XID3s received from virtual telecommunications access method (VTAM).
Remote CP	Control point name for the remote node connected by this CMPC TG. The name is extracted from XID3 received from the remote node.
MaxIn	Maximum path information unit (PIU) the remote node is allowed to send to VTAM. The value is the max PIU field in the XID3s received from VTAM.
MaxOut	Maximum PIU VTAM is allowed to send to the remote node. The value is the lowest of the max PIU field in the XID3 received from the remote node, the LF (length field) size in the RIF, and the CMCC virtual interface MTU size.
HPR	Valid values are YES and NO. If HPR is active on this CMPC TG, then the value will display YES.
HPR LSAP	Local SAP value used for HPR traffic. This value will be the same as the configured local service access point (SAP) value.

Table 50 show extended channel tg oper Field Descriptions (continued)

Field	Description
HPR RSAP	Remote SAP value used for HPR traffic. This value is extracted from the XID3s during the connection negotiation between VTAM and the remote node.
RIF	Routing information field. If the CMPC TG LLC connection is established using source-route bridging, then the RIF used for the connection is displayed here.

The following is sample output on a Cisco 7500 router from the **show extended channel tg stats** command for a CMPC TG:

```
Router# show extended channel 3/2 tg stats detailed MVS2-TG1

CMPC-TG:MVS2ISR1
  IFramesIn   :51             IFramesOut  :41
  IBytesIn    :4378           IBytesOut   :51803
  UIFramesIn  :0              UIFramesOut :0
  UIBytesIn   :0              UIBytesOut  :0
  TESTRspsIn  :1              TESTCmdsOut :1
  XIDCmdsIn   :3              XIDCmdsOut  :3
  XIDRspsIn   :0              XIDRspsOut  :0
  ConnectReqs :2              ConnectInds :0
  ConnectRsps :2              ConnectCnfms:0
  DISCReqs    :1              DISCInds    :0
  SweepReqsIn :0              SweepReqsOut:0
  SweepRspsIn :0              SweepRspsOut:0
  Wraps       :0
  LastSeqNoIn :9              LastSeqNoOut:7
  LastSeqNoFailureCause     : None
TimeSinceLastSeqNoFailure : never
  LLC2 Connection Statistics:
 LAN Token  0 Adapter   1 4000.cdcd.cdcd
   Local SAP=04 Remote MAC=4000.4040.1996 Remote SAP=04
     LocalBusies    =          0  RemoteBusies   =          0
     IFramesIn      =         51  IFramesOut     =         41
     IOctetsIn      =       4378  IOctetsOut     =      51803
     SFramesIn      =          0  SFramesOut     =          0
     REJsIn         =          0  REJsOut        =          0
     RetransmitsOut =          0  WwCountChanges =          0
```

Table 51 describes the specified fields shown in the display.

Table 51 show extended channel tg stats Field Descriptions

Field	Description
IFramesIn	Number of connection-oriented PIUs received by this CMPC TG from the remote network node.
IFramesOut	Number of connection-oriented PIUs sent by this CMPC TG to the remote network node.
IBytesIn	Number of bytes for connection-oriented PIUs received by this CMPC TG from the remote network node.
IBytesOut	Number of bytes for connection-oriented PIUs sent by this CMPC TG to the remote network node.
UIFramesIn	Number of connectionless PIUs (HPR frames) received by this CMPC TG from the remote network node.

Table 51 show extended channel tg stats Field Descriptions (continued)

Field	Description
UIFramesOut	Number of connectionless PIUs (HPR frames) sent by this CMPC TG to the remote network node.
UIBytesIn	Number of bytes for connectionless PIUs received by this CMPC TG from the remote network node.
UIBytesOut	Number of bytes for connectionless PIUs sent by this CMPC TG to the remote network node.
TESTRspsIn	Number of TEST responses received for this CMPC TG.
TESTCmdsOut	Number of TEST commands sent by this CMPC TG to the configured remote MAC address.
XIDCmdsIn	Number of XID commands received for this CMPC TG.
XIDCmdsOut	Number of XID commands sent by this CMPC TG.
XIDRspsIn	Number of XID responses received for this CMPC TG.
XIDRspsOut	Number of XID responses sent by this CMPC TG.
ConnectReqs	Number of connect requests received from the host by this CMPC TG.
ConnectInds	Number of connect indications sent to the host by this CMPC TG.
ConnectRsps	Number of connect responses received from the host by this CMPC TG.
ConnectCnfms	Number of connect confirms sent to the host by this CMPC TG.
DISCReqs	Number of disconnect requests received from the host by this CMPC TG.
DISCInds	Number of disconnect indications sent to the host by this CMPC TG.
SweepReqsIn	Number of CMPC sweep requests received from VTAM on this CMPC TG.
SweepReqsOut	Number of CMPC sweep requests sent to VTAM on the CMPC TG.
SweepRspsIn	Number of CMPC responses received from VTAM on this CMPC TG.
SweepRspsOut	Number of CMPC responses sent to VTAM on this CMPC TG.
Wraps	The number of times the sequence numbers wrapped for this CMPC TG.
LastSeqNoIn	The sequence number on the last CMPC data block sent to the host from this CMPC TG.
LastSeqNoOut	The sequence number on the last CMPC data block received from the host for this CMPC TG.

Table 51 show extended channel tg stats Field Descriptions (continued)

Field	Description
LastSeqNoFailureCause	The cause of the last sequence number failure for this CMPC TG. Valid values are as follows: • None—No sequence number failures have occurred on this CMPC TG since it was configured or the interface was last "no shut." • Block—The sequence number failure occurred on an Multi-Path Channel plus (MPC) data block received from the host for this CMPC TG. • Sweep—The sequence number failure occurred on a sweep command received from the host for this CMPC TG.
TimeSinceLastSeqNoFailure	Time since the last CMPC sequence number failure for this CMPC TG. If there have been no failures, "never" is displayed.

The following is sample output on a Cisco 7500 router from the **show extended channel tg stats** command for a CMPC TG when the interface is shut down:

```
Router# show extended channel 3/2 tg stats detailed MVS2-TG1

CIP LLC-TG:MVS2ISR1 -Statistics Not Available
```

The following is sample output from the **show extended channel tg** command for a CMPC+ TG:

```
CMPC-TG:MPCPTG2   Status:Active
  Local IP address:10.44.4.1                    Remote IP Address :10.44.4.2

  Connection Info: Type=TCP/IP
  Local VC Token  :0500109002                    Local Conn. Token :0500109003
  Remote VC Token :0500201002                    Remote Conn. Token:0500201002
  VC Status       :Active                        Connection Status :Active

CMPC-TG:MPCPTG3   Status:Active
  Local IP address:172.18.3.1                    Remote IP Address :172.18.3.2

  MPC+ Connection Info: Type=HSAS IP
  Local VC Token  :0500109002                    Local Conn. Token :0500109003
  Remote VC Token :0500201002                    Remote Conn. Token:0500201002
  VC Status       :Active                        Connection Status :PendingActive
```

Table 52 describes the specified fields shown in the display.

Table 52 show extended channel tg Field Descriptions

Field	Description
Status	Connection status of the CMPC+ TG. Valid values are: • Shutdown—CMCC virtual interface is shut down. In this state, all nonconfigurable values will not be displayed and the connection operational values displayed when the **detailed** keyword is specified also are not displayed. • Ready—CMCC virtual interface is operational. • Unknown—Unknown status. • Inactive—CMPC+ TG is reset ready to activate. • Active—CMPC+ TG connection active.
Local IP Address	IP address of the CMCC interface for this TG. This address matches the router's IP address configured on the corresponding TG statement.
Remote IP Address	IP address of the host for this TG. This address matches the host IP address configured on the corresponding TG statement.
Type	Valid IP connection types are: • TCP/IP—Indicates that the connection is via the TCP/IP stack. • HSAS IP—Indicates that the connection is via the High Speed Access Services (HSAS) stack.
Local VC Token	CMCC adapter's token for the virtual circuit.
Remote VC Token	Host's token for the virtual circuit.
VC Status	Valid states for the virtual circuit are: • Reset—Awaiting a connection request from the host or CMCC adapter. • Active—Virtual circuit active indication was received from the host and the CMCC adapter sent a virtual circuit active indication to the host. The virtual circuit is now ready to send and receive connection requests.
Local Conn Token	CMCC adapter's token for the Multi-Path Channel plus (MPC+) connection.
Remote Conn Token	Host's token for the MPC+ connection.
Connection Status	The valid states for a connection are: • Reset—Awaiting a connection request from the host or CMCC adapter. • ConnectionRequestSent—CMCC adapter sent a Connection Request to the host and is waiting a Connection Confirm from the host. • PendingActive—CMCC adapter is waiting for the host to enable traffic flow on the connection. • Active—Connection is active and both the CMCC adapter and the host have enabled traffic flow on the connection. At this point, the CMCC adapter has added a static route on the router for the host's IP address. Verify with the **show ip route static** command.

The following sample shows output on a CMCC adapter from the **show extended channel tg stats** command for a CMPC+ TG:

```
Router# show extended channel 3/2 tg stats MVS2-TG1

CMPC-TG:MPCPTG2
  PacketsIn     :       81361   PacketsOut     :       71369
  BytesIn       :  3874888438   BytesOut       :   377499994
  ConnNr        :           0   ConnNs         :           0
  SweepReqsIn   :           0   SweepReqsOut   :           0
  SweepRspsIn   :           0   SweepRspsOut   :           0
  Wraps         :           0
  LastSeqNoIn   :    56047093   LastSeqNoOut   :     6751136
  LastSeqNoFailureCause     : None
  TimeSinceLastSeqNoFailure : never
CMPC-TG:MPCPTG3
  PacketsIn     :       44361   PacketsOut     :       63369
  BytesIn       :  6834888438   ByteOuts       :   954539994
  ConnNr        :           0   ConnNs         :           0
  SweepReqsIn   :           0   SweepReqsOut   :           0
  SweepRspsIn   :           0   SweepRspsOut   :           0
  Wraps         :           0
  LastSeqNoIn   :     6274700   LastSeqNoOut   :     1829808
  LastSeqNoFailureCause     : None
  TimeSinceLastSeqNoFailure : never
```

Table 53 describes the specified fields shown in the display.

Table 53 show extended channel tg stats Field Descriptions

Field	Description
PacketsIn	Number of packets sent to the host on this TG.
PacketsOut	Number of packets sent by the host on this TG.
BytesIn	Total byte count for all packets sent to the host on this TG.
BytesOut	Total byte count for all packets sent by the host on this TG.
ConnNr	Sequence number of the last MPC+ frame on this connection from the host. Because IP traffic is all connectionless, the value is always 0.
ConnNs	Sequence number of the last MPC+ frame on this connection sent to the host. Because IP traffic is always connectionless, the value is always 0.
SweepsReqsIn	Number of CMPC+ sweep requests received from the host on this CMPC+ TG.
SweepsReqsOut	Number of CMPC+ sweep requests sent to the host on the CMPC+ TG.
SweepsRspsIn	Number of CMPC+ sweep responses received from the host on the CMPC+ TG.
SweepsRspsOut	Number of CMPC+ responses sent to the host on this CMPC+ TG.
Wraps	Number of times the CMPC+ sequence number for this TG has wrapped on the write subchannel.
LastSeqNoIn	Last block sequence number sent on the read subchannel.
LastSeqNoOut	Last block sequence number received on the write subchannel.

Table 53 show extended channel tg stats Field Descriptions (continued)

Field	Description
Last SeqNoFailureCause	Valid values are: • None—No sequence number failures detected since the program started. • Block—Sequence number received in a data block on the write subchannel was not the expected sequence number. • Sweep—Sequence number received in a sweep message on the write subchannel was not the expected sequence number.
TimeSinceLastSeqNoFailure	Number of seconds since the last sequence number failure.

Related Commands

Command	Description
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.
tg (CMPC)	Defines LLC connection parameters for the CMPC transmission group.
tg (CMPC+)	Defines IP connection parameters for the CMPC+ transmission group.
show extended channel cmgr	Displays information about the MPC+ transmission group connection manager.

show extended channel tn3270-server

To display current server configuration parameters and the status of the physical unit (PU)s defined for the TN3270 server, use the **show extended channel tn3270-server** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tn3270-server**

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
port	Port value for a TN3270 server will always be 2.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The following fields were added to the output display: • lu-termination • lu-deletion
12.2	The Named value was added for the lu-deletion field in the output display.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel tn3270-server** command:

```
Router# show extended channel 3/2 tn3270-server

<current stats> < connection stats >  <response time(ms)>
server-ip:tcp        lu in-use   connect disconn fail   host     tcp
172.28.1.106:23     510     1       12       11     0     54     40
172.28.1.107:23     511     0        0        0     0      0      0
172.28.1.108:23     255     0        0        0     0      0      0
total              1276     1
configured max_lu 20000  unbind-action disconnect
idle-time 0  keepalive 1800 (send nop)
tcp-port 23  generic-pool permit no timing-mark
lu-termination unbind lu-deletion never
dlur MPX.GOANCP                              status SHUT
dlus MPX.NGMVMPC
name(index)    ip:tcp              xid   state     link   destination   r-lsap
```

```
EXT2(1)       172.28.1.106:23     05D18092 ACTIVE    tok 0  4000.7470.00e7 08 04
PUS10(2)      172.28.1.107:23     05D19010 ACTIVE    tok 0  4000.7470.00e7 08 2C
PUS11(3)      172.28.1.107:23     05D19011 ACTIVE    tok 0  4000.7470.00e7 08 28
PUS12(4)      172.28.1.108:23     05D19012 ACTIVE    tok 0  4000.7470.00e7 08 24
PUS9(5)       172.28.1.109:23     05D18509 SHUT      tok 0  4001.3745.1088 04 40
SDTF(7)       172.28.1.107:23     12345678 ACTIVE    tok 0  0800.5a4b.1cbc 04 08
TEST(8)       172.28.1.106:23     05D18091 ACTIVE    tok 0  4000.7470.00e7 08 30
INT1(6)       172.28.1.106:23     05D18091 SHUT      dlur
```

Table 54 describes the significant fields in the display. Those fields not described correspond to configured values.

Table 54 show extended channel tn3270-server Field Descriptions

Field	Description
server	IP address and TCP port number, listen point, configured on one or more PUs.
lu	Total number of logical unit (LU)s available for this listen point.
in-use	Number of LUs in use.
connect	Total number of connections since the TN3270 feature was started.
disconn	Total number of disconnects since the TN3270 feature was started.
fail	Total number of failed connections since the TN3270 feature was started.
response time, host	The average response time from the host across all sessions through this server IP address. This is measured from sending Carrier Detect (CD) to the host to receiving the reply.
response time, tcp	Average response time from the clients on this server IP address. This is measured only when TIMING MARKs are sent. If **no timing-mark** is configured, they are sent only on special occasions, such as Bind.
idle-time *number*	Configured idle-time for this physical unit (PU).
keepalive	Configured keepalive time for this PU. *action* is one of the following: • **send nop**—The Telnet command for no operation is sent to the TN3270 client to verify the physical connection. • **send timing mark** *number*—Number of seconds within which the TN3270 server expects a response to the DO TIMING-MARK from the TN3270 client.
unbind-action	Configured unbind action for LUs on this PU.
tcp-port	Configured TCP port number.
generic-pool	Configured generic pool for LUs on this PU.

Table 54 show extended channel tn3270-server Field Descriptions (continued)

Field	Description
lu-termination	Displays the value configured for the **lu termination** siftdown command for the PUs supported by the TN3270 server. The **lu termination** command specifies whether a TERMSELF or UNBIND request/response unit (RU) is sent by the TN3270 server when a client turns off the device or disconnects. The values are: • termself—Termination of all sessions and session requests associated with an LU is ordered upon disconnect. • unbind—Termination of the session by the application is requested upon LU disconnect.
lu-deletion	Displays the value configured for the **lu deletion** siftdown command for the PUs supported by the TN3270 server. The **lu deletion** command specifies whether the TN3270 server sends a REPLY-PSID poweroff request to virtual telecommunications access method (VTAM) to delete the corresponding LU when a client disconnects. The values are: • always—Dynamic LUs for this PU are always deleted upon disconnect. • named—Only named LUs for this PU are deleted upon disconnect. • normal—Only screen LUs for this PU are deleted upon disconnect. • non-generic—Only specified LUs for this PU are deleted upon disconnect. • never—None of the LUs for this PU are ever deleted upon disconnect.
dlur	Configured fully qualified Dependent Logical Unit Requestor (DLUR) CP name(fq-cpname).
status	Shows the status of the DLUR-DLUS pipe followed by the state of the pipe. Values for the status are: • RESET—The pipe is reset. • PND-ACTV—The pipe is pending active. • ACTIVE—The pipe is active. • PND-INAC—The pipe is pending inactive. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the CMCC adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.
dlus	Active DLUS.
name	This is the name of the PU as configured.
ip:tcp	IP address and TCP port number configured for the PU.
xid	Configured exchange identification (XID)—idblk and idnum.

Table 54 show extended channel tn3270-server Field Descriptions (continued)

Field	Description
state	STATE values and their meanings are: • SHUT—The PU is configured but in shut state. • RESET—The link station of this PU is not active. • TEST—PU is sending a TEST to establish link. • XID—TEST is responded, XID is sent. • P-ACTPU—The link station is up but no Activate Physical Unit (ACTPU) is received. • ACTIVE—ACTPU is received and acknowledged positively. • ACT/BUSY—Awaiting host to acknowledge the system services control points (SSCP) data. • WAIT—Waiting for PU status from CMCC adapter. • OTHER—PU in undefined state. • P-RQACTPU-R—DLUR PU is pending request ACTPU response. • P-ACTIVE—ACTPU received by DLUR but not yet passed to PU. • P-DACTPU—PU is pending Deactivate Physical Unit (DACTPU). • UNKNOWN—State cannot be obtained.
link *type*	Link type is either internal adapter type and internal adapter number or dlur if it is a Systems Network Architecture (SNA) Session Switch PU.
Destination	If a direct PU, then it is the destination MAC address; otherwise, it is the name of the partner PU.
r-lsap	Remote and local service access point (SAP) values.

show extended channel tn3270-server client-ip-address

To display information about all clients at a specific IP address, use the **show extended channel tn3270-server client-ip-address** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tn3270-server client-ip-address** *ip-address* [**disconnected** | **in-session** | **pending**]

Syntax Description

slot	Slot number.
port	Port number.
ip-address	IP address of the client.
disconnected	(Optional) Displays all clients with the *ip-address* argument in disconnected state. Disconnected state refers to an logical unit (LU) session state of ACTIVE or INACTIVE. In this case, the *ip-address* argument refers to the client that last used the LU.
in-session	(Optional) Displays all clients with the *ip-address* argument in active session state. Active session state refers to an LU session state of ACT/SESS.
pending	(Optional) Displays all clients with the *ip-address* argument in pending state. Pending session state refers to an LU session state of P-SDT, P-ACTLU, P-NTF/AV, P-NTF/UA, P-RESET, P-PSID, P-BIND, P-UNBIND, WT-UNBND, WT-SDT, or UNKNOWN.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server client-ip-address** command is valid only on the virtual channel interface. Note that this command does not display information about LUs that have never been connected.

Examples

The following is sample output from the **show extended channel tn3270-server client-ip-address** command. The example shows only active sessions because no other session types exist at this client IP address.

```
Router# show extended channel 3/2 tn3270-server client-ip-address 192.195.80.40

lu    name   client-ip:tcp        nail state    model   frames in out   idle for
1   PUS11001 192.195.80.40:3169    Y   ACT/SESS 327804   5       5       0:5:47
```

```
pu is PUS11, lu is DYNAMIC type 2, negotiated TN3270
bytes 155 in, 1758 out; RuSize 1024 in, 3840 out; NegRsp 0 in, 0 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out
```

The following is sample output using the **disconnected** keyword:

```
Router# show extended channel 2/2 tn3270 client-ip-address 10.14.1.21 disconnected

Total 2 clients found using 10.14.1.21
```

The following is sample output using the **in-session** keyword:

```
Router# show extended channel 2/2 tn3270 client-ip-address 10.14.1.21 in-session

Note: if state is ACT/NA then the client is disconnected

lu    name   client-ip:tcp       nail state    model   frames in out   idle for
3    PU1L03 10.14.1.21:35215      N   ACT/SESS 327804    317     316     0:0:1

pu is PU1, lu is DYNAMIC type 2, negotiated TN3270
bytes 12167 in, 225476 out; RuSize 2048 in, 1536 out; NegRsp 0 in, 0 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out
Note: if state is ACT/NA then the client is disconnected

lu    name   client-ip:tcp       nail state    model   frames in out   idle for
4    PU1L04 10.14.1.21:35216      N   ACT/SESS 327804   317     316     0:0:1

pu is PU1, lu is DYNAMIC type 2, negotiated TN3270
bytes 12167 in, 225476 out; RuSize 2048 in, 1536 out; NegRsp 0 in, 0 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out
Note: if state is ACT/NA then the client is disconnected
Total 2 clients found using 10.14.1.21
```

The following is sample output using the **pending** keyword:

```
Router# show extended channel 2/2 tn3270 client-ip-address 10.14.1.21 pending

Total 2 clients found using 10.14.1.21
```

Table 55 describes the significant fields in the display.

Table 55 show extended channel tn3270-server client-ip-address Field Descriptions

Field	Description
lu	Local address of the logical unit (LU).
name	If the physical unit (PU) is directly connected, then the name shown is the one generated by the seed. If LU, then only the unqualified portion is shown. The network entity title (NET) ID portion will be the same as the current Dependent Logical Unit Server (DLUS)
client-ip:tcp	Client's IP address and TCP port number.
nail	Status of LU nailing, either Y or N.

Table 55 show extended channel tn3270-server client-ip-address Field Descriptions (continued)

Field	Description
state	LU state values and their meanings are: • UNKNOWN—LU in an undefined state. • INACTIVE—LU did not receive activate logical unit (ACTLU). • ACT/NA—LU received ACTLU and acknowledged positively. • P-SDT—LU is bound but there is no Structured Data Transfer (SDT) yet.
state (continued)	• ACT/SESS—LU is bound and in session. • P-ACTLU—Telnet connects in and is waiting for ACTLU. • P-NTF/AV—Awaiting host notify-available response. • P-NTF/UA—Awaiting host notify-unavailable response. • P-RESET—Awaiting a buffer to send Deactivate LU (DACTLU) response. • P-PSID—Awaiting NMVT Reply PSID response. • P-BIND—Waiting for host to send bind. • P-UNBIND—Awaiting host unbind response. • WT-UNBND—Waiting for client to acknowledge disconnection. • WT-SDT—Waiting for client to acknowledge SDT.
model	IBM 3278 model type of client; blank if Static LU.
frames in	Number of frames sent inbound to the host.
frames out	Number of frames sent outbound from the host.
idle for	Time the client has been idle. The time is in HH:MM:SS.
pu is	Name of the PU.
lu is	Whether LU is DYNAMIC or STATIC.
negotiated	Whether client is TN3270 or TN3270E.
bytes in/out	Total number of bytes sent to and received from the host.
RuSize in/out	Request/response unit (RU) size as configured in the bind.
NegRsp in/out	Number of Systems Network Architecture (SNA) negative responses sent to and received from the host.
pacing window in/out	SNA pacing window as configured in the bind.
credits in	Number of frames that can be sent inbound without requiring an isolated pacing response.
queue size in	Indicates the number of SNA frames waiting to be sent to the host that are blocked and are waiting for a pacing response.
queue-size out	SNA frames not yet acknowledged by an isolated pacing response by the TN3270 server.

Related Commands

Command	Description
client ip lu	Defines a specific LU or range of LUs to a client at the IP address or subnet.

show extended channel tn3270-server client-name

To display information about all connected clients with a specific machine name, use the **show extended channel tn3270-server client-name** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server client-name** *name*

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
virtual-channel	Virtual channel number.
name	Specifies the client machine name. This name is specified originally in the **client pool** command.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There is not a **no** form for this command.

Examples

The following is sample output from the **show extended channel tn3270-server client-name** command:

```
Router# show extended channel 4/2 tn3270-server client-name dhcp-rtp-34-40.cisco.com

Note: if state is ACT/NA then the client is disconnected

lu    name   client-name           nail state    model    frames in out   idle for
6            dhcp-rtp-34-40.cisco. N    P-ACTLU  3278S2E  1         0     0:1:59

pu is T240CA, lu is DYNAMIC unbound, negotiated TN3270E
bytes 101 in, 0 out; RuSize 256 in, 256 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
response time buckets 0 0 0 0 0
average total response time 0 average IP response time 0
number of transactions 0
Note: if state is ACT/NA then the client is disconnected
lu    name   client-name         nail   state    model frames in out   idle for
7   T240DA07 dhcp-rtp-34-40.cisco. N   P-BIND   3278S2E  4       3       0:1:32
```

```
pu is T240CA, lu is DYNAMIC unbound, negotiated TN3270E
bytes 199 in, 407 out; RuSize 256 in, 256 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
response time buckets 0 0 0 0 0
average total response time 0 average IP response time 0
number of transactions 0
Total 2 clients found using dhcp-rtp-34-40.cisco.com
```

Table 56 describes the significant fields in the display.

Table 56 show extended channel tn3270-server client-name Field Descriptions

Field	Description
lu	Local address of the logical unit (LU).
name	If the physical unit (PU) is directly connected, then the name shown is the one generated by the seed. If LU, then only the unqualified portion is shown. The network entity title (NET) ID portion will be the same as the current Dependent Logical Unit Server (DLUS)
client-name	Client's machine name.
nail	Status of LU nailing, either Y or N.
state	LU state values and their meanings are: • UNKNOWN—LU in an undefined state. • INACTIVE—LU did not receive activate logical unit (ACTLU). • ACT/NA—LU received ACTLU and acknowledged positively. • P-SDT—LU is bound but there is no Structured Data Transfer (SDT) yet. • ACT/SESS—LU is bound and in session. • P-ACTLU—Telnet connects in and is waiting for ACTLU. • P-NTF/AV—Awaiting host notify-available response. • P-NTF/UA—Awaiting host notify-unavailable response. • P-RESET—Awaiting a buffer to send Deactivate LU (DACTLU) response. • P-PSID—Awaiting NMVT Reply PSID response. • P-BIND—Waiting for host to send bind. • P-UNBIND—Awaiting host unbind response. • WT-UNBND—Waiting for client to acknowledge disconnection. • WT-SDT—Waiting for client to acknowledge SDT.
model	IBM 3278 model type of client; blank if Static LU.
frames in	Number of frames sent inbound to the host.
frames out	Number of frames sent outbound from the host.
idle for	Time the client has been idle. The time is in HH:MM:SS.
pu is	Name of the PU.
lu is	Whether LU is DYNAMIC or STATIC.
negotiated	Whether client is TN3270 or TN3270E.

Table 56 show extended channel tn3270-server client-name Field Descriptions (continued)

Field	Description
bytes in/out	Total number of bytes sent to and received from the host.
RuSize in/out	Request/response unit (RU) size as configured in the bind.
NegRsp in/out	Number of Systems Network Architecture (SNA) negative responses sent to and received from the host.
pacing window in/out	SNA pacing window as configured in the bind.
credits in	Number of frames that can be sent inbound without requiring an isolated pacing response.
queue size in	Indicates the number of SNA frames waiting to be sent to the host that are blocked and are waiting for a pacing response.
response time buckets	Number of transactions in each response-time "bucket" for the specified LU. The bucket boundaries are defined using the **response-time group** command.
average total response time	Average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Average IP transit response time (in tenths of seconds) for the total number of response-time transactions.
number of transactions	Total number of response-time transactions across all response-time buckets.

show extended channel tn3270-server dlur

To display information about the Systems Network Architecture (SNA) session switch, use the **show extended channel tn3270-server dlur** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tn3270-server dlur**

Syntax Description

slot	Slot number.
port	Port number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server dlur** command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel tn3270-server dlur** command:

```
Router# show extended channel 3/2 tn3270-server dlur

dlur MPX.GOANCP
current dlus MPX.NGMVMPC                dlur-dlus status ACTIVE
preferred dlus MPX.NGMVMPC              backup dlus MPX.NGMVMPB
preferred server MPX.NGMVMPA
lsap token-adapter   0 5C     vrn MPX.LAN4           status ACTIVE
link P390                 remote 4000.7470.00e7 08  status ACTIVE
```

Table 57 describes the significant fields in the display.

Table 57 show extended channel tn3270-server dlur Field Descriptions

Field	Description
dlur	Fully qualified control point (CP) name used by the SNA session switch and the logical unit (LU) name for the Dependent Logical Unit Requestor (DLUR) function configured as the fully qualified CP named on the dlur statement.
current dlus	Name of the active Dependent Logical Unit Server (DLUS), either the primary DLUS or the backup DLUS.

Table 57 show extended channel tn3270-server dlur Field Descriptions (continued)

Field	Description
dlur-dlus status	Values for the status of the DLUR-DLUS pipe and their meanings are: • RESET—The pipe is reset. • PND-ACTV—The pipe is pending active. • ACTIVE—The pipe is active. • PND-INAC—The pipe is pending inactive. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the Cisco Mainframe Channel Connection (CMCC) adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.
preferred dlus	Name of the DLUS as configured on the DLUR statement.
backup dlus	Name of the DLUS that is used if the preferred DLUS is unavailable.
preferred server	Fully qualified name of the preferred network node server.
lsap	Configured value for the local service access point (SAP) on the configured internal adapter. Token-adapter specifies the type of internal adapter used.
vrn	Name of the connection network as configured by the vrn statement for this Link Service Access Point (LSAP) and internal adapter pair.
lsap...status	LSAP values and their meanings are: • ACTIVE—The SAP is open. • INACTIVE—Not connected to the adapter. • PDN-ACTV—SAP activation in progress. • PND-INAC—SAP deactivation in progress. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the CMCC adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.
link	Name of the configured link. If not a configured link, then the name is an invented name, @DLUR

Table 57 show extended channel tn3270-server dlur Field Descriptions (continued)

Field	Description
remote	Remote MAC and SAP for this link.
link status	Values and their meanings are: • ACTIVE—Link is active. • INACTIVE—Not connected to host. • PND-ACTV—Link activation in progress. • PND-INAC—Link deactivation in progress. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the CMCC adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.

show extended channel tn3270-server dlurlink

To display information about the Dependent Logical Unit Requestor (DLUR) components, use the **show extended channel tn3270-server dlurlink** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tn3270-server dlurlink** *name*

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
port	Port number.
name	Name of the Systems Network Architecture (SNA) session switch link to be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server dlurlink** command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel tn3270-server dlurlink** command:

```
Router# show extended channel 3/2 tn3270-server dlurlink P390

lsap token-adapter  0 5C  vrn MPX.LAN4              status ACTIVE
link P390                 remote 4000.7470.00e7 08  status ACTIVE
partner MPX.NGMVMPC       tgn 1                     maxdata   1033
```

Table 58 describes the significant fields in the display.

Table 58 show extended channel tn3270-server dlurlink Field Descriptions

Field	Description
lsap vrn status	Values and their meanings are: • ACTIVE—The service access point (SAP) is open. • INACTIVE—Not connected to the adapter. • PDN-ACTV—SAP activation in progress. • PND-INAC—SAP deactivation in progress. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the CMCC adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.
link	Name is an invented name, @DLUR*nn*, if not a configured link.
link status	Values and their meanings are: • ACTIVE—The SAP is open. • INACTIVE—Not connected to the adapter. • PDN-ACTV—SAP activation in progress. • PND-INAC—SAP deactivation in progress. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the CMCC adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.
partner	Control point (CP) name of the remote node for this link.
tgn	Transmission group (TG) number for this link. Because the SNA session switch supports only one TG per pair of CP names, it is typically 0 or 1.
maxdata	Maximum frame size allowed on this link.

Related Commands

Command	Description
client pool	Nails clients to pools.

show extended channel tn3270-server nailed-domain

To list all nailing statements with a specific nailed-domain name, use the **show extended channel tn3270-server nailed-domain** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server nailed-domain** *name*

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
virtual-channel	Virtual channel number.
name	Specifies the *exact* nailed-domain name, as specified originally in the **client pool** command. Output is displayed for the nailed-domain name *exactly* as specified. That is, specifying “cisco.com” is different from specifying “.cisco.com.”

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There is not a **no** form for this command.

Examples

The following is sample output from the **show extended channel tn3270-server nailed-domain** command:

```
Router# show extended channel 1/2 tn3270-server nailed-domain .cisco.com

.CISCO.COM  listen-point 172.18.4.18  pool PCPOOL
```

Table 59 describes the significant fields in the display.

Table 59 show extended channel tn3270-server nailed-domain Field Descriptions

Field	Description
.CISCO.COM	Nailed domain name.
listen point	Listen point IP address under which the **client pool** command was configured.
pool	Pool name to which the client is nailed.

show extended channel tn3270-server nailed-ip

To display mappings between a nailed client IP address and nailed logical unit (LU)s, use the **show extended channel tn3270-server nailed-ip** command in user EXEC or privileged EXEC mode.

show extended channel *slot/port* **tn3270-server nailed-ip** *ip-address*

Syntax Description

slot	Slot number.
port	Port number.
ip-address	Remote client IP address.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server nailed-ip** command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel tn3270-server nailed-ip** command:

```
Router# show extended channel 3/2 tn3270-server nailed-ip 172.28.0.0

172.28.1.0  255.255.255.192    pu BAGE1  lu 1     50
172.28.1.80 255.255.255.248    pu BAGE2  lu 100  200    printer
172.28.1.83                    pu BAGE3  lu 1     60    printer
172.28.1.82                    pu BAGE1  lu 100  200
```

Table 60 describes the significant fields in the display.

Table 60 show extended channel tn3270-server nailed-ip Field Descriptions

Field	Description
172.28.1.0	IP address of the nailed client.
255.255.255.192	Network mask for the range of configured nailed clients.
pu BAGE1	PU name under which the **client** command was configured.

Table 60 show extended channel tn3270-server nailed-ip Field Descriptions (continued)

Field	Description
lu 1 50	LU local address range showing the first local address and last local address. There need not be a last local address if only a single local address rather than a range is configured.
printer	Type of device being nailed to the local addresses. If printer is specified, only clients that are printers are nailed to the local addresss. If screen is specified, only clients that are screens are nailed to the local addresss. If neither is specified, both screens and printers can use the local addresss. A printer client is any client with a device type of “328*”. A screen client is a client with any other device type.

show extended channel tn3270-server nailed-name

To list all nailing statements with a specific nailed machine name, use the **show extended channel tn3270-server nailed-name** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server nailed-name** *name*

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
virtual-channel	Virtual channel number.
name	Specifies the nailed machine name. This name is specified originally in the **client pool** command.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel tn3270-server nailed-name** command:

```
Router# show extended channel 1/2 tn3270-server nailed-name myclient.cisco.com

MYCLIENT.CISCO.COM     listen-point 172.18.4.18  pool PCPOOL
HISCLIENT.CISCO.COM    listen-point 172.18.4.18  pool UNIXPOOL
HERCLIENT.CISCO.COM    listen-point 172.18.4.19  pool GENERALPOOL
```

Table 61 describes the significant fields in the display.

Table 61 show extended channel tn3270-server nailed-name Field Descriptions

Field	Description
MYCLIENT.CISCO.COM	Fully qualified domain name of nailed client.
listen point	Listen point IP address under which the **client pool** command was configured.
pool	Pool name to which the client is nailed.

show extended channel tn3270-server pu

To display configuration parameters for a physical unit (PU) and all the logical unit (LU)s attached to the PU, including the logical unit (LU) cluster layout and pool name, use the **show extended channel tn3270-server pu** command in user EXEC or privileged EXEC mode.

show extended channel *slot/virtual-channel* **tn3270-server pu** *pu-name* [**cluster | client-name**]

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
virtual-channel	Virtual channel number.
pu-name	Name that uniquely identifies this PU.
cluster	(Optional) Displays cluster information for the LUs within the pool.
client-name	(Optional) Displays client name information for the LUs within the pool.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
11.2(2.1)	ACT/NA replaced ACTIVE status for logical unit (LU) states. A note was added to the output to describe its meaning.
11.2(18)BC	The **cluster** keyword was added.
12.0(5)T	The following fields were added to the output display: • lu-termination • lu-deletion
12.1(5)T	The **client-name** keyword was added.
12.2	The named value was added for the lu-deletion field in the output display.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server pu** command is valid only on the virtual channel interface. The display shown depends on whether the PU is a direct PU or a Systems Network Architecture (SNA) session switch PU.

The output from the **show extended channel tn3270-server pu** command varies based on use of the optional **cluster** keyword. Without the **cluster** keyword, the output column headings for the LU information appear as "model," "frames in out," and "idle for."

When you use the **cluster** keyword, the output column headings for the LU information appear as "cluster," "pool," and "count." The cluster heading lists the specific cluster within the pool to which the LU belongs, along with the specific cluster layout after the slash.

The pool heading identifies the corresponding pool name, and the count heading identifies the cluster number out of the total number of clusters in the pool.

There is not a **no** form for this command.

Examples

The following example shows a sample router configuration and the corresponding output using the **show extended channel tn3270-server pu** command:

```
interface Channel6/1
 no ip address
 no keepalive
 csna E160 40
!
interface Channel6/2
 ip address 172.18.4.17 255.255.255.248
 no keepalive
 lan TokenRing 15
  source-bridge 15 1 500
  adapter 15 4000.b0ca.0015
 lan TokenRing 16
  source-bridge 16 1 500
  adapter 16 4000.b0ca.0016
 tn3270-server
  pool PCPOOL   cluster layout 4s1p
  pool SIMPLE   cluster layout 1a
  pool UNIXPOOL cluster layout 49s1p
  dlur NETA.SHEK NETA.MVSD
   lsap token-adapter 15 04
    link SHE1     rmac 4000.b0ca.0016
  listen-point 172.18.4.18 tcp-port 23
   pu PU1      91903315 dlur
    allocate lu 1 pool PCPOOL   clusters 10
    allocate lu 51 pool UNIXPOOL clusters 2
    allocate lu 200 pool SIMPLE   clusters 50
  listen-point 172.18.4.19 tcp-port 2023
   pu PU2      91913315 token-adapter 16 08
    allocate lu 1 pool UNIXPOOL clusters 2
    allocate lu 101 pool SIMPLE   clusters 100
    allocate lu 201 pool PCPOOL   clusters 10
```

The following sample output from the **show extended channel tn3270-server pu** command without the cluster keyword for a PU named PU1:

```
Router# show extended channel 6/2 tn3270-server pu pu1

name(index)    ip:tcp               xid   state     link   destination r-lsap
PU1(1)       172.18.4.18:23      91903315 ACTIVE    dlur   NETA.SHPU1

idle-time 0  keepalive 1800 (send nop)  unbind-act disconnect  generic-poolperm
ip-preced-screen 0  ip-preced-printer 0  ip-tos-screen 0  ip-tos-printer 0
lu-termination unbind  lu-deletion never
bytes 27019 in, 73751 out; frames 1144 in, 869 out; NegRsp 0 in, 0 out
actlus 5, dactlus 0, binds 5
Note: if state is ACT/NA then the client is disconnected
```

```
lu    name   client-ip:tcp       nail state    model   frames in out  idle for
1   SHED1001 10.44.100.162:1538   N   ACT/SESS 3278S2E  228     172    0:0:2
51  SHED1051 10.44.100.162:1539   N   ACT/SESS 3278S2E  240     181    0:0:2
151 SHED1151 10.44.100.162:1536   N   ACT/SESS 327802E  212     160    0:0:5
152 SHED1152 10.44.100.162:1537   N   ACT/SESS 3278S2E  220     166    0:0:4
200 SHED1200 10.44.100.162:1557   N   ACT/SESS 3278S2E  244     184    0:0:2
```

The following is sample output from the **show extended channel tn3270-server pu** command with the cluster keyword for a PU named PU1. In the example, 1/1a identifies cluster 1 with a layout of 1a, which contains one LU of any type.

```
Router# show extended channel 6/2 tn3270-server pu pu1 cluster

name(index)    ip:tcp              xid   state     link   destination  r-lsap
PU1(1)       172.18.4.18:23      91903315 ACTIVE    dlur   NETA.SHPU1

idle-time 0  keepalive 1800 (send nop)  unbind-act discon  generic-poolperm
ip-preced-screen 0  ip-preced-printer 0  ip-tos-screen 0  ip-tos-printer 0
lu-termination unbind lu-deletion never
bytes 27489 in, 74761 out; frames 1164 in, 884 out; NegRsp 0 in, 0 out
actlus 5, dactlus 0, binds 5
Note: if state is ACT/NA then the client is disconnected

lu    name   client-ip:tcp       nail state    cluster   pool  count
1   SHED1001 10.44.100.162:1538   N   ACT/SESS 1/4s1p  PCPOOL   1/5
51  SHED1051 10.44.100.162:1539   N   ACT/SESS 1/49s1p UNIXPOOL 1/50
151 SHED1151 10.44.100.162:1536   N   ACT/SESS 1/1a    :GENERIC 1/1
152 SHED1152 10.44.100.162:1537   N   ACT/SESS 1/1a    :GENERIC 1/1
200 SHED1200 10.44.100.162:1557   N   ACT/SESS 1/1a    SIMPLE   1/1
```

Note If the cluster layout is very long, only the first eight bytes are displayed under the cluster column. The pool called: GENERIC is shown for all LUs that are not allocated to any specific pool name.

The following is sample output from the **show extended channel tn3270-server pu** command with the **client-name** keyword for a PU named JADOEPU:

```
Router# show extended channel 1/2 tn3270-server pu jadoepu client-name

  name(index)    ip:tcp              xid   state     link   destination   r-lsap
  JADOEPU(1)   172.18.5.168:23     91922362 ACTIVE    tok 31 4000.4000.0001 04 10

  idle-time    0      keepalive   30      unbind-act discon   generic-pool perm
  ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen  0 ip-tos-printer  0
  lu-termination unbind lu-deletion never
  bytes 824 in, 2619 out; frames 36 in, 39 out; NegRsp 0 in, 0 out
  actlus 4, dactlus 0, binds 3
  Note: if state is ACT/NA then the client is disconnected

  lu    name   client-name            nail  state    model frames in out  idle for
  1   VINCDP01 never connected          Y  ACT/NA          1       1       2:31:43
  2   VINCDP02 never connected          Y  ACT/NA          1       1       2:31:43
  5   VINDG005 HERCLIENT.CISCO.COM      Y  ACT/SESS 327904E 22      21      0:0:6
  6   VINDG006 HISCLIENT.CISCO.COM      Y  ACT/NA   327904E 12      12      1:44:47

  client-ip        mask             nail-type   lu-first  lu-last
  10.20.30.40                       screen      1         2
  20.30.40.50                       screen      9         10

  client-name                       nail-type   lu-first  lu-last
  MYCLIENT.CISCO.COM                screen      5         10
  .CISCO.COM                        screen      11        15
```

Table 62 describes the significant fields in the display.

Table 62 show extended channel tn3270-server pu Field Descriptions

Field	Description
name (index)	Name and index of the PU as configured.
ip:tcp	IP address and TCP port number configured for the PU.
xid	Configured XID—idblk and idnum.
state	pu-state values and their meaning are: • SHUT—PU is configured but in shut state. • RESET—Link station of this PU is not active. • TEST—PU is sending a TEST to establish link. • XID—TEST is responded, exchange identification (XID) is sent. • P-ACTPU—Link station is up but no Activate Physical Unit (ACTPU) is received. • ACTIVE—ACTPU is received and acknowledged positively. • ACT/BUSY—Awaiting host to acknowledge the system services control points (SSCP)-PU data. • WAIT—Waiting for PU status from CMCC adapter. • UNKNOWN—Direct PU in undefined state. • P-RQACTPU-R—PU is pending request ACTPU response. • P-ACTIVE—Dependent Logical Unit Requestor (DLUR) PU and direct PU states disagree. • P-DACTPU—PU is pending Deactivate Physical Unit (DACTPU). • OTHER—State is an undefined value.
link	LINK type is either internal adapter type and internal adapter number, or dlur if it is an SNA Session Switch PU.
destination	If a direct PU, then it is the destination MAC address; otherwise, it is the name of the partner PU.
r-lsap	Remote and local service access point (SAP) values.
idle-time	Configured idle time for this PU.
keepalive	Configured keepalive time for this PU. The *action* is one of the following: • **send nop**—The Telnet command for no operation is sent to the TN3270 client to verify the physical connection. • **send timing mark** *number*—Number of seconds within which the TN3270 server expects a response to the DO TIMING-MARK from the TN3270 client.
unbind-act	Configured unbind action for LUs on this PU.
generic-pool	Configured generic pool for LUs on this PU.
ip-preced-screen	IP precedence value for screen LUs on this PU.
ip-preced-printer	IP precedence value for printer LUs on this PU.

Table 62 show extended channel tn3270-server pu Field Descriptions (continued)

Field	Description
ip-tos-screen *number*	IP type of service (ToS) value for screen LUs on this PU.
ip-tos-printer *number*	IP ToS value for printer LUs on this PU.
lu-termination	Value configured in the PU for the **lu termination** siftdown command. The **lu termination** command specifies whether a TERMSELF or UNBIND request/response unit (RU) is sent by the TN3270 server when a client turns off the device or disconnects. The values are: • termself—Termination of all sessions and session requests associated with an LU is ordered upon disconnect. • unbind—Termination of the session by the application is requested upon LU disconnect.
lu-deletion	Value configured in the PU for the **lu deletion** siftdown command. The **lu deletion** command specifies whether the TN3270 server sends a REPLY-PSID poweroff request to virtual telecommunications access method (VTAM) to delete the corresponding LU when a client disconnects. The values are: • always—Dynamic LUs for this PU are always deleted upon disconnect. • named—Only named LUs for this PU are deleted upon disconnect. • normal—Only screen LUs for this PU are deleted upon disconnect. • non-generic—Only specified LUs for this PU are deleted upon disconnect. • never—None of the LUs for this PU are ever deleted upon disconnect.
bytes in/out	Total number of bytes sent to or received from the host for this PU.
frames in/out	Total number of frames sent to or received from the host for this PU.
NegRsp in/out	Total number of SNA negative responses sent to or received from the host.
actlus	Total number of ACTLUs received from the host.
dactlus	Total number of DACTLUs received from the host.
binds	Total number of BINDs received from the host.
lu	Local address of the LU.
name	Name of the TN3270 LU.
client-name	Client's IP address and TCP port number.
nail	Status of LU nailing, either Y or N

Table 62 show extended channel tn3270-server pu Field Descriptions (continued)

Field	Description
state	LU state values and their meanings: • UNKNOWN—LU in an undefined state. • INACTIVE—LU did not receive activate logical unit (ACTLU). • ACT/NA—LU received ACTLU and acknowledged positively. If a client IP address is shown, then the client is disconnected. • P-SDT—LU is bound but there is no Structured Data Transfer (SDT) yet. • ACT/SESS—LU is bound and in session. • P-ACTLU—Telnet has connected and is awaiting ACTLU. • P-NTF/av—Awaiting host notify-available response. • P-NTF/UA—Awaiting host notify-unavailable response. • P-RESET—Waiting for a buffer to send Deactivate LU (DACTLU) response. • P-PSID—Waiting for NMVT Reply psid response. • P-BIND—Waiting for host to send bind. • P-UNBIND—Awaiting host unbind response. • WT-UNBND—Waiting for client to acknowledge disconnection. • WT-SDT—Waiting for client to acknowledge SDT.
model	IBM 3278 model type of client.
frames in	Number of frames sent inbound to the host.
frames out	Number of frames sent outbound from the host.
idle for	Time the client has been idle. The time is in HH:MM:SS.
client-ip	Remote client IP address.
mask	Current network mask.
nail-type	LU nailing type, screen or printer.
lu-first	First LU address in the range.
lu-last	Last LU address in the range, if one is specified in the **client** configuration command.
client-name	Client machine name or domain name.
nail-type	LU nailing type, screen or printer.
lu-first	First LU address in the range.
lu-last	Last LU address in the range, if one is specified in the **client** configuration command.

Related Commands

Command	Description
allocate lu	Assigns LUs to a pool.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.

show extended channel tn3270-server pu lu

To display information about the TN3270 server logical unit (LU)s running on the Cisco Mainframe Channel Connection (CMCC) adapter interface, use the **show extended channel tn3270-server pu lu** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tn3270-server pu** *pu-name* **lu** *locaddr* [**history**]

Syntax Description

slot	Specifies a particular CMCC adapter in the router where the *slot* argument is the slot number. The port value for a TN3270 server will always be 2.
port	Port value for a TN3270 server will always be 2.
pu-name	Physical unit (PU) name that uniquely identifies this PU.
locaddr	Logical unit (LU) local address that uniquely identifies the LU.
history	(Optional) Displays the LU trace history.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
11.2(2.1)	ACT/NA replaced ACTIVE status for LU states. A note was added to the output to describe its meaning.
11.2(18)BC	The response time buckets, average total response time, average IP response time, and the number of transactions fields were added to the output display.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server pu lu** command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel tn3270-server pu lu** command for a Systems Network Architecture (SNA) session switch PU:

```
Router# show extended channel 3/2 tn3270 pu int1 lu 1

Note: if state is ACT/NA then the client is disconnected

lu    name   client-ip:tcp       nail  state      model   frames in out   idle for
```

```
1   GOAN1X01 10.69.176.77:3828    N    ACT/NA              4       4       0:4:51

pu is INT1, lu is STATIC type 0, negotiated TN3270E
bytes 74 in, 1219 out; RuSize 0 in, 0 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
```

The following is sample output from the **show extended channel tn3270-server pu lu history** command:

```
Router# show extended channel 3/2 tn3270 pu pus20 lu 1 history

Note: if state is ACT/NA then the client is disconnected

lu    name    client-ip:tcp       nail  state      model   frames in out   idle for
1   PUS20001 10.195.80.40:2480    N    ACT/SESS  327804    5       4       0:0:8

pu is PUS20, lu is DYNAMIC type 2, negotiated TN3270
bytes 155 in, 1752 out; RuSize 1024 in, 3840 out; NegRsp 0 in, 0 out>pacing window 0 in, 1
out; credits 0 in, queue-size 0 in, 0 out
traces:
         Client connect req
         Reply PSID pos rsp
         actlu req
         bind req
         sdt req
OUT len=12   2Dxxxxxxxx456B80000D0201
IN  len=25   xxxxxxxxxx45EB80000D0201000000
OUT len=53   2Dxxxxxxxx466B800031010303B1
IN  len=10   2D0001010646EB800031
OUT len=10   2D00010106476B8000A0
IN  len=10   2D0001010647EB8000A0
OUT len=1677 2Cxxxxxxxx010381C07EC7114040
IN  len=9    2C0001010001838100
```

The following example shows the response-time information using the **show extended channel tn3270-server pu lu** command for the LU at local address 1 associated with the PU named vincdpu:

```
sydney# show extended channel 1/2 tn3270-server pu vincdpu lu 1
Note: if state is ACT/NA then the client is disconnected

lu    name    client-ip:tcp       nail   state    model frames in out   idle for
1   VINDG001 10.44.100.210:1315   N   ACT/NA   3278S2E  12      11      0:0:18

pu is VINCDPU, lu is DYNAMIC unbound, negotiated TN3270E
bytes 253 in, 954 out; RuSize 0 in, 0 out; NegRsp 1 in, 0 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out
response time buckets 14 31 15 3 1
average total response time 19 average IP response time 8
number of transactions 64
```

Table 63 describes the significant fields in the display.

Table 63 show extended channel tn3270-server pu lu Field Descriptions

Field	Description
lu	Local address of the LU.
name	Name of the TN3270 LU.
client-ip:tcp	Client's IP address and TCP port number.

Table 63 show extended channel tn3270-server pu lu Field Descriptions (continued)

Field	Description
state	LU state values and their meanings are: • UNKNOWN—LU in an undefined state. • INACTIVE—LU did not receive activate logical unit (ACTLU). • ACT/NA—LU received ACTLU and acknowledged positively. If a client IP address is shown, then the client is disconnected. • P-SDT—LU is bound but there is no Structured Data Transfer (SDT) yet. • ACT/SESS—LU is bound and in session. • P-ACTLU—Telnet connects in and is awaiting ACTLU. • P-NTF/AV—Awaiting host notify-available response. • P-NTF/UA—Awaiting host notify-unavailable response. • P-RESET—Waiting for a buffer to send Deactivate LU (DACTLU) response. • P-PSID—Waiting for NMVT Reply PSID response. • P-BIND—Waiting for host to send bind. • P-UNBIND—Awaiting host unbind response. • WT-UNBND—Waiting for client to acknowledge disconnection. • WT-SDT—Waiting for client to acknowledge SDT.
model	IBM 3278 model type of client; blank if Static LU.
frames in	Number of frames sent inbound to the host.
frames out	Number of frames sent outbound from the host.
idle for	Time the client has been idle. The time is in HH:MM:SS.
pu is	Name of the PU.
lu is	Whether LU is DYNAMIC or STATIC.
negotiated	Whether client is TN3270 or TN3270E.
bytes in/out	Total number of bytes sent to or received from the host.
RuSize in/out	Request/response unit (RU) size as configured in the bind.
NegRsp in/out	Number of Systems Network Architecture (SNA) negative responses sent to or received from the host.
pacing window in/out	SNA pacing window as configured in the bind.
credits in	Number of frames that can be sent inbound without requiring an isolated pacing response.
queue-size in	If nonzero, indicates the number of SNA frames waiting to be sent to the host that are blocked, waiting for a pacing response.
queue-size out	SNA frames not yet acknowledged by an isolated pacing response by the TN3270 server.

Table 63 show extended channel tn3270-server pu lu Field Descriptions (continued)

Field	Description
response time buckets	Displays the number of transactions in each response-time "bucket" for the specified LU. The bucket boundaries are defined using the **response-time group** command.
average total response time	Average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
response-time group	Configures a client subnet group for response-time measurements.

show extended channel tn3270-server response-time application

To display information for application client groups, use the **show extended channel tn3270-server response-time application** command in privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server response-time application** [*appl-name* [**detail**]]

Syntax Description

slot	Slot number.
virtual-channel	Virtual channel number.
appl-name	(Optional) Display only the client group corresponding to the virtual telecommunications access method (VTAM) application name.
detail	(Optional) List client members and their response-time statistics following the client group entry.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If optional keywords are not used for the **show extended channel tn3270-server response-time application** command, a complete list of existing per-application client groups is displayed along with their collection control parameters. If you specify the *appl-name* argument, only the client group corresponding to that application is displayed. If you specify the **detail** keyword, the client group entry is followed by a list of its client members and their response-time statistics.

Examples

The following is sample output from the **show extended channel tn3270-server response-time application** command:

```
Router# show extended channel 3/2 tn3270-server response-time application MYAPPL
group APPL MYAPPL
  aggregate NO excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
```

Table 64 describes the significant fields in the display.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 64 show extended channel tn3270-server response-time application Field Descriptions

Field	Description
aggregate	Displays whether the response time statistics for the clients in this response-time group are reported collectively for the group (YES) or individually by client (NO). This value is automatically set to NO by the TN3270 server for application client response-time groups.
excludeip	Displays whether the IP component (the client/server path) is included in the response time for any transaction (NO) or if only the Systems Network Architecture (SNA) component (the server/host path) is included in the response time for any transaction (YES). This value is automatically set to NO by the TN3270 server for application client response-time groups.
dynamic definite response	Displays whether the server adds a Definite Response request to the first-in-chain (FIC) reply in each transaction, to get a response from the client so that the IP component can be included in the response time. The value is automatically set to NO by the TN3270 server for all types of response-time groups.
sample period multiplier	Displays the number that is multiplied by an interval of 20 seconds to determine the collection interval for the response-time group. The multiplier value is defined using the **response-time group** command. For example, a sample period multiplier of 30 results in a collection interval of 600 seconds (30 x 20 seconds), or 10 minutes, for this client group.
response time buckets	Displays the number of transactions in each response-time "bucket" for the specified application group. The bucket boundaries are defined using the **response-time group** command.
average total response time	Displays the average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Displays the average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Displays the total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.

Command	Description
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.

show extended channel tn3270-server response-time global

To display collection control parameters for the global client group, use the **show extended channel tn3270-server response-time global** command in privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server response-time global**

Syntax Description

slot	Slot number.
virtual-channel	Virtual channel number.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server response-time global** command displays collection control parameters for the global client group.

Examples

The following is sample output from the **show extended channel tn3270-server response-time global** command:

```
Router# show extended channel 3/2 tn3270-server response-time global

group CLIENT GLOBAL
  aggregate YES excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 105 118 211 109 104
  average total response time 33 average IP response time 24
  number of transactions 647
```

Table 65 describes the significant fields in the display.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 65 show extended channel tn3270-server response-time global Field Descriptions

Field	Description
aggregate	Displays whether the response time statistics for the clients in this response-time group are reported collectively for the group (YES) or individually by client (NO). This value is automatically set to YES by the TN3270 server for global client response-time groups.
excludeip	Displays whether the IP component (the client/server path) is included in the response time for any transaction (NO) or if only the Systems Network Architecture (SNA) component (the server/host path) is included in the response time for any transaction (YES). This value is automatically set to NO by the TN3270 server for global client response-time groups.
dynamic definite response	Displays whether the server adds a Definite Response request to the first-in-chain (FIC) reply in each transaction, to get a response from the client so that the IP component can be included in the response time. The value is automatically set to NO by the TN3270 server for all types of response-time groups.
sample period multiplier	Displays the number that is multiplied by an interval of 20 seconds to determine the collection interval for the response-time group. The multiplier value is defined using the **response-time group** command. For example, a sample period multiplier of 30 results in a collection interval of 600 seconds (30 x 20 seconds), or 10 minutes, for this client group.
bucket boundaries	Displays the value of the response-time bucket boundaries in tenths of seconds. The bucket boundaries are defined using the **response-time group** command.
buckets	Displays the number of transactions in each response-time bucket for the specified application group.
average total response time	Displays the average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Displays the average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Displays the total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.

show extended channel tn3270-server response-time link

To display information about host link client groups, use the **show extended channel tn3270-server response-time link** command in privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server response-time link** [*link-name*]

Syntax Description

slot	Slot number.
virtual-channel	Port number.
link-name	(Optional) physical unit (PU) name for a direct PU or link name for a Dependent Logical Unit Requestor (DLUR) PU.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(18)BC	This command was first introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays information clients groups by host link. If no optional arguments are specified, a complete list of existing client groups by host link is displayed along with their collection control parameters and aggregate response-time statistics. If a value for the *link-name* argument is specified, only the client group corresponding to that link is displayed.

Examples

The following is sample output from the **show extended channel tn3270-server response-time link** command without optional arguments. It shows all client groups by host link:

```
Router# show extended channel 3/2 tn3270-server response-time link

group DIRECT LINK MYLINK
  aggregate YES excludeip YES dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 10 18 21 10 10
  average total response time 37 average IP response time 23
  number of transactions 69
group DLUR LINK HISLINK
  aggregate YES excludeip YES dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 14 31 15 3 1
```

```
  average total response time 19 average IP response time 8
  number of transactions 64
```

The following is sample output from the **show extended channel tn3270-server response-time link** command for the link named Direct link mylink:

```
Router# show extended channel 3/2 tn3270-server response-time link direct link mylink

group DIRECT LINK MYLINK
  aggregate YES excludeip YES dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 10 18 21 10 10
  average total response time 37 average IP response time 23
  number of transactions 69
```

Table 66 describes the significant fields in the display.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 66 show extended channel tn3270-server response-time link Field Descriptions

Field	Description
aggregate	Displays whether the response time statistics for the clients in this response-time group are reported collectively for the group (YES) or individually by client (NO). This value is automatically set to YES by the TN3270 server for link client response-time groups.
excludeip	Displays whether the IP component (the client/server path) is included in the response time for any transaction (NO) or if only the Systems Network Architecture (SNA) component (the server/host path) is included in the response time for any transaction (YES). This value is automatically set to YES by the TN3270 server for link client response-time groups.
dynamic definite response	Displays whether the server adds a Definite Response request to the first-in-chain (FIC) reply in each transaction, to get a response from the client so that the IP component can be included in the response time. The value is automatically set to NO by the TN3270 server for all types of response-time groups.
sample period multiplier	Displays the number that is multiplied by an interval of 20 seconds to determine the collection interval for the response-time group. The multiplier value is defined using the **response-time group** command. For example, a sample period multiplier of 30 results in a collection interval of 600 seconds (30 x 20 seconds), or 10 minutes, for this client group.
bucket boundaries	Displays the value of the response-time bucket boundaries in tenths of seconds. The bucket boundaries are defined using the **response-time group** command.
buckets	Displays the number of transactions in each response-time bucket for the specified application group.

Table 66 show extended channel tn3270-server response-time link Field Descriptions

Field	Description
average total response time	Displays the average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Displays the average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Displays the total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.

show extended channel tn3270-server response-time listen-point

To display information about listen-point client groups, use the **show extended channel tn3270-server response-time listen-point** command in privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server response-time listen-point**

Syntax Description

slot	Slot number.
virtual-channel	Virtual channel number.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(18)BC	This command was first introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server response-time listen-point** command displays information about groups of clients summarized by listen point. A complete list of currently existing listen-point client groups is displayed along with their collection control parameters and aggregate response-time statistics.

Examples

The following is sample output from the **show extended channel tn3270-server response-time listen-point** command:

```
Router# show extended channel 3/2 tn3270-server response-time listen-point

group LP 10.20.30.40:23
  aggregate YES excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 10 18 21 10 10
  average total response time 37 average IP response time 23
  number of transactions 69
group LP 50.60.70.80:23
  aggregate YES excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 310 418 521 510 210
```

```
average total response time 27 average IP response time 20
number of transactions 1969
```

Table 67 describes the significant fields in the display.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 67 show extended channel tn3270-server response-time listen-point Field Descriptions

Field	Description
aggregate	Displays whether the response time statistics for the clients in this response-time group are reported collectively for the group (YES) or individually by client (NO). This value is automatically set to YES by the TN3270 server for link client response-time groups.
excludeip	Displays whether the IP component (the client/server path) is included in the response time for any transaction (NO) or if only the Systems Network Architecture (SNA) component (the server/host path) is included in the response time for any transaction (YES). This value is automatically set to NO by the TN3270 server for link client response-time groups.
dynamic definite response	Displays whether the server adds a Definite Response request to the first-in-chain (FIC) reply in each transaction, to get a response from the client so that the IP component can be included in the response time. The value is automatically set to NO by the TN3270 server for all types of response-time groups.
sample period multiplier	Displays the number that is multiplied by an interval of 20 seconds to determine the collection interval for the response-time group. The multiplier value is defined using the **response-time group** command. For example, a sample period multiplier of 30 results in a collection interval of 600 seconds (30 x 20 seconds), or 10 minutes, for this client group.
bucket boundaries	Displays the value of the response-time bucket boundaries in tenths of seconds. The bucket boundaries are defined using the **response-time group** command.
buckets	Displays the number of transactions in each response-time bucket for the specified application group.
average total response time	Displays the average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Displays the average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Displays the total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.

show extended channel tn3270-server response-time subnet

To display information about subnet client groups, use the **show extended channel tn3270-server response-time subnet** command in privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server response-time subnet** [**ip-address** *ip-mask* [**detail**]]

Syntax Description

slot	Slot number.
virtual-channel	Virtual channel number.
ip-address	(Optional) Subnet IP address.
ip-mask	(Optional) Subnet mask.
detail	(Optional) Each client group entry is followed by a list of its client members and their respective response-time statistics.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(18)BC	This command was first introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays information about client subnet client groups. This includes all configured groups and the CLIENT SUBNET OTHER group. If no optional parameters are specified, a complete list of client subnet client groups is displayed along with their collection control parameters. If you specify values for the **ip-address** keyword and *ip-mask* argument, only client groups containing that subnet are displayed. If you specify the **detail** keyword, each client group entry is followed by a list of its client members and their response-time statistics.

Examples

The following is sample output from all configured client groups using the **show extended channel tn3270-server response-time subnet** command:

```
Router# show extended channel 3/2 tn3270-server response-time subnet

group SUBNETGROUP1
  subnet 10.10.10.0 255.255.255.192
  aggregate NO excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
```

```
group SUBNETGROUP2
  subnet 10.10.10.128 255.255.255.192
  subnet 10.10.10.192 255.255.255.192
  aggregate NO exclude ip NO dynamic definite response NO
  sample period multiplier 40
  bucket boundaries 20 30 60 120
group CLIENT SUBNET OTHER
  aggregate NO exclude ip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
```

The following is sample output from subnet 10.10.10.0 with IP mask 255.255.255.192, which shows a list of the client members and their response-time statistics:

```
Router# show extended channel 3/2 tn3270-server response-time subnet
10.10.10.0 255.255.255.192 detail

group SUBNETGROUP1
  subnet 10.10.10.0 255.255.255.192
  aggregate NO excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  client 10.10.10.129:23
    buckets 5 8 11 9 4
    average total response time 33 average IP response time 24
    number of transactions 37
  client 10.10.10.130:23
    buckets 6 9 10 10 2
    average total response time 32 average IP response time 25
    number of transactions 37
  client 10.10.10.131:23
    buckets 11 14 10 8 7
    average total response time 27 average IP response time 19
    number of transactions 50
```

Table 68 describes the significant fields in the display.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 68 show extended channel tn3270-server response-time subnet Field Descriptions

Field	Description
subnet	Displays the IP address and IP mask of the client subnet group for which response-time statistics are being shown.
aggregate	Displays whether the response time statistics for the clients in this response-time group are reported collectively for the group (YES) or individually by client (NO). This value is automatically set to NO by the TN3270 server for subnet client response-time groups.

Table 68 show extended channel tn3270-server response-time subnet Field Descriptions (continued)

Field	Description
excludeip	Displays whether the IP component (the client/server path) is included in the response time for any transaction (NO) or if only the Systems Network Architecture (SNA) component (the server/host path) is included in the response time for any transaction (YES). This value is automatically set to NO by the TN3270 server for subnet client response-time groups.
dynamic definite response	Displays whether the server adds a Definite Response request to the first-in-chain (FIC) reply in each transaction, to get a response from the client so that the IP component can be included in the response time. The value is automatically set to NO by the TN3270 server for all types of response-time groups.
sample period multiplier	Displays the number that is multiplied by an interval of 20 seconds to determine the collection interval for the response-time group. The multiplier value is defined using the **response-time group** command. For example, a sample period multiplier of 30 results in a collection interval of 600 seconds (30 x 20 seconds), or 10 minutes, for this client group.
bucket boundaries	Displays the value of the response-time bucket boundaries in tenths of seconds. The bucket boundaries are defined using the **response-time group** command.
buckets	Displays the number of transactions in each response-time bucket for the specified application group.
average total response time	Displays the average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Displays the average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Displays the total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.

show extended channel tn3270-server security

To display information about the TN3270 security enhancement, use the **show extended channel tn3270-server security** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server security** [**sec-profile** *profilename*] [**listen-point** *ip-address* [**tcp-port** *number*]]

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
virtual-channel	Virtual channel number.
sec-profile *profilename*	(Optional) Alphanumeric name that specifies the security profile name to be associated with a listen point. The character range is from 1 to 24. This name is specified originally in the **profile** command.
listen-point *ip-address*	(Optional) IP address that the clients should use as the host IP address to map to logical unit (LU) sessions under this physical unit (PU) and listen point.
tcp-port *number*	(Optional) Port number used for the listen operation. The default value is 23.

Defaults

The default **tcp-port** value is 23.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There is not a **no** form for this command.

Examples

The following is sample output from the **show extended channel tn3270-server security** command with the optional **sec-profile** keyword configured:

```
Router# show extended channel 3/2 tn3270-server security sec-profile cert40

status:ENABLE Default Profile: (Not Configured)
Name               Active LUs  keylen encryptorder            Mechanism
CERT40                     0     40    RC4 RC2 RC5 DES 3DES    SSL
Servercert:slot0:coach188.pem
```

```
Certificate Loaded:YES Default-Profile:NO
```

The following is sample output from the **show extended channel tn3270-server security** command with the optional **listen-point** keyword configured:

```
Router# show extended channel 3/2 tn3270-server security listen-point 172.18.5.188

status:ENABLE Default Profile: (Not Configured)
IPaddress      tcp-port   Security-Profile   active-sessions  Type    State
172.18.5.188    23        CERT40               0              Secure  ACTIVE
Active Sessions using Deleted Profile:0
```

Table 69 describes the significant fields in the display.

Table 69 show extended channel tn3270-server security Field Descriptions

Field	Description
status ENABLE	Status of TN3270 server security. Enable or Disable.
Default Profile (Not Configured)	Displays if a default profile is configured. (Not Configured) or (Configured).
Name	Name of the security profile as specified in the **profile** command.
Active LUs	Number of active LUs.
keylen	Maximum encryption key length in bits.
encryptorder	Order of encryption algorithms. Choices are DES, 3DES, RC4, RC2, or RC5.
Mechanism	Type of security protocol being used. Values are SSL or none.
Servercert	Location of the TN3270 server's security certificate status in the Flash memory.
Certificate Loaded	Security certificate is loaded. YES or NO.
Default-Profile	Default profile is configured. YES or NO.
IPaddress	IP address that the clients should use as the host IP address to map to LU sessions under this PU and listen point.
tcp-port	Port number used for the listen operation. The default value is 23.
Security-Profile	Name of the security profile as specified in the **profile** command.
active-sessions	Number of active sessions.
Type	Type of connection.
State	State of the listen point.
Active Sessions using Deleted Profile:	Number of sessions using a security profile that has been deleted.

Related Commands

Command	Description
sec-profile	Specifies the security profile to be associated with a listen point.
listen-point	Defines an IP address for the TN3270 server.

show extended channel udp-listeners

To display information about the User Datagram Protocol (UDP) listener sockets running on the Cisco Mainframe Channel Connection (CMCC) adapter interfaces, use the **show extended channel udp-listeners** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **udp-listeners** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
udp-listeners	Specifies UDP listener port display.
ip-address	(Optional) IP address specified by the **offload** interface configuration command or the **tn3270-server pu** command.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel udp-listeners** command is valid on both physical and virtual channel interfaces.

Examples

The following is sample output from the **show extended channel udp-listeners** command:

```
Router# show extended channel 0/1 udp-listeners

UDP Listener: IP Address 10.11.198.3        LocalPort 7
UDP Listener: IP Address 10.11.198.3        LocalPort 9
UDP Listener: IP Address 10.11.198.3        LocalPort 19
```

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.

Command	Description
pu (TN3270)	Creates a PU entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.

show extended channel udp-stack

To display information about the User Datagram Protocol (UDP) stack running on the Cisco Mainframe Channel Connection (CMCC) adapter interfaces, use the **show extended channel udp-stack** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **udp-stack** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
udp-stack	Selects UDP stack display.
ip-address	(Optional) IP address specified by the **offload** interface configuration command or the **tn3270-server pu** command.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	The Alias addresses field was added to the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel udp-stack** command is valid on both physical and virtual channel interfaces.

Examples

The following is sample output from the **show extended channel udp-stack** command:

```
Router# show extended channel o1 udp-stack

UDP Statistics for IP Address 10.11.198.2
  InDatagrams : 6            NoPorts     : 6
  InErrors    : 0            OutDatagrams: 0
UDP Statistics for IP Address 10.11.198.3
  InDatagrams : 6            NoPorts     : 6
  InErrors    : 0            OutDatagrams: 1
```

The following examples show sample output from the **show extended channel udp-stack** command when you specify the real IP address or the alias IP address, for an offload device at real IP address 10.10.21.3 and alias IP address of 10.2.33.88:

```
Router# show extended channel 3/1 udp-stack 10.10.21.3

UDP Statistics for IP Address 10.10.21.3
```

```
 Alias addresses: 10.2.33.88
  InDatagrams : 6            NoPorts     : 6
  InErrors    : 0            OutDatagrams: 1

Router# show extended channel 3/1 udp-stack 10.2.33.88

UDP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  InDatagrams : 6            NoPorts     : 6
  InErrors    : 0            OutDatagrams: 1
```

Table 70 describes the specified fields shown in the display.

Table 70 show extended channel udp-stack Field Descriptions

Field	Description
Alias addresses	Virtual IP addresses assigned to the real IP address of an offload device.
InDatagrams	Total number of UDP datagrams delivered to UDP users.
NoPorts	Total number of received UDP datagrams for which there was no application at the destination port.
InErrors	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
OutDatagrams	Total number of UDP datagrams sent from this entity.

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
pu (TN3270)	Creates a physical unit (PU) entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.