show cable-diagnostics tdr through switchport voice vlan

- show cable-diagnostics tdr, page 3
- show etherchannel, page 6
- show interfaces, page 14
- show interfaces port-channel, page 60
- show l2protocol-tunnel, page 67
- show lacp, page 72
- show link state group, page 79
- show mac-address-table dynamic, page 80
- show pagp, page 85
- show power inline, page 87
- snmp trap illegal-address, page 89
- speed, page 91
- switchport, page 98
- switchport access vlan, page 102
- switchport autostate exclude, page 104
- switchport backup, page 106
- switchport block unicast, page 109
- switchport mode, page 111
- switchport port-security, page 115
- switchport port-security aging, page 117
- switchport private-vlan host-association, page 119
- switchport private-vlan mapping, page 121
- switchport protected, page 123

- switchport trunk, page 125
- switchport voice vlan, page 132

show cable-diagnostics tdr

To display the test results for the Time Domain Reflectometry (TDR) cable diagnostics, use the **showcable-diagnosticstdr**command in privileged EXEC mode.

show cable-diagnostics tdr interface *interface interface-number*

Syntax Description

interface *interface*	Specifies the interface type; valid values are**fastethernet** and **gigabitethernet**.
interface-number	Module and port number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

12.2(18)SXD	The output was changed as follows:
	• The Local Pair field was changed to the Pair field. The local pair designations were changed as follows:
	  • Pair A to Pair 1-2
	  • Pair B to Pair 3-4
	  • Pair C to Pair 5-6
	  • Pair D to Pair 7-8
	• The Remote Pair field was removed.
	• The Channel field was added to display the pair designation and are as follows:
	  • Pair A
	  • Pair B
	  • Pair C
	  • Pair D

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **showcable-diagnosticstdr** command is supported on specific modules. See the Release Notes for Cisco IOS Release 12.2 SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720, Superivsor Engine 32, and Supervisor Engine 2 for the list of the modules that support TDR.

In the event of an open or shorted cable, the accuracy of length of where the cable is open or shorted is plus or minus 2 meters.

The pair length can be displayed in meters (m), centimeters (cm), or kilometers (km).

If the TDR test has not been run on the port, the following message is displayed:

```
TDR test was never run on Gi2/12
```

Examples

This example shows how to display the information about the TDR test:

```
Router# show cable-diagnostics tdr interface gigabitethernet 8/1
TDR test last run on: February 25 11:18:31
Interface Speed Pair Cable length        Distance to fault   Channel Pair status
--------- ----- ---- ------------------- ------------------- ------- ------------
Gi8/1     1000  1-2  1    +/- 6  m       N/A                 Pair B  Terminated
                3-4  1    +/- 6  m       N/A                 Pair A  Terminated
                5-6  1    +/- 6  m       N/A                 Pair C  Terminated
                7-8  1    +/- 6  m       N/A                 Pair D  Terminated
```

The table below describes the fields in the **showcable-diagnosticstdr**command output.

Table 1: show cable-diagnostics tdr Command Output Fields

Field	Description
Interface	Interface tested.
Speed	Current line speed.
Pair	Local pair name.
Cable Length	Cable length and accuracy. The accuracy unit is displayed in meters (m), centimeters (cm), or kilometers (km).
Channel	Pair designation.

Field	Description
Pair status	Pair status displayed is one of the following: • Terminated--The link is up. • Shorted--A short is detected on the cable. • Open--An opening is detected on the cable. • Not Completed--The test on the port failed. • Not Supported--The test on the port is not supported. • Broken--The pair is bad--either open or shorted. • ImpedanceMis--The impedance is mismatched. • InProgress--The diagnostic test is in progress.

Related Commands

Command	Description
clear cable-diagnostics tdr	Clears a specific interface or clear all interfaces that support TDR.
test cable-diagnostics	Tests the condition of 10-Gigabit Ethernet links or copper cables on 48-port 10/100/1000 BASE-T modules.

show etherchannel

To display EtherChannel information for a channel, use the **showetherchannel** command in privileged EXEC mode.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

show etherchannel [*channel-group*] {**port-channel**| **brief**| **detail**| **summary**| **port**| **load-balance**}

Cisco Catalyst Switches

show etherchannel [*channel-group*] {**port-channel**| **brief**| **detail**| **summary**| **port**| **load-balance**| **protocol**} [*expression*]

Syntax Description

channel -group	(Optional) Number of the channel group. If you do not specify a value for the *channel -group* argument, all channel groups are displayed.
port -channel	Displays port channel information.
brief	Displays a summary of EtherChannel information.
detail	Displays detailed EtherChannel information.
summary	Displays a one-line summary per channel group.
port	Displays EtherChannel port information.
load -balance	Displays load-balance information.
protocol	Displays the enabled protocol.
expression	(Optional) Expression in the output to use as a reference point.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XE	This command was introduced on Cisco Catalyst 6000 family switches.
12.1(3a)E3	This command was modified. The number of valid values for the *channel -group* argument were changed.

Release	Modification
12.1(5c)EX	This command was modified. The number of valid values for the *channel-group* argument were changed.
12.2(2)XT	This command was modified to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17a)SX1	This command was modified. The output of the **showetherchannelload-balance** command was changed to include IPv6 information. The display was changed to include Multiprotocol Label Switching (MPLS) information.
12.2(17d)SXB	This command was modified to support the Supervisor Engine 2.
12.2(8)T	This command was modified to support switchport creation.
12.2(33)SXH	This command was modified. The output of the **showetherchannelport-channel** and the **showetherchanneldetail**commands was changed to include Link Aggregation Control Protocol (LACP) fast switchover status. The number of valid values for the *channel -group* argument was changed.
12.2(33)SRC	This command was modified. The output of the **showetherchannelport-channel** and the **showetherchanneldetail**commands was changed to show the status of the LACP Single Fault Direct Load Balance Swap feature, to show the last applied hash distribution algorithm, and to include LACP fast switchover status.
12.2(33)SXI3	This command was modified. The output of the **showetherchannelsummary**, **showetherchannelport-channel**, and **showetherchanneldetail** commands was changed to show the standalone disable option.

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The *channel-group* argument supports six EtherChannels and eight ports in each channel.

If you do not specify a value for the *channel-group* argument, all channel groups are displayed.

Cisco Catalyst Switches

The number of valid values for the *channel-group* argument depends on the software release. For software releases prior to Cisco IOS Release 12.1(3a)E3, valid values are from 1 to 256; for Cisco IOS Release 12.1(3a)E3, 12.1(3a)E4, and 12.1(4)E1, valid values are from 1 to 64. Cisco IOS Release 12.1(5c)EX and later support a maximum of 64 values ranging from 1 to 256. Cisco IOS Release 12.2(33)SXH supports a maximum of 64 values ranging fro m 1 to 282.

If you do not specify a value for the *channel-group* argument, all channel groups are displayed.

In the output, the Passive port list field is displayed for Layer 3 port channels only. This field means that the physical interface, which is still not up, is configured to be in the channel group (and indirectly in the only port channel in the channel group).

The *channel-group*values from 257 to 282 are supported on the Catalyst 6500 series Cisco Services Module (CSM) and the Catalyst 6500 series Firewall Services Module (FWSM) only.

In the output, the Passive port list field is displayed for Layer 3 port channels only. This field means that the physical interface, which is still not up, is configured to be in the channel group (and indirectly is the only port channel in the channel group).

If the interface is configured as part of the channel in ON mode, the**showetherchannelprotocol** command displays Protocol: - (Mode ON).

In the output of the **showetherchannelsummary** command, the following conventions apply:

- In the column that displays the protocol that is used for the channel, if the channel mode is ON, a hyphen (-) is displayed.
- For LACP, multiple aggregators are supported. For example, if two different bundles are created, Po1 indicates the primary aggregator, and Po1A and Po1B indicates the secondary aggregators.

In the output of the **showetherchannelload-balance** command, the following conventions apply:

- For EtherChannel load balancing of IPv6 traffic, if the traffic is bridged onto an EtherChannel (for example, it is a Layer 2 channel and traffic in the same VLAN is bridged across it), the traffic is always load balanced by the IPv6 addresses or src, dest, or src-dest, depending on the configuration. For this reason, the switch ignores the MAC/IP/ports for bridged IPv6 traffic. If you configure src-dst-mac, the src-dst-ip(v6) address is displayed. If you configure src-mac, the src-ip(v6) address is displayed.
- IPv6 traffic that is routed over a Layer 2 or a Layer 3 channel is load balanced based on MAC addresses or IPv6 addresses, depending on the configuration. The MAC/IP and the src/dst/src-dst are supported, but load balancing that is based on Layer 4 ports is not supported. If you use the **port** keyword, the IPv6 addresses or either src, dst, or src-dst, is displayed.

Examples

Examples

The following example shows how to display the enabled protocol:

```
Router# show etherchannel protocol
Channel-group listing:
                -----------------------
Group: 12
----------
Protocol:  PAgP
Group: 24
----------
Protocol:   -  (Mode ON)
Router#
```

Examples

The following example shows how to display port channel information for a specific group:

```
Router# show etherchannel 12 port-channel
Group: 12
----------
               Port-channels in the group:
               ----------------------
Port-channel: Po1
------------
Age of the Port-channel   = 143h:01m:12s
Logical slot/port   = 14/1          Number of ports = 2
GC                  = -             HotStandBy port = null
```

```
Port state          = Port-channel Ag-Inuse
Protocol            = LACP
Fast-switchover     = enabled
Ports in the Port-channel:
Index   Load   Port    EC state
------+------+------+-----------
  0     55     Fa4/1   active
  1     AA     Fa4/2   active
Time since last port bundled:    16h:28m:58s    Fa4/1
Time since last port Un-bundled: 16h:29m:00s    Fa4/4
```

The following example shows that direct load swapping is enabled.

```
Router# show etherchannel 15 port-channel
               Port-channels in the group:
Port-channel: Po15    (Primary Aggregator)
Age of the Port-channel   = 0d:18h:16m:49s
Logical slot/port   = 14/7          Number of ports = 1
HotStandBy port = null
Port state              = Port-channel Ag-Inuse
Protocol                =   LACP
! The following line of output is added with support
of the LACP Single Fault Direct Load Swapping feature. !
Direct Load Swap = enabled
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+------+------+-----------------+-----------
  0     FF     Fa4/1    Active    8
Time since last port bundled:    0d:00h:06m:12s    Fa4/1
```

Examples

The following examples show how to display load-balancing information:

```
Router#
 show etherchannel load-balance
Source XOR Destination mac address
Router#
 show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        dst-mac
        mpls label-ip
EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Destination MAC address
  IPv4: Destination MAC address
  IPv6: Destination MAC address (routed packets)
        Destination IP address (bridged packets)
  MPLS: Label or IP
```

Examples

The following example shows how to display a summary of information for a specific group:

```
Router#
show etherchannel 1 brief
Group state = L3
Ports: 2   Maxports = 8
port-channels: 1 Max port-channels = 1
Partner's information:
```

The following example shows the hash distribution algorithm that was last applied:

```
Router# show etherchannel
 10 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
<snip>
```

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
10     Po10(RU)        LACP      Gi3/7(P)       Gi3/9(P)
! The following line of output is added with support
of the EtherChannel Load Distribution feature. !
Last applied Hash Distribution Algorithm: Fixed
Router#
```

Examples The following example shows how to display detailed information for a specific group:

```
Router#
show etherchannel 12 detail
Group state = L2
Ports: 1   Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol:   PAgP
Fast-switchover = enabled
                Ports in the group:
                -------------------
Port: Fa5/2
------------
Port state    = Down Not-in-Bndl
Channel group = 12          Mode = Desirable-Sl     Gcchange = 0
Port-channel  = null        GC   = 0x00000000          Pseudo port-channel = Po1
2
Port index    = 0           Load = 0x00        Protocol =   PAgP
Flags:  S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs
        A - Device is in active mode       P - Device is in passive mode
Local information:
                          LACP Port    Admin     Oper    Port     Port
Port      Flags   State     Priority      Key      Key     Number   State
Fa4/1     SA      bndl      32768         100      100     0xc1     0x75
Partner's information:
         Partner               Partner              Partner
Port     System ID             Port Number    Age    Flags
Fa4/1    8000,00b0.c23e.d861    0x81           14s    SP
         LACP Partner    Partner     Partner
         Port Priority   Oper Key    Port State
         32768            128         0x81
Age of the port in the current state: 16h:27m:42s
                Port-channels in the group:
                ----------------------
Port-channel: Po12
------------
Age of the Port-channel   = 04d:02h:52m:26s
Logical slot/port   = 14/1          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
Protocol            =   PAgP
```

Note When LACP 1:1 redundancy is configured, the **showetherchanneldetail** command also displays fast-switchover status information.

Examples The following example shows how to display a one-line summary per channel group:

```
Router#
show etherchannel summary
U-in use  I-in port-channel   S-suspended   D-down  i-stand-alone  d-default
Group Port-channel  Ports
----- ------------  ----------------------------------------------------------
1     Po1(U)        Fa5/4(I)  Fa5/5(I)
2     Po2(U)        Fa5/6(I)  Fa5/7(I)
```

```
255                 Fa5/9(i)
256                 Fa5/8(i)
```

Examples The following example shows how to display EtherChannel port information for all ports and all groups:

```
Router#
show etherchannel port
                Channel-group listing:
                ----------------------
Group: 1
----------
                Ports in the group:
                -------------------
Port: Fa5/4
------------
Port state    = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1           Mode = Desirable     Gcchange = 0
Port-channel  = null        GC   = 0x00000000    Psudo-agport = Po1
Port indx     = 0           Load = 0x00
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.
Local information:
                              Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Fa5/4     d     U1/S1           1s       0        128        Any      0

Age of the port in the current state: 02h:40m:35s
Port: Fa5/5
------------
Port state    = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1           Mode = Desirable     Gcchange = 0
Port-channel  = null        GC   = 0x00000000    Psudo-agport = Po1
Port indx     = 0           Load = 0x00
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.
```

Examples The following example shows how to display the information about the EtherChannel port for a specific group:

```
Router#
show etherchannel 1 port
                Channel-group listing:
                ----------------------
Group: 1
----------
                Ports in the group:
                -------------------
Port: Fa5/4
------------
Port state    = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1           Mode = Desirable     Gcchange = 0
Port-channel  = null        GC   = 0x00000000    Psudo-agport = Po1
Port index    = 0           Load = 0x00        Protocol =   LACP
Flags:  S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs
        A - Device is in active mode       P - Device is in passive mode
Local information:
                              LACP Port    Admin     Oper    Port     Port
Port      Flags   State     Priority      Key       Key     Number   State
Fa5/4     SA      bndl      32768         100       100     0xc1     0x75
Partner's information:
          Partner               Partner               Partner
Port      System ID             Port Number    Age    Flags
Fa5/4     8000,00b0.c23e.d861   0x81            14s    SP
```

```
         LACP Partner    Partner     Partner
         Port Priority   Oper Key    Port State
         32768            128         0x81
Age of the port in the current state: 04d:02h:57m:38s
```

Examples

The following example shows the **showetherchannelsummary** command output with a port in suspended state:

```
Router# show etherchannel 42 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
Number of channel-groups in use: 8
Number of aggregators:           8
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po42(SU)        LACP      Fa1/17(s)  Fa1/18(P)  Fa1/19(P)  Fa1/20(P)
```

The following example shows the **showetherchannelport-channel** command output with the status of Standalone Disable option:

```
Router# show etherchannel 42 port-channel
                Port-channels in the group:
                ----------------------
Port-channel: Po42    (Primary Aggregator)
------------
Age of the Port-channel   = 0d:21h:28m:22s
Logical slot/port   = 14/42          Number of ports = 3
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Fast-switchover     = disabled
Load share deferral = disabled
Standalone Disable  = enabled
Ports in the Port-channel:
Index   Load      Port          EC state       No of bits
------+------+------------+------------------+-----------
 2      49         Fa1/18             Active   3
 1      92         Fa1/19             Active   3
 3      24         Fa1/20             Active   2
Time since last port bundled:    0d:03h:37m:07s    Fa1/18
Time since last port Un-bundled: 0d:03h:34m:27s    Fa1/17
Last applied Hash Distribution Algorithm: Fixed
```

The following example shows the **showetherchanneldetail** command output with the status of Standalone Disable option:

```
Router# show etherchannel 42 detail

Group state = L2
Ports: 4   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
Minimum Links: 2
Standalone Disable: enabled
                Ports in the group:
                -------------------
Port: Fa1/17
------------
Port state    = Up Cnt-bndl Suspend Not-in-Bndl
Channel group = 42           Mode = Active      Gcchange = -
Port-channel  = null        GC   =   -         Pseudo port-channel = Po2
Port index    = 0           Load = 0x00        Protocol =   LACP
```

```
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Fa1/17    FP      susp      1             0x2       0x2     0x112       0x82
Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
Fa1/17    FP      susp      1             0x0       0x2      0x312       0x36
Age of the port in the current state: 0d:03h:44m:04s
Port: Fa1/18
------------
Port state    = Up Mstr In-Bndl
Channel group = 42           Mode = Active      Gcchange = -
Port-channel  = Po2          GC   =   -         Pseudo port-channel = Po2
Port index    = 2            Load = 0x49        Protocol =   LACP
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Fa1/18    SA      bndl      2             0x2       0x2     0x113       0x3D
Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
Fa1/18    SA      bndl      2             0x0       0x2      0x313       0x3D
Age of the port in the current state: 0d:03h:43m:24s
Port-channels in the group:
Port-channel: Po42    (Primary Aggregator)
Age of the Port-channel   = 0d:21h:34m:45s
Logical slot/port   = 14/42          Number of ports = 3
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Fast-switchover     = disabled
Load share deferral = disabled
Standalone Disable  = enabled
Ports in the Port-channel:
Index   Load      Port          EC state       No of bits
------+------+------------+------------------+-----------
 2      49         Fa1/18             Active   3
 1      92         Fa1/19             Active   3
 3      24         Fa1/20             Active   2
Time since last port bundled:    0d:03h:43m:30s    Fa1/18
Time since last port Un-bundled: 0d:03h:40m:50s    Fa1/17
Last applied Hash Distribution Algorithm: Fixed
```

Related Commands

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
channel-protocol	Sets the protocol that is used on an interface to manage channeling.
interface port-channel	Accesses or creates the IDB port channel.

show interfaces

To display statistics for all interfaces configured on the router or access server, use the **show interfaces** command in privileged EXEC mode.

Cisco 2500 Series, Cisco 2600 Series, Cisco 4700 Series, and Cisco 7000 Series

show interfaces [*type number*] [*first*] [*last*] **[accounting]**

Catalyst 6500 Series, Cisco 7200 Series and Cisco 7500 Series with a Packet over SONET Interface Processor

show interfaces [**type slot**/**port**] [**accounting**| **counters protocol status**| **crb**| **dampening**| **description**| **dot1ad**| **etherchannel** [**module number**]| **fair-queue**| **irb**| **mac-accounting**| **mpls-exp**| **precedence**| **random-detect**| **rate-limit**| **stats**| **summary**| **switching**| **utilization** {*type number*}]

Cisco 7500 Series with Ports on VIPs

show interfaces [*type slot*/*port-adapter*/*port*]

Cisco 7600 Series

show interfaces [*type number*| **null** *interface-number*| **vlan** *vlan-id*]

Channelized T3 Shared Port Adapters

show interfaces serial [*slot*/*subslot*/*port*/*t1-num* : *channel-group*]

Shared Port Adapters

show interfaces type [*slot*/*subslot*/*port* [/*sub-int*]]

Syntax Description

type	(Optional) Interface type. Allowed values for *type* can be **atm**, **async**, **auto-template**, **bvi**, **bri0**, **ctunnel**, **container**, **dialer**, **e1**, **esconPhy**, **ethernet**, **fastethernet**, **fcpa**, **fddi**, **filter**, **filtergroup**, **gigabitethernet**, **ge-wan**, **hssi**, **longreachethernet**, **loopback**, **mfr**, **multilink**, **module**,**null**, **posport-channel**, , **port-group**, **pos-channel**, **sbc**, **sdcc**, **serial**, **sysclock**, **t1**, **tengigabitethernet**, **token**, **tokenring**, **tunnel**, **vif**, **vmi**, **virtual-access**, **virtual-ppp**, **virtual-template**, **virtual-tokenring**. **voaBypassIn**, **voaBypassOut**, **voaFilterIn**, **voaFilterOut**, **voaIn**, **voaOut**. **Note** The type of interfaces available is based on the type of router used.
number	(Optional) Port number on the selected interface.

first last	(Optional) For Cisco 2500 series routers, ISDN Basic Rate Interfae (BRI) only. The *first* argument can be either 1 or 2. The *last* argument can only be 2, indicating B channels 1 and 2. D-channel information is obtained by using the command without the optional arguments.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
counters protocol status	(Optional) Displays the current status of the protocol counters enabled.
crb	(Optional) Displays interface routing or bridging information.
dampening	(Optional) Displays interface dampening information.
description	(Optional) Displays the interface description.
etherchannel [**module***number*]	(Optional) Displays interface Ether Channel information. • **module** --The **module** keyword limits the display to interfaces available on the module.
fair-queue	(Optional) Displays interface Weighted Fair Queueing (WFQ) information.
irb	(Optional) Displays interface routing or bridging information.
mac-accounting	(Optional) Displays interface MAC accounting information.
mpls-exp	(Optional) Displays interface Multiprotocol Label Switching (MPLS) experimental accounting information.
precedence	(Optional) Displays interface precedence accounting information.
random-detect	(Optional) Displays interface Weighted Random Early Detection (WRED) information.
rate-limit	(Optional) Displays interface rate-limit information.
stats	(Optional) Displays interface packets and octets, in and out, by using switching path.

summary	(Optional) Displays an interface summary.
switching	(Optional) Displays interface switching.
null *interface-number*	(Optional) Specifies the null interface, that is **0**.
slot	(Optional) Slot number. Refer to the appropriate hardware manual for slot information.
/ *port*	(Optional) Port number. Refer to the appropriate hardware manual for port information.
/ *port-adapter*	(Optional) Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.
slot / *subslot* / *port* / *t1-num* **:** *channel-group*	(Optional) Channelized T3 Shared Port Adapters Number of the chassis slot that contains the channelized T3 Shared Port Adapters (SPA) (for example, 5/0/0:23), where: • *slot* --(Optional) Chassis slot number. For SPA interface processors (SIPs), refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. • / *subslot*-- (Optional) Secondary slot number on a SIP where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information. • / *port* --(Optional) Port or interface number. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide. • / *t1-num*-- (Optional) T1 time slot in the T3 line. The value can be from 1 to 28. • **:** *channel-group*-- (Optional) Number 0-23 of the DS0 link on the T1 channel.

[*slot*/*subslot*/*port*/*sub-int*]]	(Optional) Shared Port Adapters Number of the chassis slot that contains the SPA interface (for example, 4/3/0), where: • *slot* --(Optional) Chassis slot number. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. • / *subslot*-- (Optional)Secondary slot number on a SIP where a SAP is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information. • / *port* --(Optional) Port or interface number. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topics in the platform-specific SPA software configuration guide. • / *sub-int* -- (Optional) Subinterface number (for those SPAs that support subinterface configuration).
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	This command was modified to include support for flow-based WRED .
12.0(4)T	This command was modified to include enhanced display information for dialer bound interfaces.
12.0(7)T	This command was modified to include **dialer** as an interface type and to reflect the default behavior.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(20)S2	This command was integrated into Cisco IOS Release 12.2(20)S2 and introduced a new address format and output for SPA interfaces on the Cisco 7304 router. The *subslot* argument was introduced.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3.
12.2(14)SX	This command was modified. Support for this command was added for the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2SX. The uplink dual-mode port information was updated.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
2.2(33)SXJ01	This command was integrated into Cisco IOS Release 12.2(33)SXJ01.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers, and the **tengigabitethernet** interface type was added. 10-Gigabit Ethernet interfaces were introduced with the release of the 1-Port 10-Gigabit Ethernet SPA.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB1	This command was updated to display operational status for Gigabit Ethernet interfaces that are configured as primary and backup interfaces (Cisco 7600 series routers).
12.2(31)SB	This command was integrated in Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command was modified. The default value of the command was modified on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(50)SY	This command was integrated in Cisco IOS Release 12.2(50)SY and the dot1ad keyword was added.
15.1(01)SY	This command was integrated in Cisco IOS Release 15.1(50)SY.

Usage Guidelines

Display Interpretation

The **show interfaces** command displays statistics for the network interfaces. The resulting output varies, depending on the network for which an interface has been configured. The resulting display on the Cisco 7200 series routers shows the interface processors in slot order. If you add interface processors after booting the system, they will appear at the end of the list, in the order in which they were inserted.

Information About Specific Interfaces

The *number* argument designates the module and port number. If you use the **show interfaces** command on the Cisco 7200 series routers without the *slot*/*port* arguments, information for all interface types will be shown. For example, if you type **show interfaces** you will receive information for all Ethernet, serial, Token Ring, and FDDI interfaces. Only by adding the type *slot*/*port* argument you can specify a particular interface.

Cisco 7600 Series Routers

Valid values for the *number* argument depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The port channels from 257 to 282 are internally allocated and are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

Statistics are collected on a per-VLAN basis for Layer 2-switched packets and Layer 3-switched packets. Statistics are available for both unicast and multicast traffic. The Layer 3-switched packet counts are available for both ingress and egress directions. The per-VLAN statistics are updated every 5 seconds.

In some cases, you might see a difference in the duplex mode that is displayed between the **show interfaces** command and the **show running-config**commands. In this case, the duplex mode that is displayed in the **show interfaces** command is the actual duplex mode that the interface is running. The **show interfaces** command shows the operating mode for an interface, and the **show running-config** command shows the configured mode for an interface.

If you do not enter any keywords, all counters for all modules are displayed.

Command Variations

You will use the **show interfaces** command frequently while configuring and monitoring devices. The various forms of the **show interfaces** commands are described in detail in the sections that follow.

Dialer Interfaces Configured for Binding

If you use the **show interfaces** command on dialer interfaces configured for binding, the display will report statistics on each physical interface bound to the dialer interface; see the following examples for more information.

Removed Interfaces

If you enter a **show interfaces** command for an interface type that has been removed from the router or access server, interface statistics will be displayed accompanied by the following text: “Hardware has been removed.”

Weighted Fair Queueing Information

If you use the **show interfaces** command on a router or access server for which interfaces are configured to use weighted fair queueing through the **fair-queue** interface command, additional information is displayed. This information consists of the current and high-water mark number of flows.

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, when a multilink PPP (MLP) interface is down/down, its default bandwidth rate is the sum of the serial interface bandwidths associated with the MLP interface.

In Cisco IOS Release 12.2(31)SB, the default bandwidth rate is 64 Kbps.

Examples

The following is sample output from the **show interfaces** command. Because your display will depend on the type and number of interface cards in your router or access server, only a portion of the display is shown.

Note If an asterisk (*) appears after the throttles counter value, it means that the interface was throttled at the time the command was run.

```
Router# show interfaces
Ethernet 0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
  Internet address is 10.108.28.8, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters 0:00:00
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 2000 bits/sec, 4 packets/sec
     1127576 packets input, 447251251 bytes, 0 no buffer
     Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5332142 packets output, 496316039 bytes, 0 underruns
     0 output errors, 432 collisions, 0 interface resets, 0 restarts
.
.
.
```

Examples

The following example shows partial sample output when custom output queueing is enabled:

```
Router# show interfaces
Last clearing of “show interface” counters 0:00:06
Input queue: 0/75/0 (size/max/drops); Total output drops: 21
Output queues: (queue #: size/max/drops)
     0: 14/20/14  1: 0/20/6  2: 0/20/0 3: 0/20/0 4: 0/20/0 5: 0/20/0
     6: 0/20/0 7: 0/20/0  8: 0/20/0  9: 0/20/0  10: 0/20/0
.
.
.
```

When custom queueing is enabled, the drops accounted for in the output queues result from bandwidth limitation for the associated traffic and lead to queue length overflow. Total output drops include drops on all custom queues and the system queue. Fields are described with the weighted fair queueing output in the table below.

Examples

For each interface on the router or access server configured to use weighted fair queueing, the **show interfaces** command displays the information beginning with *Inputqueue***:** in the following display:

```
Router# show interfaces
Ethernet 0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
  Internet address is 10.108.28.8, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of “show interface” counters 0:00:00
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
```

```
  Five minute output rate 2000 bits/sec, 4 packets/sec
     1127576 packets input, 447251251 bytes, 0 no buffer
     Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5332142 packets output, 496316039 bytes, 0 underruns
     0 output errors, 432 collisions, 0 interface resets, 0 restarts
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Output queue: 7/64/0 (size/threshold/drops)
         Conversations 2/9 (active/max active)
```

The table below describes the input queue and output queue fields shown in the preceding two displays.

Table 2: Weighted-Fair-Queueing Output Field Descriptions

Field	Description
Input Queue	
size	Current size of the input queue.
max	Maximum size of the queue.
drops	Number of messages discarded in this interval.
Total output drops	Total number of messages discarded in this session.
Output Queue	
size	Current size of the output queue.
threshold	Congestive-discard threshold. Number of messages in the queue after which new messages for high-bandwidth conversations are dropped.
drops	Number of dropped messages.
Conversations: active	Number of currently active conversations.
Conversations: max active	Maximum number of concurrent conversations allowed.

Examples

To display the number of packets of each protocol type that have been sent through all configured interfaces, use the **show interfaces accounting** command. When you use the **accounting** option, only the accounting statistics are displayed.

Note Except for protocols that are encapsulated inside other protocols, such as IP over X.25, the accounting option also shows the total bytes sent and received, including the MAC header. For example, it totals the size of the Ethernet packet or the size of a packet that includes High-Level Data Link Control (HDLC) encapsulation.

Per-packet accounting information is kept for the following protocols:

- AppleTalk
- Address Resolution Protocol (ARP) (for IP, Frame Relay, Switched Multimegabit Data Service (SMDS))
- Connectionless Network Service (CLNS)
- Digital Equipment Corporation (DEC) Maintenance Operations Protocol (MOP)

The routers use MOP packets to advertise their existence to Digital Equipment Corporation machines that use the MOP. A router periodically broadcasts MOP packets to identify itself as a MOP host. This results in MOP packets being counted, even when DECnet is not being actively used.

- DECnet
- HP Probe
- IP
- LAN Manager (LAN Network Manager and IBM Network Manager)
- Novell
- Serial Tunnel Synchronous Data Link Control (SDLC)
- Spanning Tree
- SR Bridge
- Transparent Bridge

Examples

The following is sample output from the **show interfaces** command when distributed WRED (DWRED) is enabled on an interface. Notice that the packet drop strategy is listed as "VIP-based weighted RED."

```
Router# show interfaces hssi 0/0/0
Hssi0/0/0 is up, line protocol is up
  Hardware is cyBus HSSI
  Description: 45Mbps to R1
Internet address is 10.200.14.250/30
MTU 4470 bytes, BW 45045 Kbit, DLY 200 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:02, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Packet Drop strategy: VIP-based weighted RED
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1976 packets input, 131263 bytes, 0 no buffer
Received 1577 broadcasts, 0 runts, 0 giants
0 parity
4 input errors, 4 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
1939 packets output, 130910 bytes, 0 underruns
0 output errors, 0 applique, 3 interface resets
0 output buffers copied, 0 interrupts, 0 failures
```

Examples

The following is sample output from the **show interfaces** command for serial interface 2 when Airline Control (ALC) Protocol is enabled:

```
Router# show interfaces serial 2
Serial2 is up, line protocol is up
Hardware is CD2430
MTU 1500 bytes, BW 115 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

```
Encapsulation ALC, loopback not set
Full-duplex enabled.
     ascus in UP state: 42, 46
     ascus in DOWN state:
     ascus DISABLED:
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 3 interface resets
0 output buffer failures, 0 output buffers swapped out
DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
```

Examples

The following is sample output from the **show interfaces** command for an SDLC primary interface supporting the SDLC function:

```
Router# show interfaces
Serial 0 is up, line protocol is up
 Hardware is MCI Serial
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation SDLC-PRIMARY, loopback not set
      Timers (msec): poll pause 100 fair poll 500. Poll limit 1
      [T1 3000, N1 12016, N2 20, K 7] timer: 56608 Last polled device: none
      SDLLC [ma: 0000.0C01.14--, ring: 7 bridge: 1, target ring: 10
             largest token ring frame 2052]
SDLC addr C1 state is CONNECT
       VS 6, VR 3, RCNT 0, Remote VR 6, Current retransmit count 0
       Hold queue: 0/12 IFRAMEs 77/22 RNRs 0/0 SNRMs 1/0 DISCs 0/0
       Poll: clear, Poll count: 0, chain: p: C1 n: C1
       SDLLC [largest SDLC frame: 265, XID: disabled]
  Last input 00:00:02, output 00:00:01, output hang never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 517 bits/sec, 30 packets/sec
  Five minute output rate 672 bits/sec, 20 packets/sec
       357 packets input, 28382 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       926 packets output, 77274 bytes, 0 underruns
       0 output errors, 0 collisions, 0 interface resets, 0 restarts
       2 carrier transitions
```

The table below shows the fields relevant to all SDLC connections.

Table 3: show interfaces Field Descriptions When SDLC Is Enabled

Field	Description
Timers (msec)	List of timers in milliseconds.
poll pause, fair poll, Poll limit	Current values of these timers.
T1, N1, N2, K	Current values for these variables.

The table below shows other data given for each SDLC secondary interface configured to be attached to this interface.

Table 4: SDLC Field Descriptions

Field	Description
addr	Address of this secondary interface.
State	Current state of this connection. The possible values follow: • BOTHBUSY--Both sides have told each other that they are temporarily unable to receive any more information frames. • CONNECT--A normal connect state exists between this router and this secondary. • DISCONNECT--No communication is being attempted to this secondary. • DISCSENT--This router has sent a disconnect request to this secondary and is awaiting its response. • ERROR--This router has detected an error, and is waiting for a response from the secondary acknowledging this. • SNRMSENT--This router has sent a connect request (SNRM) to this secondary and is awaiting its response. • THEMBUSY--This secondary has told this router that it is temporarily unable to receive any more information frames. • USBUSY--This router has told this secondary that it is temporarily unable to receive any more information frames.
VS	Sequence number of the next information frame this station sends.
VR	Sequence number of the next information frame from this secondary that this station expects to receive.
RCNT	Number of correctly sequenced I-frames received when the Cisco IOS software was in a state in which it is acceptable to receive I-frames.
Remote VR	Last frame transmitted by this station that has been acknowledged by the other station.
Current retransmit count	Number of times the current I-frame or sequence of I-frames has been retransmitted.

Field	Description
Hold queue	Number of frames in hold queue/Maximum size of hold queue.
IFRAMEs, RNRs, SNRMs, DISCs	Sent and received count for these frames.
Poll	"Set" if this router has a poll outstanding to the secondary; "clear" if it does not.
Poll count	Number of polls, in a row, given to this secondary at this time.
chain	Shows the previous (p) and next (n) secondary address on this interface in the round-robin loop of polled devices.

Examples

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

```
Router# show interfaces accounting
Interface TokenRing0 is disabled
Ethernet0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP     873171  735923409      34624    9644258
                  Novell     163849   12361626      57143    4272468
                 DEC MOP          0          0          1         77
                     ARP      69618    4177080       1529      91740
Interface Serial0 is disabled
Ethernet1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP          0          0         37      11845
                  Novell          0          0       4591     275460
                 DEC MOP          0          0          1         77
                     ARP          0          0          7        420
Interface Serial1 is disabled
Interface Ethernet2 is disabled
Interface Serial2 is disabled
Interface Ethernet3 is disabled
Interface Serial3 is disabled
Interface Ethernet4 is disabled
Interface Ethernet5 is disabled
Interface Ethernet6 is disabled
Interface Ethernet7 is disabled
Interface Ethernet8 is disabled
Interface Ethernet9 is disabled
Fddi0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                  Novell          0          0        183      11163
                     ARP          1         49          0          0
```

When the output indicates that an interface is " disabled," the router has received excessive errors (over 5000 in a keepalive period).

Examples

The following is sample output from the **show interfaces** command issued for the serial interface 1 for which flow-based WRED is enabled. The output shows that there are 8 active flow-based WRED flows, that the

maximum number of flows active at any time is 9, and that the maximum number of possible flows configured for the interface is 16:

```
Router# show interfaces serial 1
Serial1 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.1.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
Reliability 255/255, txload 237/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive not set
  Last input 00:00:22, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:17:58
  Input queue: 0/75/0 (size/max/drops); Total output drops: 2479
Queueing strategy: random early detection(RED)
    flows (active/max active/max): 8/9/16
    mean queue depth: 27
    drops: class  random   tail     min-th   max-th   mark-prob
           0      946      0        20       40       1/10
           1      488      0        22       40       1/10
           2      429      0        24       40       1/10
           3      341      0        26       40       1/10
           4      235      0        28       40       1/10
           5      40       0        31       40       1/10
           6      0        0        33       40       1/10
           7      0        0        35       40       1/10
           rsvp   0        0        37       40       1/10
  30 second input rate 1000 bits/sec, 2 packets/sec
  30 second output rate 119000 bits/sec, 126 packets/sec
     1346 packets input, 83808 bytes, 0 no buffer
     Received 12 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     84543 packets output, 9977642 bytes, 0 underruns
     0 output errors, 0 collisions, 6 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Examples

The following is sample output from the **show interfaces** command when distributed weighted fair queueing (DWFQ) is enabled on an interface. Notice that the queueing strategy is listed as "VIP-based fair queueing."

```
Router# show interfaces fastethernet 1/1/0
Fast Ethernet 1/1/0 is up, line protocol is up
  Hardware is cyBus Fast Ethernet Interface, address is 0007.f618.4448 (bia 00e0)
  Description: pkt input i/f for WRL tests (to pagent)
  Internet address is 10.0.2.70/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive not set, fdx, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 01:11:01, output hang never
  Last clearing of "show interface" counters 01:12:31
  Queueing strategy: VIP-based fair queueing
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     1 packets output, 60 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffers copied, 0 interrupts, 0 failures
```

Examples

When the **show interfaces** command is issued on an unbound dialer interface, the output looks as follows:

```
Router# show interfaces dialer 0
Dialer0 is up (spoofing), line protocol is up (spoofing)
  Hardware is Unknown
  Internet address is 10.1.1.2/8
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 3/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 1 seconds on reset
  Last input 00:00:34, output never, output hang never
  Last clearing of "show interface" counters 00:05:09
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 0 packets/sec
     18 packets input, 2579 bytes
     14 packets output, 5328 bytes
```

But when the **show interfaces** command is issued on a bound dialer interface, you will get an additional report that indicates the binding relationship. The output is shown here:

```
Router# show interfaces dialer 0
Dialer0 is up, line protocol is up
  Hardware is Unknown
  Internet address is 10.1.1.2/8
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 1 seconds on reset
  Interface is bound to BRI0:1
  Last input 00:00:38, output never, output hang never
  Last clearing of "show interface" counters 00:05:36
Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38 packets input, 4659 bytes
     34 packets output, 9952 bytes
Bound to:
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  Interface is bound to Dialer0 (Encapsulation PPP)
  LCP Open, multilink Open
  Last input 00:00:39, output 00:00:11, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     78 packets input, 9317 bytes, 0 no buffer
     Received 65 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     93 packets output, 9864 bytes, 0 underruns
     0 output errors, 0 collisions, 7 interface resets
     0 output buffer failures, 0 output buffers swapped out
     4 carrier transitions
```

At the end of the Dialer0 output, the **show interfaces** command is executed on each physical interface bound to it.

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

```
Router# show interfaces dialer 0 stats
Dialer0
  Switching path    Pkts In   Chars In   Pkts Out  Chars Out
       Processor          0          0          6       1694
```

```
        Route cache  2522229  610372530     720458  174343542
              Total  2522229  610372530     720464  174345236
```

Examples

In this example, the physical interface is the B1 channel of the BRI0 link. This example also illustrates that the output under the B channel keeps all hardware counts that are not displayed under any logical or virtual access interface. The line in the report that states “Interface is bound to Dialer0 (Encapsulation LAPB)” indicates that the B interface is bound to Dialer0 and the encapsulation running over this connection is Link Access Procedure, Balanced (LAPB), not PPP, which is the encapsulation configured on the D interface and inherited by the B channel.

```
Router# show interfaces bri0:1
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set

Interface is bound to Dialer0 (Encapsulation LAPB)
  LCP Open, multilink Open
  Last input 00:00:31, output 00:00:03, output hang never
  Last clearing of “show interface” counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
     110 packets input, 13994 bytes, 0 no buffer
     Received 91 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     135 packets output, 14175 bytes, 0 underruns
     0 output errors, 0 collisions, 12 interface resets
     0 output buffer failures, 0 output buffers swapped out
     8 carrier transitions
```

Any protocol configuration and states should be displayed from the Dialer0 interface.

Examples

The following is sample output from the **show interfaces fastethernet** command for the second interface (port 1) in a 4-Port 10/100 Fast Ethernet SPA located in the bottom subslot (1) of the Modular Service Cards (MSC) that is installed in slot 2 on a Cisco 7304 router:

```
Router# show interfaces fastethernet 2/1/1
FastEthernet2/1/1 is up, line protocol is up
  Hardware is SPA-4FE-7304, address is 00b0.64ff.5d80 (bia 00b0.64ff.5d80)
  Internet address is 192.168.50.1/24
  MTU 9216 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:22, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 320 bytes
     Received 1 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     8 packets output, 529 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
```

```
     2 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Examples

```
Router# show interfaces e4/0
Ethernet4/0 is up, line protocol is up
  Hardware is AmdP2, address is 000b.bf30.f470 (bia 000b.bf30.f470)
  Internet address is 10.1.1.9/24
  MTU 1500 bytes, BW 10000 Kbit, RxBW 5000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 254/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:03:36
  Input queue: 34/75/0/819 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 7138000 bits/sec, 14870 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     3109298 packets input, 186557880 bytes, 0 no buffer
     Received 217 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     22 packets output, 1320 bytes, 0 underruns
     11 output errors, 26 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

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

Table 5: show interfaces fastethernet Field Descriptions--Fast Ethernet SPA

Field	Description
Fast Ethernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, SPA-4FE-7304) and MAC address.
Description	Alphanumeric string identifying the interface. This appears only if the **description** interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface. The default is 1500 bytes for the 4-Port 10/100 Fast Ethernet SPA.
BW	Bandwidth of the interface in kilobits per second.

Field	Description
RxBW	Receiver bandwidth of the interface, in kilobits per second. This value is displayed only when an interface has asymmetric receiver and transmitter rates.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload, rxload	Load on the interface (in the transmit “tx” and receive “rx” directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
100Mb/s, 10Mb/s	Speed of the interface in megabits per second.
100BaseTX/FX	Media protocol standard.
ARP type:	Type of ARP assigned and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed. **Note** This field does not apply to SPA interfaces.

Field	Description
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: • Size--Number of packets in the input queue. • Max--Maximum size of the queue. • Drops--Number of packets dropped because of a full input queue. • Flushes--Number of packets dropped as part of selective packet discard (SPD). SPD implements a selective packet drop policy on the router's IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is first-in, first-out (FIFO).
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.

Field	Description
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is smaller than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is larger than 1536 bytes is considered a giant. **Note** For the 4-Port 10/100 Fast Ethernet SPA, the default is that a giant is any packet greater than 1536 bytes. However, if you modify the maximum transmission unit (MTU) for the interface, this counter increments when you exceed the specified MTU for the interface.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, cyclic redundancy check (CRC), frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.

Field	Description
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired. Expiration happens when receiving a packet with a length greater than 2048 bytes.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.

Field	Description
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission. **Note** This field does not apply to SPA interfaces.
output buffer failures, output buffers swapped out	These counters are not used by the 4-Port 10/100 Fast Ethernet SPA on the Cisco 7304 router.

Examples

The following is sample output from the **show interfaces gigabitethernet** command for the first interface (port 0) in a 2-Port 10/100/1000 Gigabit Ethernet SPA located in the top subslot (0) of the MSC that is installed in slot 4 on a Cisco 7304 router:

```
Router# show interfaces gigabitethernet 4/0/0

GigabitEthernet4/0/0 is up, line protocol is down
  Hardware is SPA-2GE-7304, address is 00b0.64ff.5a80 (bia 00b0.64ff.5a80)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 1000Mb/s, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
```

```
     0 watchdog, 0 multicast, 0 pause input
     109 packets output, 6540 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     1 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

Examples

The following examples show the additional lines included in the display when the command is issued on two Gigabit Ethernet interfaces that are configured as a primary interface (gi3/0/0) and as a backup interface (gi3/0/11) for the primary:

```
Router# show interfaces gigabitEthernet 3/0/0

GigabitEthernet3/0/0 is up, line protocol is up (connected)
  Hardware is GigEther SPA, address is 0005.dc57.8800 (bia 0005.dc57.8800)
  Backup interface GigabitEthernet3/0/11, failure delay 0 sec, secondary disable delay 0
sec,
  .
  .
  .
Router# show interfaces gigabitEthernet 3/0/11

GigabitEthernet3/0/11 is standby mode, line protocol is down (disabled)
  .
  .
  .
```

The table below describes the fields shown in the display for Gigabit Ethernet SPA interfaces.

Table 6: show interfaces gigabitethernet Field Descriptions--Gigabit Ethernet SPA

Field	Description
GigabitEthernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, SPA-2GE-7304) and MAC address.
Backup interface	Identifies the backup interface that exists for this, the primary interface.
Failure and secondary delay	The period of time (in seconds) to delay bringing up the backup interface when the primary goes down, and bringing down the backup after the primary becomes active again. On the Cisco 7600 router, the delay must be 0 (the default) to ensure that there is no delay between when the primary goes down and the backup comes up, and vice versa.
Standby mode	Indicates that this is a backup interface and that it is currently operating in standby mode.

Field	Description
Description	Alphanumeric string identifying the interface. This appears only if the **description** interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface. The default is 1500 bytes for the 2-Port 10/100/1000 Gigabit Ethernet SPA.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload, rxload	Load on the interface (in the transmit “tx” and receive “rx” directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
1000Mb/s, 100Mb/s, 10Mb/s	Speed of the interface in megabits per second.
link type	Specifies whether autonegotiation is being used on the link.
media type	Interface port media type: RJ45, SX, LX, or ZX.
100BaseTX/FX	Media protocol standard.
ARP type:	Type of ARP assigned and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.

Field	Description
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed. **Note** This field does not apply to SPA interfaces.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: • Size--Number of packets in the input queue. • Max--Maximum size of the queue. • Drops--Number of packets dropped because of a full input queue. • Flushes--Number of packets dropped as part of SPD. SPD implements a selective packet drop policy on the router's IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is FIFO.
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).

Field	Description
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is smaller than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is larger than 1536 bytes is considered a giant. **Note** For the 2-Port 10/100/1000 Gigabit Ethernet SPA, the default is that a giant is any packet greater than 1536 bytes. However, if you modify the MTU for the interface, this counter increments when you exceed the specified MTU for the interface.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.

Field	Description
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired. Expiration happens when receiving a packet with a length greater than 2048 bytes.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.

Field	Description
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission. **Note** This field does not apply to SPA interfaces.
output buffer failures, output buffers swapped out	These counters are not used by the 2-Port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router.

Examples

The following is sample output from the **show interfaces pos** command on a Cisco 7600 series router or Catalyst 6500 series switch for POS interface 4/3/0 (which is the interface for port 0 of the SPA in subslot 3 of the SIP in chassis slot 4):

```
Router# show interfaces pos 4/3/0
```

```
POS4/3/0 is up, line protocol is up  (APS working - active)
  Hardware is Packet over SONET
  Internet address is 10.0.0.1/8
  MTU 4470 bytes, BW 622000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Scramble disabled
  Last input 00:00:34, output 04:09:06, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
        Available Bandwidth 622000 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     782 packets input, 226563 bytes, 0 no buffer
     Received 0 broadcasts, 1 runts, 0 giants, 0 throttles
              0 parity
     1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     271 packets output, 28140 bytes, 0 underruns
     0 output errors, 0 applique, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     2 carrier transitions
```

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

Table 7: show interfaces pos Field Descriptions--POS SPA

Field	Description
POS4/3/0 is up, line protocol is up	Indicates whether the interface hardware is currently active and can transmit and receive or whether it has been taken down by an administrator.
Hardware is. . .	Hardware type: • For POSIP--cyBus Packet over SONET • For POS SPAs--Packet over SONET
Internet address is	Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.

Field	Description
Encapsulation	Encapsulation method assigned to the interface.
Loopback	Indicates whether loopbacks are set.
Keepalive	Indicates whether keepalives are set.
Scramble	Indicates whether SONET payload scrambling is enabled. SONET scrambling is disabled by default. For the POS SPAs on the Cisco 12000 series routers, scrambling is enabled by default.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2231 ms (and less than 232 ms) ago.
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).

Field	Description
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with number of packets ignored. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Not supported for POS interfaces.
parity	Report of the parity errors on the interface.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.

Field	Description
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
applique	Indicates an unrecoverable error has occurred on the POSIP applique. The system then invokes an interface reset.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.

Field	Description
output buffer failures	Not supported for POS interfaces.
output buffers swapped out	Not supported for POS interfaces.
carrier transitions	Number of times the carrier detect signal of the interface has changed state.

Examples

The following is sample output from the **show interfaces pos** command on a Cisco 12000 series router for POS interface 1/1/0 (which is the interface for port 0 of the SPA in subslot 1 of the SIP in chassis slot 1):

```
Router# show interfaces pos 1/1/0

POS1/1/0 is up, line protocol is up
  Hardware is Packet over SONET
  Internet address is 10.41.41.2/24
  MTU 4470 bytes, BW 9952000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive not set
  Scramble enabled
  Last input 00:00:59, output 00:00:11, output hang never
  Last clearing of "show interface" counters 00:00:14
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
        Available Bandwidth 9582482 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
              0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1 packets output, 314 bytes, 0 underruns
     0 output errors, 0 applique, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Examples

The following is sample output from the **show interfaces sdcc**command on a Cisco 12000 series router for POS interface 1/1/0 (which is the interface for port 0 of the SPA in subslot 1 of the SIP in chassis slot 1):

```
Router# show interfaces sdcc 1/1/0

SDCC1/1/0 is administratively down, line protocol is down
  Hardware is SDCC
  MTU 1500 bytes, BW 192 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:01:55
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

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

Table 8: show interfaces sdcc Field Descriptions--POS SPA

Field	Description
SDCC1/1/0 is administratively down, line protocol is down	Indicates whether the interface hardware is currently active and can transmit and receive or whether it has been taken down by an administrator.
Hardware is. . .	Hardware type is SDCC--Section Data Communications Channel.
Internet address is	Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to the interface.
crc	Cyclic redundancy check size (16 or 32 bits).
Loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.

Field	Description
(Last) output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2231 ms (and less than 232 ms) ago.
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with number of packets ignored. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.

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

Field	Description
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Not supported for POS interfaces.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
output buffer failures	Not supported for POS interfaces.
output buffers swapped out	Not supported for POS interfaces.
carrier transitions	Number of times the carrier detect signal of the interface has changed state.

Examples

The following example shows the interface serial statistics on the first port of a T3/E3 SPA installed in subslot 0 of the SIP located in chassis slot 5:

```
Router# show interfaces serial 5/0/0
Serial5/0/0 is up, line protocol is up
  Hardware is SPA-4T3E3
  Internet address is 10.1.1.2/24
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
     reliability 255/255, txload 234/255, rxload 234/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:05, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 40685000 bits/sec, 115624 packets/sec
  5 minute output rate 40685000 bits/sec, 115627 packets/sec
     4653081241 packets input, 204735493724 bytes, 0 no buffer
     Received 4044 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
```

```
          0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     4652915555 packets output, 204728203520 bytes, 0 underruns
     0 output errors, 0 applique, 4 interface resets
     0 output buffer failures, 0 output buffers swapped out
 2 carrier transitions
```

The table below describes the fields shown in the **show interfaces serial** output for a T3/E3 SPA.

Note The fields appearing in the ouput will vary depending on card type, interface configuration, and the status of the interface.

Table 9: show interfaces serial Field Descriptions--T3/E3 SPA

Field	Description
Serial	Name of the serial interface.
line protocol is	If the line protocol is up, the local router has received keepalive packets from the remote router. If the line protocol is down, the local router has not received keepalive packets form the remote router.
Hardware is	Designates the specific hardware type of the interface.
Internet address is	The IP address of the interface.
MTU	The maximum packet size set for the interface.
BW	Bandwidth in kilobits per second.
DLY	Interface delay in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload	Transmit load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
rxload	Receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method.
crc	CRC size in bits.
loopback	Indicates whether loopback is set.

Field	Description
keepalive	Indicates whether keepalives are set.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing of show interface counters	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 milliseconds (and less than 232 ms) ago.
Input queue	Packet statistics on the input queue reported as: • Size--Current size of the input queue. • Max--Maximum size of the input queue. • Drops--Packets dropped because the queue was full. • Flushes--Number of times that data on queue has been discarded.
Total output drops	Total number of dropped packets.

Field	Description
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue	Number of packets in the output queue (size), and the maximum size of the queue (max).
5-minute input rate	Average number of bits and packets received per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
5-minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.

Examples

The following is sample output from the **show interfaces tengigabitethernet** command for the only interface (port 0) in a 1-Port 10 Gigabit Ethernet SPA located in the top subslot (0) of the carrier card that is installed in slot 7 on a Cisco 12000 series router:

```
Router# show interfaces tengigabitethernet 7/0/0
TenGigabitEthernet7/0/0 is up, line protocol is up (connected)
  Hardware is TenGigEther SPA, address is 0000.0c00.0102 (bia 000f.342f.c340)
  Internet address is 10.1.1.2/24
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full-duplex, 10Gb/s
  input flow-control is on, output flow-control is on
ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:10, output hang never
```

```
Last clearing of "show interface" counters 20:24:30
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
   237450882 packets input, 15340005588 bytes, 0 no buffer
   Received 25 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 0 multicast, 0 pause input
   0 input packets with dribble condition detected
   1676 packets output, 198290 bytes, 0 underruns
   0 output errors, 0 collisions, 4 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 PAUSE output
   0 output buffer failures, 0 output buffers swapped out
```

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

Table 10: show interfaces tengigabitethernet Field Descriptions--10-Gigabit Ethernet SPA

Field	Description
TenGigabitEthernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type and MAC address.
Description	Alphanumeric string identifying the interface. This appears only if the **description** interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload, rxload	Load on the interface (in the transmit “tx” and receive “rx” directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.

Field	Description
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
10Gb/s	Speed of the interface in Gigabits per second.
input flow control ...	Specifies if input flow control is on or off.
ARP type:	Type of ARP assigned and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.

Field	Description
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: • Size--Number of packets in the input queue. • Max--Maximum size of the queue. • Drops--Number of packets dropped because of a full input queue. • Flushes--Number of packets dropped as part of SPD. SPD implements a selective packet drop policy on the router's IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is FIFO.
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
L2 Switched	Provides statistics about Layer 2 switched traffic, including unicast and multicast traffic.
L3 in Switched	Provides statistics about received Layer 3 traffic.
L3 out Switched	Provides statistics about sent Layer 3 traffic.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.

Field	Description
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired.
multicast	Number of multicast packets.

Field	Description
pause input	Number of pause packets received.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.

Field	Description
no carrier	Number of times the carrier was not present during the transmission.
pause output	Number of pause packets transmitted.
output buffer failures, output buffers swapped out	Number of output butters failures and output buffers swapped out.

Examples

This example shows how to display traffic for a specific interface:

```
Router# show interfaces GigabitEthernet1/1

GigabitEthernet0/1 is up, line protocol is up
  Hardware is BCM1125 Internal MAC, address is 0016.9de5.d9d1 (bia 0016.9de5.d9d1)
  Internet address is 172.16.165.40/27
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:11, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     10 packets input, 2537 bytes, 0 no buffer
     Received 10 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 46 multicast, 0 pause input
     0 input packets with dribble condition detected
     18 packets output, 3412 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     7 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     2 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Note The unknown protocol drops field displayed in the above example refers to the total number of packets dropped due to unknown or unsupported types of protocol. This field occurs on several platforms such as the Cisco 3725, 3745, 3825, and 7507 series routers.

This example shows how to display traffic for a FlexWAN module:

```
Router# show interfaces pos 6/1/0.1

POS6/1/0.1 is up, line protocol is up
  Hardware is Packet over Sonet
  Internet address is 10.1.2.2/24
  MTU 4470 bytes, BW 155000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY <<<+++ no packets info after this line
Arches#sh mod 6
Mod Ports Card Type                              Model             Serial No.
```

```
--- ----- ---------------------------------------- ------------------ -----------
  6    0  2 port adapter FlexWAN                    WS-X6182-2PA       SAD04340JY3
Mod MAC addresses                          Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  6  0001.6412.a234 to 0001.6412.a273   1.3   12.2(2004022 12.2(2004022 Ok
Mod Online Diag Status
--- -------------------
  6 Pass
Router#
```

Related Commands

Command	Description
fair-queue	Enables WFQ.
interface	Configures an interface type and enters interface configuration mode.
show controllers fastethernet	Displays Fast Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show controllers pos	Displays information about the POS controllers.
show controllers serial	Displays controller statistics.

show interfaces port-channel

To display the information about the Fast EtherChannel on Cisco 7000 series routers with the RSP7000 and RSP7000CI, Cisco 7200 series routers, and Cisco 7500 series routers, use the **showinterfacesport-channel** command in user EXEC or privileged EXEC mode.

show interfaces port-channel commandshow interfaces port-channel [*channel-number*]

Syntax Description

channel-number	(Optional) Port channel number. Range is from 1 to 4.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.1 CA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
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.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Examples

The following is sample output from the **showinterfacesport-channel** command:

Note By default the hardware type is set to Fast EtherChannel.The default MTU is set to 1500 bytes. The maximum MTU size that can be configured on the native Gigabit Ethernet ports on the Cisco 7200 series router is 9216. The range of configurable MTU value is from 1500 to 9216.

```
Router# show interfaces port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is FEChannel, address is 0000.0ca8.6220 (bia 0000.0000.0000)
  MTU 1500 bytes, BW 400000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive not set, fdx
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 4
        Member 0 : Fast Ethernet1/0/0
        Member 1 : Fast Ethernet1/1/0
```

```
       Member 2 : Fast Ethernet4/0/0
       Member 3 : Fast Ethernet4/1/0
  Last input 01:22:13, output never, output hang never
  Last clearing of “show interface” counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     223 packets input, 11462 bytes, 0 no buffer
     Received 1 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     192 packets output, 13232 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The following sample output from the **showinterfacesport-channel** shows Gigabit EtherChannel as hardware type and the MTU value as 9216:

```
Router# show interface port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is GEChannel
, address is 0001.c929.c41b (bia 0001.c929.c41b)
  MTU 9216 bytes
, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Unknown duplex, Unknown Speed, media type is unknown media type
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 1
        Member 0 : GigabitEthernet0/1 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:00:04, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     95 packets input, 34383 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     1 packets output, 77 bytes, 0 underruns
     2 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes significant fields shown in the display.

Table 11: show interfaces port-channel Field Descriptions

Field	Description
Port-channel1 is up, line protocol is up	Indicates if the interface hardware is currently active and can transmit and receive or if it has been taken down by an administrator.
Hardware is	Hardware type (Fast EtherChannel).
address is	Address being used by the interface.

Field	Description
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates if loopbacks are set.
keepalive	Indicates if keepalives are set.
fdx	Indicates the interface is operating in full-duplex mode.
ARA type	ARP type on the interface.
ARP timeout	Number of hours, minutes, and seconds an ARP cache entry will stay in the cache.
No. of active members in this channel: 4	Number of Fast Ethernet interfaces that are currently active (not down) and part of the Fast EtherChannel group.
Member 0: Fast Ethernet1/0/0	Specific Fast Ethernet interface that is part of the Fast EtherChannel group.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.

Field	Description
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms)) ago.
Queueing strategy	First-in, first-out queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.

Field	Description
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of ones bit on the interface.
watchdog	Number of times watchdog receive timer expired. It happens when receiving a packet with length greater than 2048.
multicast	Number of multicast packets received.

Field	Description
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, as some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
babbles	The transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble. The most common cause of late collisions is that your Ethernet cable segments are too long for the speed at which you are transmitting.
deferred	Deferred indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.

Field	Description
no carrier	Number of times the carrier was not present during the transmission.
output buffer failures	Number of times that a packet was not output from the output hold queue because of a shortage of MEMD shared memory.
output buffers swapped out	Number of packets stored in main memory when the output queue is full; swapping buffers to main memory prevents packets from being dropped when output is congested. The number is high when traffic is bursty.

Related Commands

Command	Description
interface multilink	Specifies a Fast EtherChannel and enters interface configuration mode.

show l2protocol-tunnel

To display the protocols that are tunneled on an interface or on all interfaces, use the **showl2protocol-tunnel** command.

show l2protocol-tunnel [**interface** *interface mod/port*| **summary**| **vlan** *vlan*]

Syntax Description

interface *interface-id*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **FastEthernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**
mod/port	Module and port number.
summary	(Optional) Displays a summary of a tunneled port.
vlan*vlan*	(Optional) Limits the display to interfaces on the specified VLAN. Valid values are from 1 to 4094.

Command Modes

EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The **showl2protocol-tunnelsummary** command output was changed to display the following information: • Global drop-threshold setting • Up status of a Layer 2-protocol interface tunnel
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was changed to add the optional **vlan***vlan* keyword and argument.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

After enabling Layer 2 protocol tunneling on an access or IEEE 802.1Q tunnel port by using the l2protocol-tunnel interface configuration command, you can configure some or all of these parameters:

- Protocol type to be tunneled
- Shutdown threshold
- Drop threshold

The **showl2protocol-tunnel** command displays only the ports that have protocol tunneling enabled.

The **showl2protocol-tunnelsummary** command displays the ports that have protocol tunneling enabled, regardless of whether the port is down or currently configured as a trunk.

Examples

The following example is an output from the show l2protocol-tunnel command:

```
Router# show l2protocol-tunnel
COS for Encapsulated Packets: 5
```

```
Drop Threshold for Encapsulated Packets: 0
```

Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter
Fa0/3	---	----	----	----	----	----
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	----	----	0	242500	
	lacp	----	----	24268	242640	
	udld	----	----	0	897960	
Fa0/4	---	----	----	----	----	----
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	1000	----	24249	242700	
	lacp	----	----	24256	242660	
	udld	----	----	0	1344820	
Gi0/3	cdp	----	----	134482	1344820	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	1000	----	0	242500	
	lacp	500	----	0	485320	
	udld	300	----	44899	448980	
Gi0/3	cdp	----	----	134482	1344820	

	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	----	1000	0	242700	
	lacp	----	----	0	485220	
	udld	300	----	44899	448980	

This example shows how to display a summary of Layer 2-protocol tunnel ports:

```
Router# show l2protocol-tunnel summary
COS for Encapsulated Packets:5
Drop Threshold for Encapsulated Packets:0
Port    Protocol    Shutdown         Drop             Status
                    Threshold        Threshold
                    (cdp/stp/vtp)    (cdp/stp/vtp)
------- ----------- ---------------- ---------------- ----------
Fa9/1   --- stp --- ----/----/----   ----/----/----   down
Fa9/9   cdp stp vtp ----/----/----   ----/----/----   up
Fa9/47  --- --- --- ----/----/----   1500/1500/1500   down(trunk)
Fa9/48  cdp stp vtp ----/----/----   ----/----/----   down(trunk)
```

This example shows how to display Layer 2-protocol tunnel information on interfaces for a specific VLAN:

```
Router# show l2protocol-tunnel vlan 1
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0
Protocol Drop Counter
-------- -------------
 cdp                0
 lldp               0
 stp                0
 vtp                0
Port               Protocol Thresholds          Counters
                            Shutdown  Drop      Encap     Decap     Drop
------------------ -------- --------- --------- --------- --------- ---------
```

Related Commands

Command	Description
debug l2protocol-tunnel	Displays the debugging options for L2PT.
l2protocol-tunnel	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
l2protocol-tunnel drop-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface before being dropped.
l2protocol-tunnel global drop-threshold	Enables rate limiting at the software level.

Command	Description
l2protocol-tunnel shutdown-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface in 1 second.

show lacp

To display Link Aggregation Control Protocol (LACP) and multi-chassis LACP (mLACP) information, use the **show lacp** command in either user EXEC or privileged EXEC mode.

show lacp {*channel-group-number* {**counters**| **internal [detail]**| **neighbor [detail]**}| **multi-chassis [load-balance]** {**group** *number*| **port-channel** *number*}| **sys-id**}

Cisco ASR 901 Series Aggregation Services Router

show lacp {*channel-group-number* {**counters**| **internal [detail]**| **neighbor [detail]**| **sys-id**}}

Syntax Description

channel-group- number	(Optional) Number of the channel group. The following are valid values: • Cisco IOS 12.2 SB and Cisco IOS XE 2.4 Releases--from 1 to 64 • Cisco IOS 12.2 SR Releases--from 1 to 308 • Cisco IOS 12.2 SX Releases--from 1 to 496 • Cisco IOS 15.1S Releases—from 1 to 564 • Cisco ASR 901 Series Aggregation Services Router—from 1 to 8
counters	Displays information about the LACP traffic statistics.
internal	Displays LACP internal information.
neighbor	Displays information about the LACP neighbor.
detail	(Optional) Displays detailed internal information when used with the **internal** keyword and detailed LACP neighbor information when used with the **neighbor** keyword.
multi-chassis	Displays information about mLACP.
load-balance	Displays mLACP load balance information.
group	Displays mLACP redundancy group information,

number	Integer value used with the **group** and **port-channel** keywords. • Values from 1 to 4294967295 identify the redundancy group. • Values from 1 to 564 identify the port-channel interface.
port-channel	Displays mLACP port-channel information.
sys-id	Displays the LACP system identification. It is a combination of the port priority and the MAC address of the device

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
12.2(33)SRE	This command was modified. The **multi-chassis**, **group**, and **port-channel**keywords and *number* argument were added.
15.1(3)S	This command was modified. The **load-balance** keyword was added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Use the **show lacp** command to troubleshoot problems related to LACP in a network.

If you do not specify a value for the argument *channel-group-number*, all channel groups are displayed. Values in the range of 257 to 282 are supported on the CSM and the FWSM only.

Examples

Examples

This example shows how to display the LACP system identification using the **show lacp sys-id**command:

```
Device> show lacp sys-id

8000,AC-12-34-56-78-90
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address that is associated to the system.

Examples

This example shows how to display the LACP statistics for a specific channel group:

```
Device# show lacp 1 counters

              LACPDUs         Marker       LACPDUs
Port       Sent   Recv     Sent   Recv     Pkts Err
---------------------------------------------------
Channel group: 1
  Fa4/1    8      15       0      0         3    0
  Fa4/2    14     18       0      0         3    0
  Fa4/3    14     18       0      0         0
  Fa4/4    13     18       0      0         0
```

The output displays the following information:

- The LACPDUs Sent and Recv columns display the LACPDUs that are sent and received on each specific interface.
- The LACPDUs Pkts and Err columns display the marker-protocol packets.

The following example shows output from a **show lacp***channel-group-number***counters**command:

```
Device1# show lacp 5 counters

             LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
-------------------------------------------------------------------
Channel group: 5
Gi5/0/0     21     18       0      0        0      0         0
```

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

Table 12: show lacp channel-group-number counters Field Descriptions

Field	Description
LACPDUs Sent Recv	Number of LACP PDUs sent and received.
Marker Sent Recv	Attempts to avoid data loss when a member link is removed from an LACP bundle.
Marker Response Sent Recv	Cisco IOS response to the Marker protocol.
LACPDUs Pkts Err	Number of LACP PDU packets transmitted and the number of packet errors.

The following example shows output from a **show lacp internal**command:

```
Device1# show lacp 5 internal

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
Channel group 5
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Gi5/0/0   SA      bndl      32768         0x5       0x5     0x42        0x3D
```

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

Table 13: show lacp internal Field Descriptions

Field	Description
Flags	Meanings of each flag value, which indicates a device activity.
Port	Port on which link bundling is configured.
Flags	Indicators of device activity.
State	Activity state of the port. States can be any of the following: • Bndl--Port is attached to an aggregator and bundled with other ports. • Susp--Port is in suspended state, so it is not attached to any aggregator. • Indep--Port is in independent state (not bundled but able to switch data traffic). This condition differs from the previous state because in this case LACP is not running on the partner port. • Hot-sby--Port is in hot standby state. • Down--Port is down.
LACP port Priority	Priority assigned to the port.
Admin Key	Defines the ability of a port to aggregate with other ports.
Oper Key	Determines the aggregation capability of the link.
Port Number	Number of the port.

Field	Description
Port State	State variables for the port that are encoded as individual bits within a single octet with the following meaning: • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired

Examples

This example shows how to display internal information for the interfaces that belong to a specific channel:

```
Device# show lacp 1 internal

Flags:  S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
        A - Device is in Active mode.       P - Device is in Passive mode.
Channel group 1
                            LACPDUs     LACP Port    Admin   Oper    Port     Port
Port      Flags    State    Interval    Priority     Key     Key     Number   State
Fa4/1     saC      bndl     30s         32768        100     100     0xc1     0x75
Fa4/2     saC      bndl     30s         32768        100     100     0xc2     0x75
Fa4/3     saC      bndl     30s         32768        100     100     0xc3     0x75
Fa4/4     saC      bndl     30s         32768        100     100     0xc4     0x75
Device#
```

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

Table 14: show lacp internal Field Descriptions

Field	Description
State	Current state of the port; allowed values are as follows: • bndl--Port is attached to an aggregator and bundled with other ports. • susp--Port is in a suspended state; it is not attached to any aggregator. • indep--Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port). • hot-sby--Port is in a hot-standby state. • down--Port is down.
LACPDUs Interval	Interval setting.
LACP Port Priority	Port-priority setting.
Admin Key	Defines the ability of a port to aggregate with other ports.
Oper Key	Determines the aggregation capability of the link.
Port Number	Port number.
Port State	Activity state of the port. • See the Port State description in the show lacp internal Field Descriptions table for state variables.

Examples

This example shows how to display the information about the LACP neighbors for a specific port channel:

```
Device# show lacp 1 neighbors

Flags:  S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
        A - Device is in Active mode.       P - Device is in Passive mode.
Channel group 1 neighbors
          Partner                 Partner
Port      System ID               Port Number     Age     Flags
Fa4/1     8000,00b0.c23e.d84e     0x81            29s     P
Fa4/2     8000,00b0.c23e.d84e     0x82            0s      P
Fa4/3     8000,00b0.c23e.d84e     0x83            0s      P
Fa4/4     8000,00b0.c23e.d84e     0x84            0s      P
          Port          Admin     Oper      Port
          Priority      Key       Key       State
Fa4/1     32768         200       200       0x81
```

```
Fa4/2      32768          200        200        0x81
Fa4/3      32768          200        200        0x81
Fa4/4      32768          200        200        0x81
Device#
```

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

Table 15: show lacp neighbors Field Descriptions

Field	Description
Port	Port on which link bundling is configured.
Partner System ID	Peer's LACP system identification (sys-id). It is a combination of the system priority and the MAC address of the peer device.
Partner Port Number	Port number on the peer device
Age	Number of seconds since the last LACP PDU was received on the port.
Flags	Indicators of device activity.
Port Priority	Port priority setting.
Admin Key	Defines the ability of a port to aggregate with other ports.
Oper Key	Determines the aggregation capability of the link.
Port State	Activity state of the port. See the Port State description in the show lacp internal Field Descriptions table for state variables.

If no PDUs have been received, the default administrative information is displayed in braces.

Related Commands

Command	Description
clear lacp counters	Clears the statistics for all interfaces belonging to a specific channel group.
lacp port-priority	Sets the priority for the physical interfaces.
lacp system-priority	Sets the priority of the system.

show link state group

To display the link-state group information., use the **showlinkstategroup** command in user EXEC or privileged EXEC mode .

show link state group detail

Syntax Description

detail	Displays the detailed information about the group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

Link State Ttracking (LST), also known as trunk failover, is a feature that binds the link state of multiple interfaces. When you configure LST for the first time, add upstream interfaces to the link state group before adding the downstream interface, otherwise the downstream interfaces would move into error-disable mode. The maximum number of link state groups configurable is 10.

Examples

The following example displays the link-state group information:

```
Router# enable
Router# show link state group 1
Link State Group: 1 Status: Enabled, Down
Router> show link state group detail
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi3/5(Dwn) Gi3/6(Dwn)
Downstream Interfaces : Gi3/1(Dis) Gi3/2(Dis) Gi3/3(Dis) Gi3/4(Dis)
Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi3/15(Dwn) Gi3/16(Dwn) Gi3/17(Dwn)
Downstream Interfaces : Gi3/11(Dis) Gi3/12(Dis) Gi3/13(Dis) Gi3/14(Dis)
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

Related Commands

Command	Description
link state track	Configures the link state tracking number.
link state group	Configures the link state group and interface, as either an upstream or downstream interface in the group.

show mac-address-table dynamic

To display dynamic MAC address table entries only, use the **showmac-address-tabledynamic** command in privileged EXEC mode.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

show mac-address-table dynamic [**address** *mac-addr*| **interface** *interface type slot/number* | **vlan** *vlan*]

Catalyst Switches

show mac-address-table dynamic [**address** *mac-addr*| **detail**| **interface** *interface number***protocol** *protocol* | **module** *number*| **vlan** *vlan*][**begin**| **exclude**| **include**| *expression*]

Catalyst 6500 Series Switches

show mac-address-table dynamic [**address** *mac-addr*| **interface** *interface interface-number* [**all**| **module** *number*]| **module** *num*| **vlan** *vlan-id* [**all**| **module** *number*]]

Syntax Description

address *mac -address*	(Optional) Specifies a 48-bit MAC address; valid format is H.H.H.
detail	(Optional) Specifies a detailed display of MAC address table information.
interface *type number*	(Optional) Specifies an interface to match; valid type values are FastEthernet and GigabitEthernet, valid number values are from 1 to 9.
interface *type*	(Optional) Specifies an interface to match; valid type values are FastEthernet and GigabitEthernet.
slot	(Optional) Adds dynamic addresses to module in slot 1 or 2.
port	(Optional) Port interface number ranges based on type of Ethernet switch network module used: • 0 to 15 for NM-16ESW • 0 to 35 for NM-36ESW • 0 to 1 for GigabitEthernet
protocol *protocol*	(Optional) Specifies a protocol. See the “Usage Guidelines” section for keyword definitions.
module *number*	(Optional) Displays information about the MAC address table for a specific Distributed Forwarding Card (DFC) module.

vlan *vlan*	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 1005.
begin	(Optional) Specifies that the output display begin with the line that matches the expression.
exclude	(Optional) Specifies that the output display exclude lines that match the expression.
include	(Optional) Specifies that the output display include lines that match the specified expression.
expression	Expression in the output to use as a reference point.
all	(Optional) Specifies that the output display all dynamic MAC-address table entries.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XE	This command was introduced on Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(33)SXH	This command was changed to support the **all** keyword on the Catalyst 6500 series switch.

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The **showmac-address-tabledynamic** command output for an EtherChannel interface changes the port-number designation (for example, 5/7) to a port-group number.

Catalyst Switches

The keyword definitions for the protocol argument are:

- **ip** --Specifies IP protocol
- **ipx** --Specifies Internetwork Packet Exchange (IPX) protocols
- **assigned** --Specifies assigned protocol entries
- **other** --Specifies other protocol entries

The **showmac-address-tabledynamic** command output for an EtherChannel interface changes the port-number designation (for example, 5/7) to a port-group number.

Catalyst 6500 Series Switches

The *mac-address*is a 48-bit MAC address and the valid format is H.H.H.

The optional **module***num* keyword and argument are supported only on DFC modules. The **module***num*keyword and argument designate the module number.

Examples

The following examples show how to display all dynamic MAC address entries. The fields shown in the various displays are self-explanatory.

Examples

```
Router# show mac-address-table dynamic

Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
000a.000a.000a          Dynamic       1     FastEthernet4/0
002a.2021.4567          Dynamic       2     FastEthernet4/0
```

Examples

```
Router# show mac-address-table dynamic
vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0010.0d40.37ff  dynamic        ip  --  5/8
   1  0060.704c.73ff  dynamic        ip  --  5/9
4095  0000.0000.0000  dynamic        ip  --  15/1
   1  0060.704c.73fb  dynamic     other  --  5/9
   1  0080.1c93.8040  dynamic        ip  --  5/9
4092  0050.f0ac.3058  dynamic        ip  --  15/1
   1  00e0.4fac.b3ff  dynamic     other  --  5/9
```

The following example shows how to display dynamic MAC address entries with a specific protocol type (in this case, assigned).

```
Router# show mac-address-table dynamic protocol assigned
vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
4092  0000.0000.0000  dynamic  assigned  --  Router
4092  0050.f0ac.3059  dynamic  assigned  --  Router
   1  0010.7b3b.0978  dynamic  assigned  --  Fa5/9
Router#
```

The following example shows the detailed output for the previous example.

```
Router# show mac-address-table dynamic protocol assigned detail
MAC Table shown in details
=======================================
 Type   Always Learn Trap Modified Notify Capture Protocol Flood
-------+------------+----+--------+------+-------+--------+-----+
     QoS bit      L3 Spare   Mac Address  Age Byte Pvlan Xtag SWbits Index
-----------------+--------+-------------+--------+-----+----+------+-----
DYNAMIC     NO        NO     YES     NO     NO    assigned   NO
   Bit Not On        0     0000.0000.0000  255      4092   0     0     0x3
```

```
DYNAMIC     NO         NO      YES     NO     NO    assigned   NO
   Bit Not On         0      0050.f0ac.3059  254      4092   0      0      0x3

DYNAMIC     NO         NO      YES     NO     NO    assigned   NO
   Bit Not On         0      0010.7b3b.0978  254      1      0      0      0x108

Router#
```

Examples

This example shows how to display all the dynamic MAC-address entries for a specific VLAN.

```
Router# show mac-address-table dynamic vlan 200 all
Legend: * - primary entry
        age - seconds since last seen
        n/a - not aevailable
vlan     mac address      type   learn    age               ports
------+---------------+--------+-----+----------+--------------------------
 200  0010.0d40.37ff   dynamic    NO      23        Gi5/8
Router#
```

This example shows how to display all the dynamic MAC-address entries.

```
Router# show mac-address-table dynamic
Legend: * - primary entry
age - seconds since last seen
n/a - not applicable
vlan     mac address      type   learn    age               ports
------+---------------+--------+-----+----------+--------------------------
* 10   0010.0000.0000   dynamic  Yes   n/a        Gi4/1
* 3    0010.0000.0000   dynamic  Yes   0          Gi4/2
* 1    0002.fcbc.ac64   dynamic  Yes   265        Gi8/1
* 1    0009.12e9.adc0   static   No    -          Router
Router#
```

Related Commands

Command	Description
show mac -address-tableaddress	Displays MAC address table information for a specific MAC address.
show mac -address-tableaging-time	Displays the MAC address aging time.
show mac -address-tablecount	Displays the number of entries currently in the MAC address table.
show mac -address-tabledetail	Displays detailed MAC address table information.
show mac -address-tableinterface	Displays the MAC address table information for a specific interface.
show mac -address-tablemulticast	Displays multicast MAC address table information.
show mac -address-tableprotocol	Displays MAC address table information based on protocol.
show mac -address-tablestatic	Displays static MAC address table entries only.
show mac -address-tablevlan	Displays the MAC address table information for a specific VLAN.

show pagp

To display port-channel information, use the **show pagp** command in user EXEC or privileged EXEC mode.

show pagp [*group-number*] {**counters**| **internal**| **neighbor**| **pgroup**}

Syntax Description

group-number	(Optional) Channel-group number; valid values are a maximum of 64 values from 1 to 282.
counters	Displays the traffic information.
internal	Displays the internal information.
neighbor	Displays the neighbor information.
pgroup	Displays the active port channels.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can enter any **show pagp** command to display the active port-channel information. To display the nonactive information, enter the **show pagp** command with a group.

The **port-channel** *number*values from 257 to 282 are supported on the CSM and the FWSM only.

Examples

This example shows how to display information about the PAgP counters:

```
Router#
show pagp
 counters
          Information        Flush
Port      Sent   Recv     Sent   Recv
```

```
---------------------------------------
Channel group: 1
  Fa5/4    2660   2452     0      0
  Fa5/5    2676   2453     0      0
Channel group: 2
  Fa5/6    289    261      0      0
  Fa5/7    290    261      0      0
Channel group: 1023
  Fa5/9    0      0        0      0
Channel group: 1024
  Fa5/8    0      0        0      0
Router#
```

This example shows how to display internal PAgP information:

```
Router# show pagp
 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.
Channel group 1
                             Hello    Partner  PAgP     Learning
Port      Flags State   Timers  Interval Count   Priority  Method
Fa5/4     SC    U6/S7           30s      1        128      Any
Fa5/5     SC    U6/S7           30s      1        128      Any
Router#
```

This example shows how to display PAgP-neighbor information for all neighbors:

```
Router# show pagp
 neighbor
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
Channel group 1 neighbors
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Fa5/4     JAB031301            0050.0f10.230c   2/45         2s SAC     2D
Fa5/5     JAB031301            0050.0f10.230c   2/46        27s SAC     2D
Channel group 2 neighbors
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Fa5/6     JAB031301            0050.0f10.230c   2/47        10s SAC     2F
Fa5/7     JAB031301            0050.0f10.230c   2/48        11s SAC     2F
Channel group 1023 neighbors
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Channel group 1024 neighbors
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Router#
```

Related Commands

Command	Description
pagp learn-method	Learns the input interface of the incoming packets.
pagp port-priority	Selects a port in hot standby mode.

show power inline

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

show power inline [*interface-type slot*/*port*] [**actual**| **configured**]

Syntax Description

interface -type	(Optional) Type of interface.
slot	(Optional) Slot number.
/ *port*	(Optional) Port number.
actual	(Optional) Displays the present power status, which might not be the same as the configured power.
configured	(Optional) Displays the configured power status.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XU	This command was introduced.
12.2(2)XT	This command was introduced on the Cisco 2600 series, the Cisco 3600 series, and the Cisco 3700 series routers to support switchport creation.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation on Cisco 2600 series, the Cisco 3600 series, and Cisco 3700 series routers.
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.
Cisco IOS XE 3.9S	This command was integrated into Cisco IOS Release XE 3.9S.

Usage Guidelines

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

Use the **show power inline** *gigabitEthernet* **detail** command on a Cisco 4400 Series Integrated Services Router (ISR) to monitor the total available power budget on your router.

Examples

The following is sample output from the **show power inlinefa0/4actual** command asking for the actual status of each interface rather than what is configured for each:

```
Router#
show power inline fastethernet 0/4 actual
Interface            Power
-------------------- -----
FastEthernet0/4      no
```

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

Examples

The following are sample outputs from the **show power inline** command and the **show power inline** *gigabitEthernet* **detail** commands

```
 Router# show power inline

Available:31.0(w)  Used:30.8(w)  Remaining:0.2(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/0/0   auto   on         15.4    Ieee PD             4     30.0
Gi0/0/1   auto   on         15.4    Ieee PD             4     30.0


Router# show power inline gigabitEthernet 0/0/0 detail
Interface: Gi0/0/0
 Inline Power Mode: auto
 Operational status: on
 Device Detected: yes
 Device Type: Ieee PD
 IEEE Class: 4
 Discovery mechanism used/configured: Ieee
 Police: off

 Power Allocated
 Admin Value: 30.0
 Power drawn from the source: 15.4
 Power available to the device: 15.4

 Absent Counter: 0
 Over Current Counter: 0
 Short Current Counter: 0
 Invalid Signature Counter: 0
 Power Denied Counter: 0
```

Related Commands

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

snmp trap illegal-address

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

snmp trap illegal-address

no snmp trap illegal-address

Syntax Description

This command has no arguments or keywords.

Command Default

No SNMP trap is issued.

Command Modes

Hub configuration

Command History

Release	Modification
11.1	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.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

speed

To configure the speed for a Fast Ethernet or Gigabit Ethernet interface, use the **speed** command in interface configuration mode. To return to the default configuration, use the **no** form of this command.

speed {**10** | **100** | **1000** [**negotiate**] | **auto** [*speed-list*]}

no speed

Syntax Description

10	Configures the interface to transmit at 10 Mbps.
100	Configures the interface to transmit at 100 Mbps.
1000	Configures the interface to transmit at 1000 Mbps. This keyword is valid only for interfaces that support Gigabit Ethernet.
auto	Enables Fast Ethernet autonegotiation. The interface automatically operates at 10 Mbps or 100 Mbps depending on environmental factors, such as the type of media and transmission speeds for the peer routers, hubs, and switches used in the network configuration. Autonegotiation is the default.
negotiate	(Optional) Enables or disables the link-negotiation protocol on Gigabit Ethernet ports.
speed-list	(Optional) Speed autonegotiation capability for a specific speed; see the "Usage Guidelines" section for valid values.

Command Default

Autonegotiation is enabled. The command is set to **auto**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2(10)P	This command was introduced.
12.1(7)E	This command was modified. The **1000** keyword was added for Gigabit Ethernet interfaces.
12.2S	This command was integrated into Cisco IOS Release 12.2 S.

Release	Modification
12.2(20)S2	This command was implemented on the 4-port 10/100 Fast Ethernet SPA and the 2-port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17a)SX	This command was modified. The *speed-list* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

Use the **speed** {**10** | **100**} command for 10/100 ports, the **speed auto 10 100 1000** command for 10/100/1000 ports, and the **speed 1000** [**negotiate**] command for Gigabit Ethernet ports.

Cisco Cloud Services Router 1000V Series

Cisco Cloud Services Router 1000V Series does not support the **speed** command.

Cisco 7600 Series Routers

Cisco 7600 Series Routers cannot automatically negotiate interface speed and duplex mode if either of the connecting interfaces is configured to a value other than **auto**.

Ethernet Interfaces

If you set the Ethernet interface speed to **auto** on a 10/100-Mbps or 10/100/1000-Mbps Ethernet interface, both duplex operation and speed are autonegotiated.

Gigabit Ethernet Interfaces

The Gigabit Ethernet interfaces are full duplex only. You cannot change the duplex mode on Gigabit Ethernet interfaces or on a 10/100/1000-Mbps interface that is configured for Gigabit Ethernet.

SPA Interfaces

The **speed** command applies to Shared Port Adapter (SPA) interfaces that use RJ-45 media. Gigabit Ethernet interfaces using fiber media support 1000-Mbps speed only and use the **negotiation** command to enable and disable autonegotiation.

See also “Flow Control” in the “Usage Guidelines” section.

Speed Command Syntax Combinations

The table below lists the supported command options by interface.

Table 16: Supported speed Command Options

Interface Type	Supported Syntax	Default Settings	Usage Guidelines
10/100-Mbps module	**speed** {**10** | **100**} **speed auto 10 100**	**auto**	If the speed is set to **auto**, you cannot set **duplex**. If the speed is set to **10** or **100**, without configuring the duplex setting, the duplex is set to **half** by default.
10/100/1000-Mbps interface	**speed auto 10 100 1000**	**auto**	If the speed is set to **auto**, you cannot set **duplex**. If the speed is set to **10** or **100**, without configuring the duplex setting, the duplex is set to **half** by default. If the speed is set to **10** or **100**, the interface is not forced to half duplex by default.
100-Mbps fiber modules	Factory set	Not applicable.	
Gigabit Ethernet module	**speed 1000** [**negotiate**]	Speed is 1000 or negotiation is enabled.	Speed, duplex, flow control, and clocking negotiations are enabled.
10-Mbps ports	Factory set	Not applicable.	

Autonegotiation

To enable the autonegotiation capability on an RJ-45 interface, you must set either the **speed** command or the **duplex** command to **auto**. The default configuration is that both commands are set to **auto**.

If you need to force an interface port to operate with certain settings and, therefore, disable autonegotiation, you must be sure that the remote link is configured for compatible link settings for proper transmission including support of flow control on the link.

When you enable link negotiation, the speed, duplex, flow control, and clocking negotiations between two Gigabit Ethernet ports are automatically enabled.

Flow Control

Flow control support is always advertised when autonegotiation is enabled.

Every interface on a 4-port 10/100 Fast Ethernet SPA supports transmission of pause frames to stop packet flow when the Modular Services Card (MSC) is full. You cannot disable flow control for an interface on the 4-port 10/100 Fast Ethernet SPA. Therefore, flow control support is not configurable, but it is advertised during autonegotiation.

If you disable autonegotiation, then you must be sure that the remote device is configured to support flow control because flow control is automatically enabled for all interfaces on the 4-port 10/100 Fast Ethernet SPA.

Speed Settings

Separate the *speed-list* entries with a space.

When manually configuring the interface speed to either 10 or 100 Mbps, the switch prompts you to configure duplex mode on the interface.

The following *speed-list* configurations are supported:

- **speed auto—**Negotiate all speeds.
- **speed auto 10 100—**Negotiate 10 and 100 speeds only.
- **speed auto 10 100 1000—**Negotiate all speeds.

Speed and Duplex Combinations

The table below describes the interface behavior for various combinations of the **duplex** and **speed** command settings. The specified **duplex** command configured with the specified **speed** command produces the resulting system action.

If you decide to configure the interface speed and duplex commands manually, and enter a value other than **speed auto** (for example, 10 or 100 Mbps), ensure that you configure a connected interface with a matching speed using the speed command without using the **auto** keyword.

If you specify both a **duplex** and **speed** setting other than **auto** on an RJ-45 interface, then autonegotiation is disabled for the interface.

You cannot set the duplex mode to **half** when the port speed is set to **1000**, and similarly, you cannot set the port speed to **1000** when the mode is set to **half duplex**. In addition, if the port speed is set to **auto**, the **duplex** command is rejected.

Caution Changing the interface speed and duplex mode might shut down and reenable the interface during reconfiguration.

Table 17: Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex auto	**speed auto**	Autonegotiates both speed and duplex settings. The interface advertises the capability for the following link settings: • 10 Mbps and half duplex • 10 Mbps and full duplex • 100 Mbps and half duplex • 100 Mbps and full duplex • 1000 Mbps and half duplex (Gigabit Ethernet only) • 1000 Mbps and full duplex (Gigabit Ethernet only)
duplex auto	**speed 10** or **speed 100** or **speed 1000**	Autonegotiates the duplex mode. The interface advertises the capability for both half-duplex and full-duplex modes at the configured speed. For example, if the **speed 100** command is configured with **duplex auto**, then the interface advertises the following capability: • 100 Mbps and half duplex • 100 Mbps and full duplex

duplex Command	speed Command	Resulting System Action
duplex half or **duplex full**	**speed auto**	Autonegotiates the speed. The interface advertises the capability for duplex mode for Fast Ethernet interfaces at a speed of 10-Mbps and 100-Mbps, and Gigabit interfaces at 10-Mbps, 100-Mbps, and 1000-Mbps. For example, if the **duplex full** command is configured with the **speed auto** command, then the interface advertises the following capability: • 10 Mbps and full duplex • 100 Mbps and full duplex • 1000 Mbps and full duplex (Gigabit Ethernet interfaces only)
duplex half	**speed 10**	Forces a speed of 10-Mbps and the half-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 10**	Forces a speed of10-Mbps and the full-duplex operation, and disables autonegotiation on the interface.
duplex half	**speed 100**	Forces a speed of 100-Mbps and the half-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 100**	Forces a speed of 100-Mbps and the full-duplex operation, and disables autonegotiation on the interface.
duplex half	**speed 1000**	Forces a speed of 1000-Mbps and the half-duplex operation, and disables autonegotiation on the interface (Gigabit Ethernet only).
duplex full	**speed 1000**	Forces a speed of 1000-Mbps and the full-duplex operation, and disables autonegotiation on the interface (Gigabit Ethernet only).

Examples

The following example specifies the advertisement of only the 10 Mbps operation and either the full-duplex or half-duplex capability during autonegotiation for the second interface (port 1) on the SPA located in the bottom subslot (1) of the MSC that is installed in slot 2 of the Cisco 7304 router:

```
Device# configure terminal
Device(config)# interface fastethernet 2/1/1
Device(config-if)# speed 10
Device(config-if)# duplex auto
```

With this configuration, the interface advertises the following capabilities during autonegotiation:

- 10 Mbps and half duplex
- 10 Mbps and full duplex

Related Commands

Command	Description
duplex	Configures the duplex operation on an interface.
interface fastethernet	Selects a particular Fast Ethernet interface for configuration.
interface gigabitethernet	Selects a particular Gigabit Ethernet interface for configuration.
show controllers fastethernet	Displays Fast Ethernet interface information, transmission statistics and errors, and the applicable MAC destination address and VLAN filtering tables.
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics and errors, and the applicable MAC destination address and VLAN filtering tables.
show interfaces fastethernet	Displays information about the Fast Ethernet interfaces.
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

switchport

Cisco 3550, 4000, and 4500 Series Switches

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the **switchport** command in interface configuration mode. To put an interface into Layer 3 mode, use the **no** form of this command.

switchport

no switchport

Cisco Catalyst 6500/6000 Series Switches and Cisco 7600 Series Routers

To modify the switching characteristics of the Layer 2-switched interface, use the **switchport** command (without keywords). Use the **no** form of this command (without keywords) to return the interface to the routed-interface status and cause all further Layer 2 configuration to be erased. Use the **switchport** commands (with keywords) to configure the switching characteristics.

switchport

switchport {**host**| **nonegotiate**}

no switchport

no switchport nonegotiate

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

To configure the server module to communicate with the router over a high-speed Multi Gigabit Fabric (MGF) backplane switch port, use the **switchport** command (with keywords) in interface configuration mode.

switchport {**access**| **mode**| **trunk**}

Syntax Description

This command has no arguments or keywords.

Table 18: Cisco Catalyst 6500/6000 Series Switches and Cisco 7600 Series Routers

host	Optimizes the port configuration for a host connection.
nonegotiate	Specifies that the device will not engage in negotiation protocol on this interface.

Table 19: Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

access	Sets the access mode characteristics of the interface.

mode	Sets the interface type: Access or Trunk.
trunk	Sets trunk characteristics when the interface is in Trunk mode. This is the default mode.

Command Default

All interfaces are in Layer 2 mode.

Catalyst 6500/6000 Series Switches and 7600 Series Routers

The default access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(15)ZJ	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
15.1(2)T	Support for IPv6 was added.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).

Usage Guidelines

Cisco 3550, 4000, and 4500 Series Switches

Use the **no switchport** command to put the interface into the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port. Entering the **no switchport** command shuts down the port and then reenables it, which might generate messages on the device to which the port is connected.

You can verify the switchport status of an interface by entering the **show running-config** privileged EXEC command.

Cisco Catalyst 6500/6000 Series Switches and Cisco 7600 Series Routers

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

To optimize the port configuration, entering the **switchport host** command sets the switch port mode to access, enables spanning tree PortFast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning-tree PortFast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other Cisco 7600 series routers, hubs, concentrators, switches, and bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

The no form of the **switchport** nonegotiate command removes nonegotiate status.

When using the **nonegotiate** keyword, Dynamic Inter-Switch Link Protocol and Dynamic Trunking Protocol (DISL/DTP)-negotiation packets are not sent on the interface. The device trunks or does not trunk according to the mode parameter given: access or trunk. This command returns an error if you attempt to execute it in dynamic (auto or desirable) mode.

You must force a port to trunk before you can configure it as a SPAN-destination port. Use the **switchport nonegotiate** command to force the port to trunk.

Examples

Examples

The following example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed (Layer 3) port:

```
Router(config-if)#
no switchport
```

Examples

The following example shows how to cause the port interface to stop operating as a Cisco-routed port and convert to a Layer 2-switched interface:

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

Note The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

The following example shows how to optimize the port configuration for a host connection:

```
Router(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Router(config-if)#
```

This example shows how to cause a port interface that has already been configured as a switched interface to refrain from negotiating trunking mode and act as a trunk or access port (depending on the mode set):

```
Router(config-if)#
switchport nonegotiate
Router(config-if)#
```

The following example shows how to cause an interface to cease operating as a Cisco-routed port and to convert it into a Layer 2 switched interface:

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

Note The **switchport** command is not used on platforms that do not support Cisco-routed (Layer 3) ports. All physical ports on such platforms are assumed to be Layer 2 switched interfaces.

Examples

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
show running-config	Displays the current operating configuration.
switchport mode	Sets the interface type: Access or Trunk
switchport trunk	Sets trunk characteristics when the interface is in Trunk mode.
switchport access vlan	Sets the VLAN when the interface is in Access mode.

switchport access vlan

To set the VLAN when the interface is in access mode, use the **switchport access vlan** command in interface configuration or template configuration mode. To reset the access-mode VLAN to the appropriate default VLAN for the device, use the **no** form of this command.

switchport access vlan *vlan-id*

no switchport access vlan

Syntax Description

vlan-id	VLAN to set when the interface is in access mode; valid values are from 1 to 4094. Valid values for Cisco UCS E-Series Servers installed in Cisco 4400 Integrated Services Routers are: • 1-2349—VLAN ID Range 1 • 2450-4095—VLAN ID Range 2

Command Default

The defaults are as follows:

- Access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- All VLAN lists include all VLANs.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport access vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

The no form of the **switchport access vlan** command resets the access-mode VLAN to the appropriate default VLAN for the device.

Examples

The following example shows how to stop the port interface from operating as a Cisco-routed port and convert to a Layer 2 switched interface:

```
Device(config-if)# switchport
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

The following example shows how to make a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN in interface configuration mode:

```
Device(config-if)# switchport access vlan 2
```

The following example shows how to make a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN, using an interface template in template configuration mode:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# switchport access vlan 2
Device(config-template)# end
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Configures a LAN interface as a Layer 2 interface.

switchport autostate exclude

To exclude a port from the VLAN interface link-up calculation, use the **switchportautostateexclude**command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport autostate exclude

no switchport autostate exclude

Syntax Description

This command has no keywords or arguments.

Command Default

All ports are included in the VLAN interface link-up calculation.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchportautostateexclude** command. This action is required only if you have not entered the **switchport** command for the interface.

Note The **switchport**command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2 switched interfaces.

A VLAN interface configured on the MSFC is considered up if there are ports forwarding in the associated VLAN. When all ports on a VLAN are down or blocking, the VLAN interface on the MSFC is considered down. For the VLAN interface to be considered up, all the ports in the VLAN need to be up and forwarding. You can enter the switchport autostate **exclude**command to exclude a port from the VLAN interface link-up calculation.

The switchport autostate **exclude** command marks the port to be excluded from the interface VLAN up calculation when there are multiple ports in the VLAN.

The **showinterface***interface***switchport** command displays the autostate mode if the mode has been set. If the mode has not been set, the autostate mode is not displayed.

Examples

This example shows how to exclude a port from the VLAN interface link-up calculation:

```
Router(config-if)#
switchport autostate exclude
```

This example shows how to include a port in the VLAN interface link-up calculation:

```
Router(config-if)#
no switchport autostate exclude
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Configures a LAN interface as a Layer 2 interface.

switchport backup

To configure an interface as a Flexlink backup interface, use the **switchport backup** command in interface configuration mode. To disable this configuration, use the **no** form of this command.

switchport backup interface *type number*[**preemption** {**delay** *delay*| **mode** {**bandwidth**| **forced**| **off**}}]

no switchport backup [**interface** *type number* [**preemption** {**delay**| **mode**}]]

Syntax Description

interface *type number*	Specifies the interface type and the module and port number to be configured as a Flexlink backup interface.
preemption delay *delay*	Specifies the preemption delay in seconds. The range is from 0 to 300 seconds.
preemption mode bandwidth	Specifies that a higher bandwidth interface is preferred for preemption.
preemption mode forced	Specifies that an active interface is preferred for preemption.
preemption mode off	Specifies that preemption is turned off.

Command Default

Interfaces are not configured as Flexilink backup interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(1)SY	This command was modified. The **no** form was modified so that specific backup configurations can be disabled.

Usage Guidelines

When you enable Flexlink, both the active and standby links are up physically, and mutual backup is provided.

Flexlink is supported on Layer 2 interfaces only and does not support routed ports.

The *number* arguement designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in

a 13-slot chassis, valid values for the slot number are from 1 to 13, and valid values for the port number are from 1 to 48.

Flexlink is designed for simple access topologies (two uplinks from a leaf node). You must ensure that there are no loops from the wiring closet to the distribution/core network to enable Flexlink to perform correctly.

Flexlink converges faster for directly connected link failures. Flexlink fast convergence does not impact any other type of network failure.

You must enter the **switchport** command without any keywords to configure a LAN interface as a Layer 2 interface before you can enter the **switchport backup** command.

You can remove all Flexilink configurations on an interface by using the **no switchport backup** command. You can remove specific backup configurations by using the optional keywords in the **no** form of this command.

Note The **switchport** command is used only on platforms that support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2 switched interfaces.

Examples

The following example shows how to enable Flexlink on an interface. This example also shows how to configure a preemption delay of 100 seconds on an interface.

```
Device(config)# interface GigabitEthernet1/1
Device(config-if)# switchport
Device(config-if)# switchport backup interface GigabitEthernet1/2
Device(config-if)# switchport backup interface GigabitEthernet1/2 preemption delay 100
Device(config-if)# end
Device# show running interface GigabitEthernet1/1

Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet1/1
 switchport
 switchport backup interface Gi1/2
 switchport backup interface Gi1/2 preemption delay 100
end

Device# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
Gi1/1                   Gi1/2                   Active Up/Backup Down
```

The following example shows how to disable specific backup configurations on an interface:

```
Device(config)# interface GigabitEthernet1/1
Device(config-if)# no switchport backup interface GigabitEthernet1/2 preemption delay
Device(config-if)# end
Device# show running-config interface GigabitEthernet1/1

Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet1/1
 switchport
 switchport backup interface Gi1/2
end
```

The following example shows how to disable Flexlink and remove all Flexlink configurations on an interface:

```
Device(config)# interface GigabitEthernet1/1
Device(config-if)# no switchport backup interface GigabitEthernet1/2
Device(config-if)# end
Device# show running-config interface GigabitEthernet1/1

Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet1/1
 switchport
end
```

Related Commands

Command	Description
show interfaces switchport backup	Displays Flexlink pairs.
show running-config	Displays the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or VC class.
switchport	Configures a LAN interface as a Layer 2 interface.
switchport autostate exclude	Excludes a port from the VLAN interface link-up calculation.

switchport block unicast

To prevent the unknown unicast packets from being forwarded, use the **switchportblockunicast**command in interface configuration mode. To allow the unknown unicast packets to be forwarded, use the **no** form of this command.

switchport block unicast

no switchport block unicast

Syntax Description

This command has no arguments or keywords.

Command Default

The default settings are as follows:

- Unknown unicast traffic is not blocked.
- All traffic with unknown MAC addresses is sent to all ports.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can block the unknown unicast traffic on the switch ports.

Blocking the unknown unicast traffic is not automatically enabled on the switch ports; you must explicitly configure it.

Note For more information about blocking the packets, refer to the Cisco 7600 Series Router Cisco IOS Software Configuration Guide.

You can verify your setting by entering the **showinterfaces** *interface-id***switchport** command.

Examples

This example shows how to block the unknown unicast traffic on an interface:

```
Router(config-if)# switchport block unicast
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport mode

To set the interface type, use the **switchport mode** command in interface configuration mode. Use the appropriate **no** form of this command to reset the mode to the appropriate default mode for the device.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

switchport mode {**access**| **trunk**}

no switchport mode

Cisco Catalyst 6500/6000 Series Switches

switchport mode {**access**| **dot1q-tunnel**| **dynamic** {**auto**| **desirable**}| **trunk**}

no switchport mode

Cisco 7600 Series Routers

switchport mode {**access**| **dot1q-tunnel**| **dynamic** {**auto**| **desirable**}| **private-vlan**| **trunk**}

no switchport mode

switchport mode private-vlan {**host**| **promiscuous**}

no switchport mode private-vlan

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

switchport mode {**access**| **trunk**}

no switchport mode {**access**| **trunk**}

Syntax Description

access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.
dot1q-tunnel	Sets the trunking mode to TUNNEL unconditionally.
dynamic auto	Sets the interface to convert the link to a trunk link.
dynamic desirable	Sets the interface to actively attempt to convert the link to a trunk link.
private vlan host	Specifies that the ports with a valid private VLAN (PVLAN) association become active host private VLAN ports.
private vlan promiscuous	Specifies that the ports with a valid PVLAN mapping become active promiscuous ports.

Table 20: Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.

Command Default The default is **access** mode.

Command Default The default mode is dependent on the platform; it should be either **dynamic auto** for platforms that are intended as wiring closets or **dynamic desirable** for platforms that are intended as backbone switches. The default for PVLAN ports is that no mode is set.

Command Default The defaults are as follows:

- The mode is dependent on the platform; it should either be **dynamic auto** for platforms that are intended for wiring closets or **dynamic desirable** for platforms that are intended as backbone switches.
- No mode is set for PVLAN ports.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Cisco Catalyst 6000 family switches.
12.1(1)E	This command was integrated on the Cisco Catalyst 6000 family switches.
12.1(8a)EX	The switchport mode **private-vlan** {**host** | **promiscuous**} syntax was added.
12.2(2)XT	Creation of switchports became available on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for creation of switchports on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

If you enter a forced mode, the interface does not negotiate the link to the neighboring interface. Ensure that the interface ends match.

The **no** form of the command is not supported on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Cisco Catalyst 6500/6000 Switches and Cisco 7600 Series Routers

If you enter **access** mode, the interface goes into permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

If you enter **trunk** mode, the interface goes into permanent trunking mode and negotiates to convert the link into a trunk link even if the neighboring interface does not agree to the change.

If you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

If you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

If you configure a port as a promiscuous or host-PVLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid PVLAN association or mapping configured.
- The port is a SPAN destination.

If you delete a private-port PVLAN association or mapping, or if you configure a private port as a SPAN destination, the deleted private-port PVLAN association or mapping or the private port that is configured as a SPAN destination becomes inactive.

If you enter **dot1q-tunnel** mode, PortFast Bridge Protocol Data Unit (BPDU) filtering is enabled and Cisco Discovery Protocol (CDP) is disabled on protocol-tunneled interfaces.

Examples

Examples

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)#switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)#switchport mode trunk
```

Examples

The following example shows how to set the interface to dynamic desirable mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode dynamic desirable
```

The following example shows how to set a port to PVLAN-host mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode private-vlan host
```

The following example shows how to set a port to PVLAN-promiscuous mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode private-vlan promiscuous
```

The following example shows how to configure tunneling on port 4/1 and verify the configuration:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode dot1q-tunnel
Router(config-if)# end
```

Examples

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
```

Related Commands

Command	Description
show dot1q-tunnel	Displays a list of 802.1Q tunnel-enabled ports.
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
show interfaces trunk	Displays trunk information.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.
switchport private vlan host association	Defines a PVLAN association for an isolated or community port.
switchport private vlan mapping	Defines the PVLAN mapping for a promiscuous port.
switchport trunk	Sets trunk characteristics when the interface is in trunking mode.

switchport port-security

To enable port security on an interface, use the **switchportport-security** command in i nterface configuration mode . To disable port security, use the **no** form of this command.

switchport port-security

no switchport port-security

Syntax Description

This command has no keywords or arguments.

Command Default

D isabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks.
- With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
- With releases earlier than Release 12.2(18)SXE, port security is not supported on 802.1Q tunnel ports.
- A secure port cannot be a destination port for a Switch Port Analyzer (SPAN).
- A secure port cannot belong to an EtherChannel.
- A secure port cannot be a trunk port.

- A secure port cannot be an 802.1X port. If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.

Examples

This example shows how to enable port security:

```
Router(config-if)#
switchport port-security
```

This example shows how to disable port security:

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security aging

To configure the port security aging , use the **switchport** port-security aging time command in interface configuration mode . To disable aging, use the **no** form of this command.

switchport port-security aging {**time** *time*| **type** {**absolute| inactivity**}}

no switchport port-security aging

Syntax Description

time *time*	Sets the duration for which all addresses are secured; valid values are from 1 to 1440 minutes.
type	Specifies the type of aging.
absolute	Specifies absolute aging; see the “Usage Guidelines” section for more information.
inactivity	Specifies that the timer starts to run only when there is no traffic; see the “Usage Guidelines” section for more information.

Command Default

The defaults are as follows:

- Disabled.
- If enabled, t he defaults are as follows:
  - *time* is 0.
  - **type** is **absolute**

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

Release	Modification
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. • The **type**, **absolute**, and **inactivity** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks. With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. With releases earlier than Release 12.2(18)SXE, port security is not supported on 802.1Q tunnel ports.

You can apply one of two types of aging for automatically learned addresses on a secure port:

- Absolute aging times out the MAC address after the age-time has been exceeded, regardless of the traffic pattern. This default is for any secured port, and the age-time is set to 0.
- Inactivity aging times out the MAC address only after the age_time of inactivity from the corresponding host has been exceeded.

Examples

This example shows how to set the aging time as 2 hours:

```
Router(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes:

```
Router(config-if)# switchport port-security aging time 2
```

This example shows how to set the aging type on a port to absolute aging:

```
Router(config-if) switchport port-security aging type absolute
```

This example shows how to set the aging type on a port to inactivity aging:

```
Router(config-if) switchport port-security aging type
 inactivity
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport private-vlan host-association

To define a PVLAN association for an isolated or community port, use the **switchportprivate-vlanhost-association**command in i nterface configuration mode . To remove the PVLAN mapping from the port, use the **no** form of this command.

switchport private-vlan host-association *primary-vlan-id secondary-vlan-id*

no switchport private-vlan host-association

Syntax Description

primary-vlan-id	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.

Command Default

No PVLAN is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to t Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

There is no run-time effect on the port unless it is in PVLAN-host mode. If the port is in PVLAN-host mode but neither of the VLANs exist, the command is allowed but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

Examples

This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN (VLAN 20):

```
Router(config-if)#
switchport private-vlan host-association 18 20
```

This example shows how to remove the PVLAN association from the port:

```
Router(config-if)#
no switchport private-vlan host-association
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport mode	Displays the administrative and operational status of a switching (nonrouting) port.

switchport private-vlan mapping

To define the PVLAN mapping for a promiscuous port, use the **switchportprivate-vlanmapping** command in interface configuration mode. To clear all mappings from the primary VLAN, use the **no** form of this command.

{**switchport private-vlan mapping primary-vlan-id secondary-vlan-list**| **add secondary-vlan-list**| **remove secondary-vlan-list**}

no switchport private-vlan mapping

Syntax Description

primary-vlan-id	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
secondary-vlan- list	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.
add	Maps the secondary VLANs to the primary VLAN.
remove	Clears mapping between the secondary VLANs and the primary VLAN.

Command Default

No PVLAN mappings are configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

There is no run-time effect on the port unless it is in PVLAN-promiscuous mode. If the port is in PVLAN-promiscuous mode but the VLANs do not exist, the command is allowed but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

Examples

This example shows how to configure the mapping of primary VLAN 18 to secondary isolated VLAN 20 on a port:

```
Router(config-if)#
switchport private-vlan mapping 18 20
```

This example shows how to add a VLAN to the mapping:

```
Router(config-if)#
switchport private-vlan mapping 18 add 21
```

This example shows how to remove the PVLAN mapping from the port:

```
Router(config-if)#
no switchport private-vlan mapping
```

Related Commands

Command	Description
show interfaces private-vlan mapping	Displays the information about the PVLAN mapping for VLAN SVIs.

switchport protected

Use the switch**portprotected**command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch in interface configuration mode. To disable protection on the port, use the **no** form of the command.

switchport protected

no switchport protected

Syntax Description

This command has no arguments or keywords.

Command Default

No protected port is defined. All ports are nonprotected.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(4)EA1	This command was first introduced.
12.4(15)T	This command was implemented on the following platforms: the Cisco 1841 Integrated Services Router (ISR), Cisco 2800 series ISRs, and Cisco 3800 series ISRs.

Usage Guidelines

The switchport protection feature is local to the switch; communication between protected ports on the same switch is possible only through a Layer 3 device. To prevent communication between protected ports on different switches, you must configure the protected ports for unique VLANs on each switch and configure a trunk link between the switches.

Beginning with Cisco IOS Release 12.4(15)T, the following Cisco ISRs support port protection when an appropriate high-speed WAN interface card (HWIC) is installed:

- Cisco 1841 ISR
- Cisco 2800 Series ISRs, including models 2801, 2811, 2821, and 2851
- Cisco 3800 Series ISRs, including models 3825 and 3845

To support port protection, the Cisco routers listed above must be equipped with one of the following HWICs:

- HWIC-4ESW
- HWIC-D-9ESW

Note Only the ports attached to the HWICs can be configured with port protection.

A protected port does not forward any unicast, multicast, or broadcast traffic to any other protected port. A protected port continues to forward unicast, multicast, and broadcast traffic to unprotected ports and vice versa.

Port monitoring does not work if both the monitor and monitored ports are protected ports.

A protected port is different from a secure port.

Examples

The following example shows how to enable a protected port on an interface:

```
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# switchport protected
```

You can verify the previous command by entering the**showinterfacesswitchport**privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport block	Prevents unknown multicast or unicast traffic on the interface.

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command in interface configuration mode. To reset all of the trunking characteristics back to the original defaults, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

switchport trunk {**encapsulation dot1q**| **native vlan**| **allowed vlan**}

no switchport trunk {**encapsulation dot1q**| **native vlan**| **allowed vlan**}

Cisco 7600 Series Routers and Catalyst 6500 Series Switches

{**switchport trunk encapsulation** {**isl**| **dot1q** [**ethertype** *value*]| **negotiate**}| **native vlan** {**tag**| *vlan-id*}| **allowed vlan** *vlan-list*| **pruning vlan** *vlan-list*}

no switchport trunk {**encapsulation** {**isl**| **dot1q** [**ethertype** *value*]| **negotiate**}| **native vlan [tag]**| **allowed vlan**| **pruning vlan**}

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

switchport trunk {**native vlan** *vlan-id*| **allowed vlan** *vlan-list*}

no switchport trunk {**native vlan** *vlan-id*| **allowed vlan** *vlan-list*}

Syntax Description

encapsulation isl	Sets the trunk encapsulation format to Inter-Switch Link (ISL).
encapsulation dot1q	Sets the trunk encapsulation format to 802.1Q.
native vlan	Sets the native VLAN for the trunk in 802.1Q trunking mode.
allowed vlan *vlan list*	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.
ethertype *value*	(Optional) Sets the EtherType value; valid values are from 0x0 to 0x5EF-0xFFFF.
encapsulation negotiate	Specifies that if the Dynamic Inter-Switch Link (DISL) protocol and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, ISL is the selected format.
native vlan tag	Enables the native VLAN tagging state on the interface.
native vlan *vlan id*	The particular native VLAN.

pruning vlan *vlan list*	Sets the list of VLANs that are enabled for VLAN Trunking Protocol (VTP) pruning when the interface is in trunking mode. See the "Usage Guidelines" section for the *vlanlist*argument formatting guidelines.

Table 21: Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

native vlan *vlan-id*	The particular native VLAN. Valid values are: • 1-2349—VLAN ID Range 1 • 2450-4095—VLAN ID Range 2
allowed vlan *vlan-list*	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode. **Note** For *vlan-list* format, see **Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers** section under **Usage Guidelines**.

Command Default

- The default encapsulation type is dot1q.
- The default access VLAN and trunk interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- The default for all VLAN lists is to include all VLANs.

Command Default

- The encapsulation type is dependent on the platform or interface hardware.
- The access VLAN and trunk interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- The default for all VLAN lists is to include all VLANs.
- **ethertype** *value* for 802.1Q encapsulation is 0x8100.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6500 series switches.

Release	Modification
12.1(1)E	Switchport creation on Catalyst 6500 series switches was added.
12.2(2)XT	This command was introduced to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switch port creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX to support the Supervisor Engine 720 on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.2(17a)SX	This command was modified to include the following: • Restriction of ISL trunk-encapsulation. • Addition of the **dot1q** keyword and **ethertype***value* keyword and argument.
12.2(17d)SXB	Support for the Supervisor Engine 2 on the Cisco 7600 series routers and Catalyst 6500 series switches was added.
12.2(18)SXD	This command was modified to allow the **switchport trunk allowed vlan**command to be entered on interfaces where the span destination port is either a trunk or an access port.
12.2(18)SXE	This command added a restriction that Gigabit Ethernet (GE) Optimized Layer 2 WAN ports are not supported on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs from 1 to 4094 for specified platforms.
12.2(33)SXH	This command was changed as follows: • Allowed the tagging of native VLAN traffic on a per-port basis. • Introduced on the Supervisor Engine 720-10GE.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).

Usage Guidelines

802.1Q Trunks

- When you connect Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.

- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning-tree loops. Cisco recommends that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure that your network is free of physical loops before disabling spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree bridge protocol data units (BPDUs) on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Shared Spanning Tree Protocol (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
- The 802.1Q switches that are not Cisco switches maintain only a single instance of spanning-tree (Mono Spanning Tree [MST]) that defines the spanning-tree topology for all VLANs. When you connect a Cisco switch to a switch through an 802.1Q trunk without a Cisco switch, the MST of the switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning-tree topology known as the Common Spanning Tree (CST).
- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, switches that are not Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the 802.1Q cloud receive these flooded BPDUs. This condition allows Cisco switches to maintain a per-VLAN spanning-tree topology across a cloud of 802.1Q switches that are not Cisco switches. The 802.1Q cloud of switches separating the Cisco switches is treated as a single broadcast segment among all switches connected to the 802.1Q cloud of switches that are not Cisco switches through 802.1Q trunks.
- Make sure that the native VLAN is the same on *all* of the 802.1Q trunks that connect the Cisco switches to the 802.1Q cloud of switches that are not Cisco switches.
- If you are connecting multiple Cisco switches to a 802.1Q cloud of switches that are not Cisco switches, all of the connections must be through 802.1Q trunks. You cannot connect Cisco switches to an 802.1Q cloud of switches that are not Cisco switches through ISL trunks or through access ports. Doing so will cause the switch to place the ISL trunk port or access port into the spanning-tree "port inconsistent" state and no traffic will pass through the port.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support 802.1Q formats.

The *vlanlist* format is **all** | **none** | **add** | **remove** | **except***vlanlist*[,*vlanlist*...] where:

- **all** --Specifies all VLANs from 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.
- **none** --Indicates an empty list. This keyword is not supported in the **switchport trunk allowed vlan** form of the command.
- **add** --Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove** --Removes the defined list of VLANs from those currently set instead of replacing the list.
- **except** --Lists the VLANs that should be calculated by inverting the defined list of VLANs.
- *vlan list*-- Is either a single VLAN number from 1 to 1005 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the

allowed VLANs when this port is in trunking mode. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.

Cisco 7600 Series Routers and Catalyst 6500 Series Switches

This command is not supported on GE Layer 2 WAN ports.

You can enter the **switchport trunk** command only on the PO. If you enter the **switchport trunk** command on a port member the following message is displayed:

```
Configuration is not allowed on Port members. Remove the interface from the Port Channel
to modify its config
```

The **switchport trunk encapsulation dot1q**command is supported only for platforms and interface hardware that can support both ISL and 802.1Q formats. Only 802.1Q encapsulation is supported by shared port adapters (SPAs).

If you enter the **switchport trunk encapsulation isl** command on a port channel containing an interface that does not support ISL-trunk encapsulation, the command is rejected.

You can enter the **switchport trunk allowed vlan** command on interfaces where the span destination port is either a trunk or an access port.

You can enter the **switchport trunk native vlan tag** command to enable the tagging of native VLAN traffic on a per-port basis. When tagging is enabled, all the packets on the native VLAN are tagged and all incoming untagged data packets are dropped, but untagged control packets are accepted. When tagging is disabled, the native VLAN packets going out on trunk ports are not tagged and the incoming untagged packets are allowed and assigned to the native VLAN. The **no switchport trunknative vlan tag** command overrides the **vlan dot1q tag native** command for global tagging.

Note The **switchport trunk native vlan tag** interface configuration mode command does not enable native VLAN tagging unless you first configure the switch to tag native VLAN traffic globally. To enable native VLAN tagging globally, use the **vlan dot1q tag native** command in global configuration mode.

Note The **switchport trunk pruning vlan** *vlan-list* command does not support extended-range VLANs; valid *vlan-list* values are from 1 to 1005.

The **dot1q ethertype** *value* keyword and argument are not supported on port-channel interfaces. You can enter the command on the individual port interface only. Also, you can configure the ports in a channel group to have different EtherType configurations.

Caution Be careful when configuring the custom EtherType value on a port. If you enter the **negotiate** keyword and DISL and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, then ISL is the selected format and may pose as a security risk. The **no** form of this command resets the trunk-encapsulation format to the default.

- The **no** form of the **switchport trunk native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.
- The **no** form of the **switchport trunk native vlan tag** command configures the Layer 2 port not to tag native VLAN traffic.

- The **no** form of the **switchport trunk allowed vlan** command resets the list to the default list, which allows all VLANs.
- The **no** form of the **switchport trunk pruning vlan**command resets the list to the default list, which enables all VLANs for VTP pruning.
- The **no** form of the **switchport trunk encapsulation dot1qethertype***value* command resets the list to the default value.

The *vlan-list* format is **all** | **none** | **add** | **remove** | **except** [*vlan-list*[**,***vlan-list*...]] where:

- **all** --Specifies all the appropriate VLANs. This keyword is not supported in the **switchporttrunkpruningvlan** command.
- **none** --Indicates an empty list. This keyword is not supported in the **switchporttrunkallowedvlan** command.
- **add** *vlan-list* **,** *vlan-list...*]-- Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove** *vlan-list* **,** *vlan-list...*]-- Removes the defined list of VLANs from those currently set instead of replacing the list. You can remove VLAN 1. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic (for example, Cisco Discovery Protocol, version 3; VTP; Port Aggregation Protocol, version 4 (PAgP4); and DTP) in VLAN 1.

Note You can remove any of the default VLANs (1002 to 1005) from a trunk; this action is not allowed in earlier releases.

- **except** *vlan-list* **,** *vlan-list...*] --Excludes the specified list of VLANs from those currently set instead of replacing the list.
- *vlan-list* **,** *vlan-list...* -- Specifies a single VLAN number from 1 to 4094 or a continuous range of VLANs that are described by two VLAN numbers from 1 to 4094. You can specify multiple VLAN numbers or ranges of numbers using a comma-separated list.

To specify a range of VLANs, enter the smaller VLAN number first, separated by a hyphen and the larger VLAN number at the end of the range.

Do not enable the reserved VLAN range (1006 to 1024) on trunks when connecting a Cisco 7600 series router running the Cisco IOS software on both the supervisor engine and the Multilayer Switch Feature Card (MSFC) to a Cisco 7600 series router running the Catalyst operating system. These VLANs are reserved in Cisco 7600 series routers running the Catalyst operating system. If enabled, Cisco 7600 series routers running the Catalyst operating system may disable the ports if a trunking channel is between these systems.

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

Note To set trunk characteristics, the interface must be in trunk mode.

The *vlan-list* format is **all** | **none** | **add** | **remove** | **except** | **WORD**, where:

- **all—**Specifies all VLANs: 1-2349**—**VLAN IDs in range 1; and 2450-4095**—**VLAN IDs in range 2.

- **none—**Indicates an empty list.
- **add—**Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove—**Removes the defined list of VLANs from those currently set instead of replacing the list.
- **except—**Lists the VLANs that should be calculated by inverting the defined list of VLANs.
- **WORD—**Is either a single VLAN number from 1 to 4095 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode.

Examples

The following example shows how to cause a port interface configured as a switched interface to encapsulate in 802.1Q trunking format regardless of its default trunking format in trunking mode:

Router(config-if)# switchport trunk encapsulation dot1q

The following example shows how to configure the Layer 2 port to tag native VLAN traffic:

```
Router(config-if)#
switchport trunk native vlan tag
```

Examples

Note To set trunk characteristics, the interface must be in trunk mode.

The following example shows how to allow trunking on specified VLANs:

```
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk allowed vlan 1-2,40,60,1002-1005
```

Related Commands

Command	Description
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
vlan dot1q tag native	Enables dot1q tagging for all VLANs in a trunk.

switchport voice vlan

To configure a voice VLAN on a multiple-VLAN access port, use the **switchportvoicevlan** command in interface configuration mode. To remove the voice VLAN from the switch port, use the **no** form of the command.

switchport voice vlan {*vlan-id*| **dot1p**| **none**| **untagged**}

no switchport voice vlan

Syntax Description

vlan id	Voice VLAN identifier (VVID) of the VLAN used for voice traffic. Valid IDs are from 1 to 1005 (IDs 1006 to 4096 are not supported). Do not enter leading zeros. The switch port is an 802.1Q trunk port.
dot1p	The telephone uses priority tagging and uses VLAN 0. The switch port is an 802.1Q trunk port.
none	The telephone is not instructed through the command line interface (CLI) about the voice VLAN. The telephone uses its own configuration from the telephone keypad and transmits untagged voice traffic in the default VLAN.
untagged	The telephone does not tag frames; it uses VLAN 4095. The switch port can be an access port or an 802.1Q trunk port.

Command Default

The switch default is to not automatically configure the telephone (**none**).

The Cisco IP 7960 telephone default is to generate an 802.1Q/802.1P frame.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XT	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support creation of switchports .
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and introduced on the Supervisor Engine 720.

Release	Modification
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB and introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

This command does not create a voice VLAN. You can create a voice VLAN in VLAN-configuration mode by entering the **vlan(globalconfigurationmode)** command. If you configure both the native VLAN and the voice VLAN in the VLAN database and set the switch port to multiple-VLAN access mode, this command brings up the switch port as operational.

If you enter a voice VLAN identifier, the switch port sends CDP packets that configure the IP phone to transmit voice traffic in the voice VLAN in 802.1Q frames that are tagged with a Layer 2 CoS value . The default Layer 2 CoS is 5. The default Layer 3 IP-precedence value is 5.

If you enter dot1p, the switch port sends CDP packets that configure the IP phone to transmit voice traffic in the default VLAN in 802.1p frames that are tagged with a Layer 2 CoS value.

If you enter none, the switch port does not send CDP packets with VVID TLVs.

If you enter **untagged**, the switch port is enabled to receive untagged packets only.

Examples

This example shows how to create an operational multiple-VLAN access port with VLAN 101 as the voice VLAN:

```
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 100
Router(config-if)# switchport voice vlan 101
Router(config-if)
```

This example shows how to change the multiple-VLAN access port to a normal access port:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# no switchport voice vlan
Router(config-if)
```

Related Commands

Command	Description
switchport access vlan	Sets the VLAN when the interface is in access mode.
switchport mode	Sets the interface type.