show facility-alarm

To display the status of a generated alarm, use the **show facility-alarm** command in privileged EXEC mode.

show facility-alarm {**status** [*severity*] | **relay**}

Cisco ASR 1000 Series Routers

show facility-alarm status [*severity*]

Syntax Description

status	Shows facility alarms by status and displays the settings of all user-configurable alarm thresholds. (Alarm thresholds are not configurable on the Cisco ASR 1000 Series Routers.)
severity	(Optional) String that identifies the severity of an alarm. The default severity level is info, which shows all alarms. Severity levels are defined as the following: • **critical**—The condition affects service. • **major**—Immediate action is needed. • **minor**—Minor warning conditions. • **info**—No action is required.
relay	Shows facility alarms by relay.

Command Default

All alarms are shown.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.4(4)T	The *severity* argument was added in Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the PRE3 for the Cisco 10000 series router.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 on the Cisco ASR 1000 Series Routers.

Usage Guidelines

When a severity level is configured, statuses of alarms at that level and higher are shown. For example, when you set a severity of major, all major and critical alarms are shown.

Examples

The following is sample output from the **show facility-alarm status** command:

```
Router# show facility-alarm status

System Totals  Critical:1  Major:0  Minor:0
Source              Severity      Description [Index]
------              --------      -------------------
Fa0/0               CRITICAL      Physical Port Link Down [0]
Fa1/0               INFO          Physical Port Administrative State Down [1]
```

The following is a sample output from the **show facility-alarm status** command with a severity level set at major:

```
Router# show facility-alarm status major

System Totals  Critical:1  Major:0  Minor:0

Source              Severity      Description [Index]
------              --------      -------------------
Fa0/0               CRITICAL      Physical Port Link Down [0]
```

Table 54 describes the significant fields shown in the displays.

Table 54 show facility-alarm status Field Descriptions

Field	Description
System Totals	Total number of alarms generated, identified by severity.
Source	Interface from which the alarm was generated.
Severity	Severity level of the alarm generated.
Description [Index]	Type of the alarm and the index of the alarm type. The index can be any number based on the number of alarm types that the device supports.

Related Commands

Command	Description
clear facility-alarm	Clears alarm conditions and resets the alarm contacts.
facility-alarm	Configures threshold temperatures for minor, major, and critical alarms.

show format

To display a fully expanded list of commands that have a spec file entry (SFE), display the SFE of a specific command, or validate a specific spec file, use the **show format** command in privileged EXEC mode.

show format [**built-in** | *location*:*local-filename*] [**cli** *command* | **validate**]

Syntax Description

built-in	(Optional) Displays the commands with SFEs in the built-in spec file, and validates the built-in spec file when used with the **validate** keyword. Displays the SFE for a specific command when used with the **cli** keyword and *command* argument.
location:*local-filename*	(Optional) Command Operational Data Model (ODM) spec file location and filename. Valid locations are **bootflash:**, **flash:**, **nvram:**, and any valid disk or slot number (such as **disk0:** or **slot1:**). ODM spec files have a .odm suffix. The pipe (|) output modifier can be used in the command. **Note** These arguments are not required if you want to use a default ODM file defined with the **format global** command.
cli *command*	(Optional) Displays only the SFE for the specified command. Enter a fully expanded command name.
validate	(Optional) Validates the built-in spec file or a specific spec file.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was modified. The **built-in** and **validate** keywords were added. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.

Usage Guidelines

Use the **show format** command to display an index of commands that have an SFE in the spec file, display the SFE of a specific command, or validate a spec file. The SFE of any command is in XML format.

Use the **show format** command to display an index of commands with an SFE in the current spec file. Some commands have an SFE in the built-in spec file of the image. Use the **show format built-in** command to display an index of the commands with an SFE in the built-in spec file.

To display the SFE for a specific command in the built-in spec file, use the **show format built-in cli** *command* command. For example, if **show inventory** is present in the built-in spec file, then **show format built-in cli** *show inventory* command will display the spec entry for this Command Line Interface (CLI). To display the SFE for a specific command in a specific spec file, use the **show format** *location*:*local-filename* **cli** *command* command.

To validate the built-in spec file use the **show format built-in validate** command. To validate a specific spec file use the **show format** *location:local-filename* **validate** command.

Examples

The following example displays the list of commands that have SFEs in the built-in spec file of the image:

```
Router# show format built-in

The following CLI are supported in built-in
show inventory
show ip interface brief
```

The following example shows a list of fully expanded command names that have spec files in the spec3.3.odm file. A message is attached that lists an incorrectly defined command.

```
Router# show format slot0:spec3.3.odm

The following CLI are supported in slot0:spec3.3.odm
show arp
show bootvar
show cdp neighbors detail
show context
show flash:
show interfaces*
show interfaces
show inventory
show ip interface*
show ip interface brief
show ip nat translations
show line value
show line
show processes memory
show region
show spanning-tree
show stacks
The following CLI are IGNORED (incorrectly entered) in slot0:spec3.3.odm
show async status
```

The following example shows the output when the spec entry for a particular command is requested from the default ODM file:

```
Router# show format cli show inventory

<?xml version='1.0' encoding='utf-8'?>
<ODMSpec>
<Command>
<Name>show inventory</Name>
</Command>
<OS>ios</OS>
<DataModel>
<Container name="ShowInventory">
<Container name="NAME:" alias = "InventoryEntry" dynamic = "true">
<Property name="NAME:" alias = "ChassisName" distance = "1" length = "1" end-de>
<Property name="DESCR:" alias = "Description" distance = "1" length = "-1" type>
<Property name="PID:" alias="PID" distance = "1" length = "5" end-delimiter = ">
<Property name="VID:" alias="VID" distance = "1" length = "1" end-delimiter = ">
<Property name="SN:" alias="SN" distance = "1" length = "1" end-delimiter = ",">
</Container>
</Container>
</DataModel>
</ODMSpec>
```

The following example shows the output when the spec entry for a particular command is requested from a specific ODM file:

```
Router# show format slot0:spec3.3.odm cli show ip interface brief

<?xml version="1.0" encoding="UTF-8"?>
<ODMSpec>

        <Command>
                <Name>show ip interface brief</Name>
        </Command>

        <OS>ios</OS>

        <DataModel>
                <Container name="ShowIpInterfaceBrief">
                        <Table name="IPInterfaces">
                                <Header name="Interface" type="String" start="0"
end="23"/>
                                <Header name="IP-Address" type="IpAddress" start="24"
end="41"/>
                                <Header name="OK" type="String" start="42" end="46"/>
                                <Header name="Method" type="String" start="47" end="53"/>
                                <Header name="Status" type="String" start="54" end="75"/>
                                <Header name="Protocol" type="String" start="76"
end="-1"/>
                        </Table>
                </Container>
</DataModel>
</ODMSpec>
```

The following example validates the built-in spec file:

```
Router# show format built-in validate

The file built-in has been validated
```

The following example shows the output when a spec file fails to validate:

```
Router# show format disk2:/spec3.4.odm validate

The following problem was detected in disk2:/spec3.4.odm bad format in the spec file, show
line value
```

The following example shows the output when a specific spec file is validated:

```
Router# show format disk2:/spec3.user1.odm validate

The file disk2:/spec3.user1.odm has been validated
```

The following example specifies the spec file named spec3.user2.odm as the default spec file instead of the built-in spec file, replaces the current spec file with it, and ensures that it is validated as the current spec file:

```
Router(config)# format global disk2:/spec3.user2.odm
Router(config)# exit
Router# spec-file install disk2:/spec3.user2.odm built-in
Replace existing file? [yes]: Enter
Router#
Router# show format validate
The file disk2:/spec3.user2.odm has been validated
```

Each display from the **show format** command is self-explanatory; see the "Usage Guidelines" section for more information.

Related Commands

Command	Description
format global	Specifies a default ODM spec file other than the built-in spec file.
show odm-format	Displays the schema of the spec file.
show xsd-format	Generates XML Schema Definition (XSD) output for a command.
spec-file install built-in	Replaces the current spec file with the built-in spec file.

show ip director default

Note Effective with Cisco IOS Release 12.4(24)T, the **show ip director default** command is not available in Cisco IOS software.

To verify default metric configuration information for DistributedDirector metrics, use the **show ip director default** command in privileged EXEC mode.

show ip director default [**priority** | **weight**]

Syntax Description

priority	(Optional) Default priorities for metrics.
weight	(Optional) Displays the weights for metrics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.4(24)T	This command was removed.

Usage Guidelines

Use this command to verify default metric configurations.

Examples

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

```
Router# show ip director default priority

Director default metric priorities:
random priority = 2
DRP route lookup external to AS priority = 1
administrative preference priority = 0
DRP route lookup internal to AS priority = 0
DRP distance to associated server priority = 0
portion priority = 0
Round-trip time from DRP to client priority = 0
DFP originated weight priority = 0
Route-map evaluation priority = 0
```

Related Commands

Command	Description
ip director default priorities	Sets default priorities for DistributedDirector metrics.

show ip director dfp

Note Effective with Cisco IOS Release 12.4(24)T, the **show ip director dfp** command is not available in Cisco IOS software.

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

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

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
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.
12.4(24)T	This command was removed.

Examples

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

```
Router# show ip director dfp

172.24.9.9:
    Max retries: 5
    Timeout between connect attempts: 60
    Timeout between updates: 90
    Last update received: 00:00:12 ago
    Server  Port BindID Address Mask
    172.28.9.9 80 0  0.0.0.0 0.0.0.0
192.168.25.25
    Max retries: 5
    Timeout between connect attempts: 60
    Timeout between updates: 90
    Last update received: 00:00:44 ago
    Server Port BindIDAddress Mask
    192.168.30.30 800 0.0.0.0 0.0.0.0
```

show ip director drp

Note Effective with Cisco IOS Release 12.4(24)T, the **show ip director drp** command is not available in Cisco IOS software.

To display information that the DistributedDirector has about specific Director Response Protocol (DRP) agents, use the **show ip director drp** command in privileged EXEC mode.

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

Syntax Description

host-name	(Optional) DRP hostname.
ip-address	(Optional) DRP IP address.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(24)T	This command was removed.

Usage Guidelines

The **show ip director drp** command displays host-specific statistics, such as the number of queries received and the number of replies sent for a host.

Examples

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

```
Router# show ip director drp

DRP agent 172.21.34.2:
 14 requests, 6 replies, 4 requeries, 0 bad replies
 Supported Servers:
   172.21.34.10
   172.21.34.11
DRP agent 192.168.34.2:
 14 requests, 6 replies, 4 requeries, 0 bad replies
 Supported servers:
    192.168.34.10
```

show ip drp

To display information about the Director Response Protocol (DRP) Server Agent for DistributedDirector, use the **show ip drp** command in user EXEC or privileged EXEC mode.

show ip drp

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Examples

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

```
Router# show ip drp

Director Responder Protocol Agent is enabled
717 director requests, 712 successful lookups, 5 failures, 0 no route
Authentication is enabled, using "test" key-chain
```

Table 55 describes the significant fields shown in the display.

Table 55 show ip drp Field Descriptions

Field	Description
director requests	Number of DRP requests that have been received (including any using authentication key-chain encryption that failed).
successful lookups	Number of successful DRP lookups that produced responses.
failures	Number of DRP failures (for various reasons including authentication key-chain encryption failures).

Related Commands

Command	Description
ip drp access-group	Controls the sources of DRP queries to the DRP server agent.
ip drp authentication key-chain	Configures authentication on the DRP server agent for DistributedDirector.

show ip drp boomerang

To display the status of various boomerang domains, use the **show ip drp boomerang** command in privileged EXEC mode.

show ip drp boomerang [*domain-name*]

Syntax Description

domain-name	(Optional) Specified domain name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **show ip drp boomerang** command can be used on the boomerang client to display the status of the various boomerang domains. The following information can be shown for each domain:

- Alias information—The number of DNS requests for each alias.
- Content server address information:
  - Number of DNS requests.
  - Number of requests dropped because server is down.
  - Number of requests dropped because there is no original server.
  - Number of requests dropped because of security failures.

Examples

The following is sample output from the **show ip drp boomerang** command:

```
Router# show ip drp boomerang www.boom1.com

DNS packets with unknown domain 0

  Domain www.boom1.com
    Content server            172.16.101.101 up
    Origin server                    0.0.0.0
    DNS A record requests                  0
    Dropped (server down)                  0
    Dropped (no origen server)             0
    Security failures                      0

  Alias www.boom2.com
    DNS A record requests                  0
```

Related Commands

Command	Description
alias (boomerang configuration)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
server (boomerang configuration)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

show ip http client

To display a report about the HTTP client, use the **show ip http client** command in user EXEC or privileged EXEC mode.

show ip http client {**all** | **cache** | **connection** | **history** | **secure status** | **session-module** | **statistics**}

Syntax Description

all	Displays a report that contains all of the information available about the HTTP client: status (enabled or disabled), registered application or session modules, active connections, cache, history, and statistics.
cache	Displays a list of information about the HTTP client cache.
connection	Displays HTTP client active connections and configured values for connections.
history	Displays a list of up to 20 URLs most recently accessed by the HTTP client.
secure status	Displays the status of the secure HTTP client configuration. **Note** This keyword is not supported with Cisco IOS Release 12.2(31)SB2.
session-module	Displays a report about sessions or applications that have registered with the HTTP client.
statistics	No statistics are collected for the HTTP client. This feature will be implemented at a later date.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **all**, **cache**, and **statistics** keywords were added.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to display information about the HTTP client.

Note The secure HTTP (HTTPS) server is not supported in Cisco IOS Release 12.2(31)SB.

Examples

The following is sample output from the **show ip http client cache** command:

```
Router# show ip http client cache

HTTP client cache:
Maximum Memory size for cache    : 100000 bytes (default)
Maximum memory per cache entry   : 2000 bytes (default)
```

```
Memory used                     : 1381 bytes
Memory Available                : 98619 bytes
Cache Ager interval             : 5 minutes (default)
Total entries created           : 2
Id    Type    Url              Memory-size(Bytes)     Refcnt     Valid(Sec)
_____________________________________________________________________________
  536  Hdr   172.25.125.69/               673            0       -1
  32   Hdr   172.25.125.7:8888/            708            0       -1
```

The report is self-explanatory and lists information about the cache.

The following is sample output from the **show ip http client connection** command:

```
Router# show ip http client connection

HTTP client current connections:
    Persistent connection = enabled (default)
    Connection establishment timeout = 10s (default)
    Connection idle timeout = 30s (default)
    Maximum number of connection establishment retries = 1 (default)
    Maximum http client connections per host : 2
    HTTP secure client capability: Not present

    local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes
                          :80    172.20.67.174:11012 12584      176

    Total client connections : 1
```

The report is self-explanatory and lists the active connections and user-configured or default values for the connections.

The following is sample output from the **show ip http client history** command:

```
Router# show ip http client history

HTTP client history:
        GET 03:25:36 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
        GET 03:25:56 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
        GET 03:26:10 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
```

The report is self-explanatory and lists the most recent URLs accessed by the HTTP client.

The following is sample output from the **show ip http client secure status** command:

```
Router# show ip http client secure status

HTTP secure client ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure client trustpoint: TP-1
```

Table 56 describes the significant fields shown in the display.

Table 56 show ip http client secure status Field Descriptions

Field	Description
HTTP secure client ciphersuite	Displays the configuration of the **ip http client secure-ciphersuite** command.
HTTP secure client trustpoint	Displays the configuration of the **ip http client secure-trustpoint** command.

The following is sample output from the **show ip http client session-module** command:

```
Router# show ip http client session-module

HTTP client application session modules:
Id                :1
Application Name :HTTP CFS
Version           :HTTP/1.1
Persistent        :non-persistent
Response-timeout :0
Retries           :0
Proxy             :

Id                :6
Application Name :httpc_ifs_0
Version           :HTTP/1.1
Persistent        :non-persistent
Response-timeout :16
Retries           :0
Proxy             :
```

Table 57 describes the fields shown in the display.

Table 57 show ip http client session-module Field Descriptions

Field	Description
Id	A number that identifies the registering application. Every application or session that registers with the HTTP client is provided an identification number.
Application Name	Name of the application in use. Every application or session that registers with the HTTP client provides a name that is displayed by this field. In the sample output, HTTP CFS is the name for the HTTP Client File Session (CFS) application, and the name httpc_ifs_0 is the HTTP client (HTTPC) Cisco IOS File System (IFS) Copy application.
Version	HTTP protocol version supported by the application. Every application or session that registers with the HTTP client indicates the HTTP protocol version it supports in this field. HTTP 1.0 does not support persistent connections; HTTP 1.1 supports both persistent and nonpersistent connections.
Persistent	Value of the persistent connection. Persistent indicates that the application needs the HTTP client to maintain connection after data transfer from itself to the remote server. Nonpersistent indicates that the application does not need the HTTP client to maintain connections after the data transfer.
Response-timeout	Configured response timeout period, in seconds. The application specifies the amount of time the HTTP client has to wait for a response from the remote server before returning a failure notice, for those data transfers initiated by this application.
Retries	Configured connection retries. The application specifies the number of retries for establishing connection that the HTTP client must attempt before returning a failure notice to the application.
Proxy	Specifies a proxy name that the HTTP client uses to route all HTTP data transfer requests to or from the application.

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.

show ip http client connection

To display a report about HTTP client active connections, use the **show ip http client connection** command in privileged EXEC mode.

show ip http client connection

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to display active connections and configured values for connections.

Examples

The following is sample output from the **show ip http client connection** command:

```
Router# show ip http client connection

HTTP client current connections:
    Persistent connection = enabled (default)
    Connection establishment timeout = 10s (default)
    Connection idle timeout = 30s (default)
    Maximum number of connection establishment retries = 1 (default)
    Maximum http client connections per host : 2
    HTTP secure client capability: Not present

    local-ipaddress:port  remote-ipaddress:port in-bytes   out-bytes
                          :80    172.20.67.174:11012 12584      176

    Total client connections : 1
```

The report is self-explanatory and lists the active connections and user-configured or default values for the connections.

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.

Command	Description
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client history	Displays the URLs accessed by the HTTP client.
show ip http client session-module	Displays a report about sessions that have registered with the HTTP client.

show ip http client cookie

To display the HTTP client cookies, use the **show ip http client cookie** command in privileged EXEC mode.

show ip http client cookie {**brief** | **summary**} [**domain** *cookie-domain* | **name** *cookie-name* | **session** *session-name*]

Syntax Description

brief	Displays a brief summary of client cookies.
summary	Displays a detailed summary of client cookies.
domain	(Optional) Displays all cookies in a domain
cookie-domain	(Optional) Client cookie domain or host name.
name	(Optional) Displays cookies matching a specific name.
cookie-name	(Optional) Client cookie name.
session	(Optional) Displays cookies specific to a client session.
session-name	(Optional) Client session name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is example output from the **show ip http client cookie brief** command:

```
Device# show ip http client cookie brief

HTTP client cookies of session HTTP CFS :
HTTP client cookies of session CWMP_CLIENT :
For expanded output please use 'summary' option for display
Name            Value                           Ver     Domain
Path
cookie8          8                              1       172.17.0.2
/cwmp-1-0/
cookie7          7                              1       172.17.0.2
/cwmp-1-0/
cookie3          3                              1       172.16.0.2
/cwmp-1-0/
cookie2          2                              1       172.16.0.2
/cwmp-1-0/
cookie1          1                              1       172.16.0.2
/cwmp-1-0/
HTTP client cookies of session cwmp_test_client :
```

The following is example output from the **show ip http client cookie brief domain** command:

```
Device# show ip http client cookie brief domain 172.16.0.2
HTTP client cookies of domain 172.16.0.2 :
For expanded output please use 'summary' option for display
```

```
Name            Value                           Ver     Domain
Path
cookie3          3                              1       172.16.0.2
/cwmp-1-0/
cookie2          2                              1       172.16.0.2
/cwmp-1-0/
cookie1          1                              1       172.16.0.2
/cwmp-1-0/
```

The following is example output from the **show ip http client cookie brief name** command:

```
Device# show ip http client cookie brief name cookie3
HTTP client cookies of name cookie3 :
For expanded output please use 'summary' option for display
Name            Value                           Ver     Domain
Path
cookie3          3                              1       172.16.0.2
/cwmp-1-0/
```

The following is example output from the **show ip http client cookie brief session** command:

```
Device# show ip http client cookie brief session CWMP_CLIENT
HTTP client cookies of session CWMP_CLIENT :
For expanded output please use 'summary' option for display
Name            Value                           Ver     Domain
Path
cookie8          8                              1       172.17.0.2
/cwmp-1-0/
cookie7          7                              1       172.17.0.2
/cwmp-1-0/
cookie3          3                              1       172.16.0.2
/cwmp-1-0/
cookie2          2                              1       172.16.0.2
/cwmp-1-0/
cookie1          1                              1       172.16.0.2
/cwmp-1-0/
```

The following is example output from the **show ip http client cookie summary** command:

```
Device# show ip http client cookie summary

HTTP client cookies of session HTTP CFS :
HTTP client cookies of session CWMP_CLIENT :

Name          : cookie8
Value         :  8
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :

Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
```

```
Name          : cookie3
Value         :  3
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :

Name          : cookie2
Value         :  2
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :

Name          : cookie1
Value         :  1
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
HTTP client cookies of session cwmp_test_client :
```

The following is example output from the **show ip http client cookie summary domain** command:

```
Device# show ip http client cookie summary domain 172.17.0.2

HTTP client cookies of domain 172.17.0.2 :

Name          : cookie8
Value         :  8
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :

Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
```

The following is example output from the **show ip http client cookie summary name** command:

```
Device# show ip http client cookie summary name cookie7

HTTP client cookies of name cookie7 :

Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
```

The following is example output from the **show ip http client cookie summary session** command:

```
Device# show ip http client cookie summary session CWMP_CLIENT

HTTP client cookies of session CWMP_CLIENT :

Name          : cookie8
Value         :  8
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :

Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :

Name          : cookie3
Value         :  3
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :

Name          : cookie2
Value         :  2
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
```

```
Comment       :
CommentURL    :

Name          : cookie1
Value         :  1
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
```

show ip http client history

To display up to 20 URLs accessed by the HTTP client, use the **show ip http client history** command in privileged EXEC mode.

show ip http client history

Syntax Description

This command has no arguments or keywords

Defaults

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command displays a list of up to 20 URLs most recently accessed by the HTTP client.

Examples

The following is sample output from the **show ip http client history** command:

```
Router# show ip http client history

HTTP client history:
        GET 03:25:36 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
        GET 03:25:56 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
        GET 03:26:10 UTC Thu Feb 26 2004
mailer.cisco.com/mailer.html
```

The report is self-explanatory and lists the most recent URLs accessed by the HTTP client.

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.

Command	Description
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client connection	Displays a report about HTTP client active connections.
show ip http client session-module	Displays a report about sessions that have registered with the HTTP client.

show ip http client secure status

To display the status of the secure HTTP client configuration, use the **show ip http client secure status** command in privileged EXEC mode.

show ip http client secure status

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show ip http client secure status** command:

```
Router# show ip http client secure status

HTTP secure client ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure client trustpoint: TP-1
```

Table 58 describes the significant fields shown in the display.

Table 58 show ip http client secure status Field Descriptions

Field	Description
HTTP secure client ciphersuite:	Displays the configuration of the **ip http client secure-ciphersuite** command.
HTTP secure client trustpoint:	Displays the configuration of the **ip http client secure-trustpoint** command.

Related Commands

Command	Description
ip http client secure-ciphersuite	Specifies the CipherSuites that should be used for encryption over the secure HTTP connection from the client to a remote server.
ip http client secure-trustpoint	Specifies the CA trustpoint that should be used if the remote HTTP server requests client authentication.

show ip http client session-module

To display a report about sessions or applications that have registered with the HTTP client, use the **show ip http client session-module** command in privileged EXEC mode.

show ip http client session-module

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to display information about applications that have registered with the HTTP client.

Examples

The following is sample output from the **show ip http client session-module** command:

```
Router# show ip http client session-module

HTTP client application session modules:
Id                :1
Application Name :HTTP CFS
Version           :HTTP/1.0
Persistent        :non-persistent
Response-timeout :0
Retries           :0
Proxy             :

Id                :6
Application Name :httpc_ifs_0
Version           :HTTP/1.1
Persistent        :non-persistent
Response-timeout :16
Retries           :0
Proxy             :
```

Table 59 describes the fields shown in the display.

Table 59 show ip http client session-module Field Descriptions

Field	Description
Id	A number that identifies the registering application. Every application or session that registers with the HTTP client is provided an identification number.
Application Name	Name of the application in use. Every application or session that registers with the HTTP client provides a name that is displayed by this field. In the sample output, HTTP CFS is the name for the HTTP Client File Session application, and the name httpc_ifs_0 is the HTTPC IFS Copy application.
Version	HTTP protocol version supported by the application. Every application or session that registers with the HTTP client indicates the HTTP protocol version it supports in this field. HTTP1.0 does not support persistent connections; HTTP1.1 supports both persistent and nonpersistent connections.
Persistent	Value of the persistent connection. Persistent indicates that the application needs the HTTP client to maintain connection after data transfer from itself to the remote server. Nonpersistent indicates that the application does not need the HTTP client to maintain connections after the data transfer.
Response-timeout	Configured response timeout period, in seconds. The application specifies the amount of time the HTTP Client has to wait for a response from the remote server before returning a failure notice, for those data transfers initiated by this application.
Retries	Configured connection retries. The application specifies the number of retries for establishing connection that the HTTP client must attempt before returning a failure notice to the application.
Proxy	Specifies a proxy name that the HTTP client uses to route all HTTP data transfer requests to or from the application.

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client connection	Displays a report about HTTP client active connections.
show ip http client history	Displays the URLs accessed by the HTTP client.

show ip http help-path

To display the current complete configured path of help files for use by the user's current GUI screen, use the **show ip http help-path** command in user EXEC or privileged EXEC mode.

show ip http help-path

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

Use this command to display the current complete help path configured in the HTTP server. This path is expected to hold help files relating to the user's current GUI screen.

Examples

The following is sample output from the **show ip http help-path** command:

```
Router# show ip http help-path

http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
```

Related Commands

Command	Description
ip http help-path	Configures the HTTP help-root URL.

show ip http server

To display details about the current configuration of the HTTP server, use the **show ip http server** command in user EXEC or privileged EXEC mode.

show ip http server {**all** | **status** | **session-module** | **connection** | **statistics** | **history**}

Syntax Description

all	Displays all HTTP server information.
status	Displays only HTTP server status configuration.
session-module	Displays only supported HTTP services (Cisco IOS modules).
connection	Displays only the current connections to the HTTP server, including the local and remote IP addresses being accessed.
statistics	Displays only HTTP server connection statistics.
history	Displays only the previous 20 connections to the HTTP server, including the IP address accessed, and the time when the connection was closed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to show detailed status information about the HTTP server.

If the HTTP secure server capability is present, the output of the **show ip http server all** command will also include the information found in the output of the **show ip http server secure status** command.

Note The secure HTTP (HTTPS) server is not supported in Cisco IOS Release 12.2(31)SB.

Examples

The following is sample output from the **show ip http server all** command:

```
Router# show ip http server all

HTTP server status: Enabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 30 seconds
Server life time-out: 120 seconds
```

```
Maximum number of requests allowed on a connection: 2
HTTP secure server capability: Not Present
HTTP server application session modules:
 Session module Name  Handle  Description
Homepage_Server       5       IOS Homepage Server
QDM                   2       QOS Device Manager Server
HTTP IFS Server       1       HTTP based IOS File Server
QDM SA                3       QOS Device Manager Signed Applet Server
WEB_EXEC              4       HTTP based IOS EXEC Server
XSM                   6       XML Session Manager
VDM                   7       VPN Device Manager Server
ITS                   8       IOS Telephony Service
ITS_LOCDIR            9       ITS Local Directory Search

HTTP server current connections:
local-ipaddress:port   remote-ipaddress:port in-bytes  out-bytes
  172.19.254.37:80     192.168.254.45:33737  70        2294

HTTP server statistics:
Accepted connections total: 1360

HTTP server history:
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes  end-time
  172.19.254.37:80     192.168.254.45:63530  60        1596       10:50:00 12/19
```

Table 60 describes the significant fields shown in the display.

Table 60 show ip http server Field Descriptions

Field	Description
HTTP server status:	Enabled or disabled. Corresponds to the [**no**] **ip http server** command.
HTTP server port:	Port used by the HTTP server. Corresponds to the **ip http port** command.
HTTP server authentication method:	Authentication method used for HTTP server logins. Corresponds to the **ip http authentication** command.
HTTP server access class:	Access list number assigned to the HTTP server. A value of zero (0) indicates no access list is assigned. Corresponds to the **ip http access-class** command.
HTTP server base path:	Base HTTP path specifying the location of the HTTP server files (HTML files). Corresponds to the **ip http path** command.
Maximum number of concurrent server connections allowed:	Corresponds to the **ip http max-connections** command.
Server idle time-out:	The maximum number of seconds the connection will be kept open if no data is received or if response data can not be sent out. Corresponds to the **ip http timeout-policy** command.
Server life time-out:	The maximum number of seconds the connection will be kept open. Corresponds to the **ip http timeout-policy** command.
Maximum number of requests allowed on a connection:	The maximum number of requests that will be processed on a connection before the connection is closed. Corresponds to the **ip http timeout-policy** command.

Table 60 show ip http server Field Descriptions (continued)

Field	Description
HTTP secure server capability:	Indicates if the running software image supports the secure HTTP server ("Present" or "Not Present"). If the capability is present, the output from the **show ip http server secure status** command will appear after this line.
HTTP server application session modules:	Cisco IOS services that use the HTTP server. Services are provided for application interfaces, including: • The Cisco Web browser user interface, which uses the Cisco IOS Homepage Server, HTTP-based EXEC Server, and HTTP IOS File System (IFS) Server • The VPN Device Manager (VDM) application, which uses the VDM Server and the XML Session Manager (XSM) • The QoS Device Manager (QDM) application, which uses the QDM Server • The IP Phone and Cisco IOS Telephony Service applications, which use the ITS Local Directory Search and IOS Telephony Server (ITS) **Note** The IP Phone and Telephony Service applications use the ITS Local Directory Search and IOS Telephony Server (ITS). Therefore, these two applications are not supported with Cisco IOS Release 12.2(31)SB2.
HTTP server current connections:	Currently active HTTP connections.
HTTP server statistics:	How many connections have been accepted.
HTTP server history:	Details about the last 20 connections, including the time the connection was closed (endtime). Endtime is given in Universal Coordinated Time (UTC or GMT), using a 24-hour clock and the following format: *hh*:*mm*:*ss month*/*day*

The following example shows sample output for the **show ip http server status** command:

```
Router# show ip http server status

HTTP server status: Disabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 600 seconds
Server life time-out: 600 seconds
Maximum number of requests allowed on a connection: 1
HTTP secure server capability: Present
HTTP secure server status: Disabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
```

The lines indicating the status of the HTTP secure (HTTPS) server will only be visible if your software image supports the HTTPS server. If your software image does not support SSL, only the following line will be visible:

HTTP secure server capability: Not present

Related Commands

Command	Description
debug ip http server all	Enables debugging output for all HTTP processes on the system.
ip http secure-server	Enables the HTTPS server.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.
show ip http server secure status	Displays the status of the HTTPS server.

show ip http server secure status

To display the status of the HTTP secure server configuration, use the **show ip http server secure status** command in privileged EXEC mode.

show ip http server secure status

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following is sample output from the **show ip http server secure status** command:

```
Router# show ip http server secure status

HTTP secure server status: Enabled
HTTP secure server port: 1025
HTTP secure server ciphersuite: rc4-128-sha rc4-128-md5
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

Table 61 describes the significant fields shown in the display.

Table 61 show ip http server secure status Field Descriptions

Field	Description
HTTP secure server status:	Displays the state of secure HTTP server (“Enabled” or “Disabled”). Corresponds to the configuration of the **ip http secure-server** command.
HTTP secure server port:	Displays the configuration of the **ip http secure-port** command.
HTTP secure server ciphersuite:	Displays the configuration of the **ip http secure-ciphersuite** command.

Table 61 show ip http server secure status Field Descriptions (continued)

Field	Description
HTTP secure server client authentication:	Displays the configuration of the **ip http secure-client-auth** command.
HTTP secure server trustpoint:	Displays the configuration of the **ip http secure-trustpoint** command. If no trustpoint is configured, the line will appear blank after the colon.

Related Commands

Command	Description
ip http secure-ciphersuite	Specifies the CipherSuites that should be used for encryption over the secure HTTP connection from the server to a remote client.
ip http secure-client-auth	Configures the HTTP server to authenticate the remote client during the connection process.
ip http secure-port	Specifies the port (socket) to be used for HTTPS connections.
ip http secure-server	Enables the HTTPS server.
ip http secure-trustpoint	Specifies the CA trustpoint that should be used for obtaining signed certificates for the secure HTTP server.

show kron schedule

To display the status and schedule information of Command Scheduler occurrences, use the **show kron schedule** command in user EXEC or privileged EXEC mode.

show kron schedule

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **show kron schedule** command to view all currently configured occurrences and when they are next scheduled to run.

Examples

The following sample output displays each configured policy name and the time interval before the policy is scheduled to run:

```
Router# show kron schedule

Kron Occurrence Schedule
week inactive, will run again in 7 days 01:02:33
may inactive, will run once in 32 days 20:43:31 at 6:30 on Jun 20
```

Table 62 describes the significant fields shown in the display.

Table 62 show kron schedule Field Descriptions

Field	Description
week inactive	The policy list named week is currently inactive.
run again in 7 days 01:02:33	Time in days, hours, minutes and seconds before the policy will run. This policy is scheduled to run on a recurring basis.
run once in 32 days 20:43:31	Time in days, hours, minutes and seconds before the policy will run. This policy is scheduled to run just once.

Related Commands

Command	Description
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.

show link monitor debug

To display the statistics of an executing process while link monitoring is enabled, use the **show link monitor debug** command in privileged EXEC mode.

show link monitor debug

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command for debugging various conditions occurring during the monitoring process.

Examples

The following example shows output of the **show link monitor debug** command:

```
Router# show link monitor debug

Link Monitor Error Statistics

CONF STRUCTURE FOUND NULL.............0
CONF STRUCTURE MALLOC FAIL............0
IPC SENT TOTAL........................25
IPC RECV TOTAL........................3
CCB CMD SENT TOTAL....................94
LOVE LETTER RECV TOTAL................1
IPC SEND FAILURE......................1
IPC RECV FAILURE......................0
CCB CMD SEND FAILURE..................0
LOVE LETTER RECV FAILURE..............0
CONFIG RESEND TO LC FAIL..............0
CHUNK ELEMENT FREE FAIL...............0
CHUNK ELEMENT MALLOC FAIL.............0
ELEMENTS IN TRAP QUEUE................0
TRAP FAIL ENQUEUE.....................0
WATCHED QUEUE CREATED
CHUNK CREATED
```

The route/switch processor (RSP) and versatile interface processors (VIPs) communicate via Inter-Process Communication (IPC) messages.

The RSP sends messages to the fast serial interface processor (FSIP) via command control block (CCB) commands.

The FSIP sends messages to the RSP via Loveletter messages.

Table 63 describes the significant fields shown in the display.

Table 63 show link monitor debug Field Descriptions

CONF STRUCTURE FOUND NULL	Number of times the link monitor sub-block was NULL.
CONF STRUCTURE MALLOC FAIL	Number of times memory for the link monitor sub-block structure was unable to be allocated.
IPC SENT TOTAL	Number of IPC messages sent.
IPC RECV TOTAL	Number of IPC messages received.
CCB CMD SENT TOTAL	Number of CCB commands sent by the RSP.
LOVE LETTER RECV TOTAL	Number of Loveletter messages received by the RSP.
IPC SEND FAILURE	• Error sending message. Could not get buffer and failed to send IPC message to the VIP. • Failed to get an IPC port for sending a message to the line card.
IPC RECV FAILURE	Number of IPC messages received that are null.
CCB CMD SEND FAILURE	Number of CCB commands not sent to the VIP.
LOVE LETTER RECV FAILURE	Error receiving love note.
CONFIG RESEND TO LC FAIL	Number of times the configuration resend to the line card failed.
CHUNK ELEMENT FREE FAIL	Number of chunk elements that were not freed properly.
CHUNK ELEMENT MALLOC FAIL	Number of chunk element requests that were rejected. This is also the number of traps that were dropped.
ELEMENTS IN TRAP QUEUE	Number of traps that are currently in the link monitor queue (waiting to be sent).
TRAP FAIL ENQUEUE	Number traps that were not in the link monitor queue. Traps that are not in the queue are dropped.
WATCHED QUEUE CREATED	Indicates whether the link monitor queue is created. If it is not created, traps are not sent.
CHUNK CREATED	Indicates whether the chunk of memory is created. If it is not created, traps are not sent.

show logging

To display the state of system logging (syslog) and the contents of the standard system logging buffer, use the **show logging** command in privileged EXEC mode.

show logging [**slot** *slot-number* | **summary**]

Syntax Description

slot *slot-number*	(Optional) Displays information in the syslog history table for a specific line card. Slot numbers range from 0 to 11 for the Cisco 12012 Internet router and 0 to 7 for the Cisco 12008 Internet router.
summary	(Optional) Displays counts of messages by type for each line card.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
11.2 GS	This command was modified. The **slot** and **summary** keywords were added for the Cisco 12000.
12.2(8)T	This command was modified. Command output was expanded to show the status of the logging count facility (“Count and time-stamp logging messages”).
12.2(15)T	This command was modified. Command output was expanded to show the status of XML syslog formatting.
12.3(2)T	This command was modified. Command output was expanded (on supported software images) to show details about the status of system logging processed through the Embedded Syslog Manager (ESM). These lines appear as references to “filtering” or “filter modules”.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was modified. Command-line interface (CLI) output was modified to show message discriminators defined at the router and syslog sessions associated with those message discriminators.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI1	This command was modified. Support for the command in the user EXEC mode was removed.

Usage Guidelines

This command runs on the privileged EXEC mode. To enter the privileged EXEC mode, type **enable** in the user EXEC mode and press Enter. Provide a password, if prompted.

This command displays the state of syslog error and event logging, including host addresses, and which logging destinations (console, monitor, buffer, or host) logging is enabled. This command also displays Simple Network Management Protocol (SNMP) logging configuration parameters and protocol activity.

This command will also display the contents of the standard system logging buffer, if logging to the buffer is enabled. Logging to the buffer is enabled or disabled using the [**no**] **logging buffered** command. The number of system error and debugging messages in the system logging buffer is determined by the configured size of the syslog buffer. This size of the syslog buffer is also set using the **logging buffered** command.

To enable and set the format for syslog message time stamping, use the **service timestamps log** command.

If debugging is enabled (using any **debug** command), and the logging buffer is configured to include level 7 (debugging) messages, debug output will be included in the system log. Debugging output is not formatted like system error messages and will not be preceded by the percent symbol (%).

Examples

The following is sample output from the **show logging** command on a software image that supports the Embedded Syslog Manager (ESM) feature:

```
Router> enable
Router# show logging

Syslog logging: enabled (10 messages dropped, 5 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 31 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: disabled
    Buffer logging: level errors, 36 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (8192 bytes)
    Count and timestamp logging messages: disabled

No active filter modules.


    Trap logging: level informational, 45 message lines logged

Log Buffer (8192 bytes):
```

The following example shows output from the **show logging** command after a message discriminator has been configured. Included in this example is the command to configure the message discriminator.

```
Router(config)# logging discriminator ATTFLTR1 severity includes 1,2,5 rate-limit 100

Specified MD by the name ATTFLTR1 is not found.
Adding new MD instance with specified MD attribute values.

Router(config)# end
Router#

000036: *Oct 20 16:26:04.570: %SYS-5-CONFIG_I: Configured from console by console

Router> enable
Router# show logging

Syslog logging: enabled (11 messages dropped, 0 messages rate-limited,
    0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.
```

```
Inactive Message Discriminator:
ATTFLTR1  severity group includes 1,2,5
    rate-limit not to exceed 100 messages per second

Console logging: level debugging, 25 messages logged, xml disabled, filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging:  level debugging, 25 messages logged, xml disabled, filtering disabled
Logging Exception size (8192 bytes)
Count and timestamp logging messages: disabled

No active filter modules.

Trap logging: level debugging, 28 message lines logged
Logging to 172.25.126.15  (udp port 1300,  audit disabled, authentication disabled,
    encryption disabled, link up),
    28 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled
Logging to 172.25.126.15  (tcp port 1307,  audit disabled, authentication disabled,
    encryption disabled, link up),
    28 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled, filtering disabled
Logging to 172.20.1.1  (udp port 514,  audit disabled,
    authentication disabled, encryption disabled, link up),
    28 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled

Log Buffer (1000000 bytes):
```

Table 64 describes the significant fields shown in the output for the two preceding examples.

Table 64 show logging Field Descriptions

Field	Description
Syslog logging:	Shows general state of system logging (enabled or disabled), the status of logged messages (number of messages dropped, rate-limited, or flushed), and whether XML formatting or ESM filtering is enabled.
No Active Message Discriminator	Indicates that a message discriminator is not being used.
Inactive Message Discriminator:	Identifies a configured message discriminator that has not been invoked.
Console logging:	Logging to the console port. Shows “disabled” or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. Corresponds to the configuration of the **logging console**, **logging console xml**, or **logging console filtered** command.

Table 64 show logging Field Descriptions (continued)

Field	Description
Monitor logging:	Logging to the monitor (all TTY lines). Shows "disabled" or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. Corresponds to the configuration of the **logging monitor**, **logging monitor xml**, or **logging monitor filtered** command.
Buffer logging:	Logging to the standard syslog buffer. Shows "disabled" or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. Corresponds to the configuration of the **logging buffered**, **logging buffered xml**, or **logging buffered filtered** command.
Trap logging:	Logging to a remote host (syslog collector). Shows "disabled" or, if enabled, the severity level limit, number of messages logged, and whether XML formatting or ESM filtering is enabled. (The word "trap" means a trigger in the system software for sending error messages to a remote host.) Corresponds to the configuration of the **logging host** command. The severity level limit is set using the **logging trap** command.
SNMP logging	Displays whether SNMP logging is enabled, the number of messages logged, and the retransmission interval. If not shown on your platform, use the **show logging history** command.
Logging Exception size (8192 bytes)	Corresponds to the configuration of the **logging exception** command.
Count and timestamp logging messages:	Corresponds to the configuration of the **logging count** command.
No active filter modules.	Appears if no syslog filter modules are configured with the **logging filter** command. Syslog filter modules are Tcl script files used when the Embedded Syslog Manager (ESM) is enabled. ESM is enabled when any of the **filtered** keywords are used in the logging commands. If configured, the URL and filename of configured syslog filter modules will appear at this position in the output. Syslog filter modules are executed in the order in which they appear here.
Log Buffer (8192 bytes):	The value in parentheses corresponds to the configuration of the **logging buffered** *buffer-size* command. If no messages are currently in the buffer, the output ends with this line. If messages are stored in the syslog buffer, they appear after this line.

The following example shows that syslog messages from the system buffer are included, with time stamps. In this example, the software image does not support XML formatting or ESM filtering of syslog messages.

```
Router> enable
Router# show logging

Syslog logging:enabled (2 messages dropped, 0 flushes, 0 overruns)
```

```
    Console logging:disabled
    Monitor logging:level debugging, 0 messages logged
    Buffer logging:level debugging, 4104 messages logged
    Trap logging:level debugging, 4119 message lines logged
        Logging to 192.168.111.14, 4119 message lines logged
Log Buffer (262144 bytes):

Jul 11 12:17:49 EDT:%BGP-4-MAXPFX:No. of prefix received from 209.165.200.225
(afi 0) reaches 24, max 24
! THE FOLLOWING LINE IS A DEBUG MESSAGE FROM NTP.
! NOTE THAT IT IS NOT PRECEEDED BY THE % SYMBOL.
Jul 11 12:17:48 EDT: NTP: Maxslew = 213866
Jul 11 15:15:41 EDT:%SYS-5-CONFIG:Configured from
tftp://host.com/addc5505-rsm.nyiix
.Jul 11 15:30:28 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Up
.Jul 11 15:31:34 EDT:%BGP-3-MAXPFXEXCEED:No. of prefix received from
209.165.200.226 (afi 0):16444 exceed limit 375
.Jul 11 15:31:34 EDT:%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Down BGP
Notification sent
.Jul 11 15:31:34 EDT:%BGP-3-NOTIFICATION:sent to neighbor 209.165.200.226 3/1
(update malformed) 0 bytes
 .
 .
 .
```

The software clock keeps an "authoritative" flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the "authoritative" flag is set, the flag prevents peers from synchronizing to the software clock.

Table 65 describes the symbols that precede the time stamp.

Table 65 Time Stamping Symbols for syslog Messages

Symbol	Description	Example
*	Time is not authoritative: the software clock is not in sync or has never been set.	*15:29:03.158 UTC Tue Feb 25 2003:
(blank)	Time is authoritative: the software clock is in sync or has just been set manually.	15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers.	.15:29:03.158 UTC Tue Feb 25 2003:

The following is sample output from the **show logging summary** command for a Cisco 12012 router. A number in the column indicates that the syslog contains that many messages for the line card. For example, the line card in slot 9 has 1 error message, 4 warning messages, and 47 notification messages.

Note For similar log counting on other platforms, use the **show logging count** command.

```
Router> enable
Router# show logging summary

+-----+-------+-------+-------+-------+-------+-------+-------+-------+
 SLOT | EMERG | ALERT | CRIT  | ERROR |WARNING| NOTICE| INFO  | DEBUG |
```

```
+-----+-------+-------+-------+-------+-------+-------+-------+-------+
|* 0* |     . |     . |     . |     . |     . |     . |     . |     . |
|  1  |       |       |       |       |       |       |       |       |
|  2  |       |       |       |     1 |     4 |    45 |       |       |
|  3  |       |       |       |       |       |       |       |       |
|  4  |       |       |       |     5 |     4 |    54 |       |       |
|  5  |       |       |       |       |       |       |       |       |
|  6  |       |       |       |       |       |       |       |       |
|  7  |       |       |       |    17 |     4 |    48 |       |       |
|  8  |       |       |       |       |       |       |       |       |
|  9  |       |       |       |     1 |     4 |    47 |       |       |
| 10  |       |       |       |       |       |       |       |       |
| 11  |       |       |       |    12 |     4 |    65 |       |       |
+-----+-------+-------+-------+-------+-------+-------+-------+-------+
```

Table 66 describes the logging level fields shown in the display.

Table 66 show logging summary Field Descriptions

Field	Description
SLOT	Indicates the slot number of the line card. An asterisk next to the slot number indicates the GRP card whose error message counts are not displayed. For information on the GRP card, use the **show logging** command.
EMERG	Indicates that the system is unusable.
ALERT	Indicates that immediate action is needed.
CRIT	Indicates a critical condition.
ERROR	Indicates an error condition.
WARNING	Indicates a warning condition.
NOTICE	Indicates a normal but significant condition.
INFO	Indicates an informational message only.
DEBUG	Indicates a debugging message.

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging count	Enables the error log count capability.
logging history size	Changes the number of syslog messages stored in the history table of the router.
logging linecard	Logs messages to an internal buffer on a line card and limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above level.
service timestamps	Configures the system to time-stamp debugging or logging messages.
show logging count	Displays a summary of system error messages (syslog messages) by facility and severity.
show logging xml	Displays the state of system logging and the contents of the XML-specific logging buffer.

show logging onboard (Cat 6K)

To display onboard failure logs (OBFL) on Cisco Catalyst 6000 series switches, use the **show logging onboard** command in privileged EXEC mode.

show logging onboard module *slot-number* [**environment | interrupt | message | temperature | uptime**] [**continuous | detail | raw | summary**] [**start** *start-time-and-date*] [**end** *end-time-and-date*] [**status**]

Syntax Description

module *slot-number*	Displays the module and the slot number. Valid slot values vary depending on the type of chassis used.
environment	(Optional) Displays the environment of the application.
interrupt	(Optional) Displays the application interruption.
message	(Optional) Displays system messages collected at the level set by the **hw-module logging onboard** global configuration command.
temperature	(Optional) Displays temperature data.
uptime	(Optional) Displays system uptime data.
continuous	(Optional) Displays continuously collected data. This can be used with the **environment**, **interrupt**, **message**, **temperature**, and **uptime** keywords.
detail	(Optional) Displays both the summary and the continuously collected data. This keyword can be used with the **environment**, **interrupt**, **message**, **temperature**, and **uptime** keywords.
raw	(Optional) Displays the logging raw information.
summary	(Optional) Displays summary data.
start *start-time-and-date* **end** *end-time-and-date*	(Optional) Specifies the start and end time for **interrupt**, **message**, **raw**, **temperature**, and **uptime** reports. You can optionally use the **start** and **end** keywords with the **continuous** and **detail** keywords. The **start** and **end** keywords prompt for the time in 24-hour format (hh:mm:ss) followed by the date, the month in three-letter format (Jun for June, as an example), and the year in the range 1993 to 2035. Examples: start 15:01:57 7 Mar 2007 end 15:04:57 14 Mar 2007
status	(Optional) Displays the platform and CLI enable status for each of the test applications (system message, interrupt, temperature, and uptime).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

The **show logging onboard** command can be entered without any keywords, which is the same as entering the **show logging onboard summary** command to display summarized information about OBFL for the device residing on the same module where the command is entered.

Use this command to view OBFL data from system hardware. The OBFL feature is enabled by default and records operating temperatures, hardware uptime, interrupts, and other important events and messages that can assist with diagnosing problems with hardware cards (or *modules*) installed in a Cisco router or switch. Data is logged to files stored in nonvolatile memory. When the onboard hardware is started up, a first record is made for each area monitored and becomes a base value for subsequent records.

The OBFL feature provides a circular updating scheme for collecting continuous records and archiving older (historical) records, ensuring accurate data about the system. Data is recorded in one of two formats: continuous information that displays a snapshot of measurements and samples in a continuous file, and summary information that provides details about the data being collected. The message "No historical data to display" is seen when historical data is not available.

See the examples for more information about the type of data collected.

Examples

Temperature

Temperatures surrounding hardware modules can exceed recommended safe operating ranges and cause system problems such as packet drops. Higher than recommended operating temperatures can also accelerate component degradation and affect device reliability. Monitoring temperatures is important for maintaining environmental control and system reliability. Once a temperature sample is logged, the sample becomes the base value for the next record. From that point on, temperatures are recorded either when there are changes from the previous record or if the maximum storage time is exceeded. Temperatures are measured and recorded in degrees Celsius.

The following example shows how you might enter this command:

```
Router# show logging onboard module 2 temperature detail

--------------------------------------------------------------------------------
TEMPERATURE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Number of sensors          : 12
Sampling frequency         : 5 minutes
Maximum time of storage    : 120 minutes
--------------------------------------------------------------------------------
Sensor                            |   ID   | Maximum Temperature 0C
--------------------------------------------------------------------------------
MB-Out                              980201     43
MB-In                               980202     28
MB                                  980203     29
MB                                  980204     38
EARL-Out                            910201     0
EARL-In                             910202     0
SSA 1                               980301     38
SSA 2                               980302     36
JANUS 1                             980303     36
JANUS 2                             980304     35
GEMINI 1                            980305     0
GEMINI 2                            980306     0
-----------------------------------------------------------------
Temp                          Sensor ID
0C     1    2    3    4    5    6    7    8    9   10   11   12
-----------------------------------------------------------------
No historical data to display
-----------------------------------------------------------------
```

```
--------------------------------------------------------------------------------
TEMPERATURE CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Sensor                              |   ID  |
--------------------------------------------------------------------------------
MB-Out                                980201
MB-In                                 980202
MB                                    980203
MB                                    980204
EARL-Out                              910201
EARL-In                               910202
SSA 1                                 980301
SSA 2                                 980302
JANUS 1                               980303
JANUS 2                               980304
GEMINI 1                              980305
GEMINI 2                              980306

--------------------------------------------------------------------------------
       Time Stamp    |Sensor Temperature 0C
MM/DD/YYYY HH:MM:SS |  1    2    3    4    5    6    7    8    9   10   11   12
--------------------------------------------------------------------------------
03/06/2007 22:32:51   31   26   27   27   NA   NA   33   32   30   29   NA   NA
03/06/2007 22:37:51   43   28   29   38   NA   NA   38   36   36   35   NA   NA
--------------------------------------------------------------------------------
```

Table 67 describes the significant fields shown in the display.

Table 67 Temperature Summary Descriptions

Field	Description
Number of sensors	The total number of temperature sensors that will be recorded. A column for each sensor is displayed with temperatures listed under the number of each sensor, as available.
Sampling frequency	The time between measurements.
Maximum time of storage	Determines the maximum amount of time, in minutes, that can pass when the temperature remains unchanged and the data is not saved to storage media. After this time, a temperature record will be saved even if the temperature has not changed.
Sensor column	Lists the name of the sensor.
ID column	Lists an assigned identifier for the sensor.
Maximum Temperature 0C	Shows the highest recorded temperature per sensor.
Temp	Indicates a recorded temperature in degrees Celsius in the historical record. Columns following show the total time each sensor has recorded that temperature.
Sensor ID	An assigned number, so that temperatures for the same sensor can be stored together.
offset	Relative time of peer clock to local clock (in milliseconds).
disp	Dispersion

Operational Uptime

The operational uptime tracking begins when the module is powered on, and information is retained for the life of the module.

The following example shows how you might enter this command:

```
Router# show logging onboard module 2 uptime detail

--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
First customer power on : 03/06/2007 22:32:51
Total uptime            :   0 years   0 weeks   2 days  18 hours  10 minutes
Total downtime          :   0 years   0 weeks   0 days   8 hours   7 minutes
Number of resets        : 130
Number of slot changes  : 16
Current reset reason    : 0xA1
Current reset timestamp : 03/07/2007 13:29:07
Current slot            : 2
Current uptime          :   0 years   0 weeks   1 days   7 hours   0 minutes
--------------------------------------------------------------------------------
Reset  |        |
Reason | Count  |
--------------------------------------------------------------------------------
0x5         64
0x6         62
0xA1         4
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Time Stamp          | Reset  | Uptime
MM/DD/YYYY HH:MM:SS | Reason | years weeks days hours  minutes
--------------------------------------------------------------------------------
03/06/2007 22:32:51   0xA1      0     0     0     0     0
--------------------------------------------------------------------------------
```

The operational uptime application tracks the following events:

- Date and time the customer first powered on a component.
- Total uptime and downtime for the component in years, weeks, days, hours, and minutes.
- Total number of component resets.
- Total number of slot (module) changes.
- Current reset timestamp to include the date and time.
- Current slot (module) number of the component.
- Current uptime in years, weeks, days, hours, and minutes.
- Reset reason; see Table 68 to translate the numbers displayed.
- Count is the number of resets that have occurred for each reset reason.

Table 68 Reset Reason Codes and Explanations

Reset Reason Code (in hex)	Component/Explanation
0x01	Chassis on
0x02	Line card hot plug in
0x03	Supervisor requests line card off or on
0x04	Supervisor requests hard reset on line card
0x05	Line card requests Supervisor off or on
0x06	Line card requests hard reset on Supervisor
0x07	Line card self reset using the internal system register
0x08	—
0x09	—
0x0A	Momentary power interruption on the line card
0x0B	—
0x0C	—
0x0D	—
0x0E	—
0x0F	—
0x10	—
0x11	Off or on after Supervisor non-maskable interrupts (NMI)
0x12	Hard reset after Supervisor NMI
0x13	Soft reset after Supervisor NMI
0x14	—
0x15	Off or on after line card asks Supervisor NMI
0x16	Hard reset after line card asks Supervisor NMI
0x17	Soft reset after line card asks Supervisor NMI
0x18	—
0x19	Off or on after line card self NMI
0x1A	Hard reset after line card self NMI
0x1B	Soft reset after line card self NMI
0x21	Off or on after spurious NMI
0x22	Hard reset after spurious NMI
0x23	Soft reset after spurious NMI
0x24	—
0x25	Off or on after watchdog NMI
0x26	Hard reset after watchdog NMI
0x27	Soft reset after watchdog NMI
0x28	—

Table 68 Reset Reason Codes and Explanations (continued)

Reset Reason Code (in hex)	Component/Explanation
0x29	Off or on after parity NMI
0x2A	Hard reset after parity NMI
0x2B	Soft reset after parity NMI
0x31	Off or on after system fatal interrupt
0x32	Hard reset after system fatal interrupt
0x33	Soft reset after system fatal interrupt
0x34	—
0x35	Off or on after application-specific integrated circuit (ASIC) interrupt
0x36	Hard reset after ASIC interrupt
0x37	Soft reset after ASIC interrupt
0x38	—
0x39	Off or on after unknown interrupt
0x3A	Hard reset after unknown interrupt
0x3B	Soft reset after unknown interrupt
0x41	Off or on after CPU exception
0x42	Hard reset after CPU exception
0x43	Soft reset after CPU exception
0xA1	Reset data converted to generic data

Interrupts

Interrupts are generated by system components that require attention from the CPU, such as ASICs and NMIs. Interrupts are generally related to hardware limit conditions or errors that need to be corrected.

The continuous format records each time a component is interrupted, and this record is stored and used as base information for subsequent records. Each time the list is saved, a timestamp is added. Time differences from the previous interrupt are counted, so that technical personnel can gain a complete record of the component's operational history when an error occurs.

The following example shows how you might enter this command:

```
Router# show logging onboard module 2 interrupt detail

--------------------------------------------------------------------------------
INTERRUPT SUMMARY INFORMATION
--------------------------------------------------------------------------------
Name                                                |  ID | Offset | Bit |  Count
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
CONTINUOUS INTERRUPT INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS mmm | Name                             |  ID | Offset | Bit
--------------------------------------------------------------------------------
03/06/2007 22:33:06 450   Port-ASIC #2                       9   0x00E7     6
--------------------------------------------------------------------------------
```

Table 69 describes the significant fields shown in the display.

Table 69 Interrupt Summary Information

Field	Description
Name	A description of the component including its position in the device.
ID	An assigned field for data storage.
Offset	The location of the next block in bytes.
Bit	The interrupt bit number recorded from the component's internal register.
The timestamp	Shows the date and time that an interrupt occurred to the millisecond.

Message Logging

The OBFL feature logs standard system messages. Instead of displaying the message to a terminal, the message is written to and stored in a file, so the message can be accessed and read at a later time. System messages range from level 1 alerts to level 7 debug messages, and these levels can be specified in the **hw module logging onboard** command.

The following example shows how you might enter this command:

```
Router# show logging onboard module 2 message detail

--------------------------------------------------------------------------------
ERROR MESSAGE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Facility-Sev-Name      | Count | Persistence Flag
MM/DD/YYYY HH:MM:SS
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
ERROR MESSAGE CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS Facility-Sev-Name
--------------------------------------------------------------------------------
03/06/2007 22:33:35  %GOLD_OBFL-3-GOLD : Diagnostic OBFL: Diagnostic OBFL testing
```

Table 70 describes the significant fields shown in the display.

Table 70 Error Message Summary Information

Field	Description
A timestamp	Shows the date and time the message was logged.
Facility-Sev-Name	A coded naming scheme for a system message, as follows: • The Facility code consists of two or more uppercase letters that indicate the hardware device (facility) to which the message refers. • Sev is a single-digit code from 1 to 7 that reflects the severity of the message. • Name is one or two code names separated by a hyphen that describe the part of the system from where the message is coming.
Error message	Follows the Facility-Sev-Name codes. For more information about system messages, see the *Cisco IOS System and Error Messages* guide.
Count	Indicates the number of instances of this message that is allowed in the history file. Once that number of instances has been recorded, the oldest instance will be removed from the history file to make room for new ones.
Persistence Flag	Gives a message priority over others that do not have the flag set.

Related Commands

Command	Description
attach	Connects to a specific line card for the purpose of executing commands on that card.
clear logging onboard (Cat 6K)	Clears onboard failure logs.
copy logging onboard (Cat 6K)	Copies OBFL data from the target OBFL-enabled module to a local or remote file system.
hw-module logging onboard (Cat 6K)	Disables and enables OBFL.

show logging persistent

To display the contents of the logging persistent files, use the **show logging persistent** command in privileged EXEC mode.

show logging persistent [**url** *filesystem*:*location*] [**selector-url** *filesystem*:*filename*]

Syntax Description

url	(Optional) Specifies the URL to display logging messages.
filesystem:	The URL or alias of the file system followed by a colon.
location	The audit folder location.
selector-url	(Optional) Specifies the URL or location for the search parameters file.
filename	The URL or alias of the search parameters file.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced.

Usage Guidelines

To display the contents of the logging persistent files based on specific parameters in the syslog messages, you need to conduct a search on the syslog messages. In order to reduce the data input complexity, the **show logging persistent** command calls for a URL of a search parameters file, which contains a collection of search and sorting rules.

The search parameters file comprise three sections: search templates, search patterns, and sorting rules. These sections are described in the following text.

Search Templates

Search templates are constructed by using logical expressions and value rules. Value rules are methods of locating the beginning and ending of the object's value. The search templates along with value rules are used to locate objects in the syslog messages and to extract the objects' value.

Table 71 provides the definition of value rules for a list of search objects that can be used to construct search templates.

Table 71 Value Rules for Object Types

Object Type	Value Rules
AUDIT_RECORD_DATE	Fixed format field.
AUDIT_RECORD_TIME	Fixed format field.
FW_DROP_PKT_CAUSE	Finds the first alphanumeric value; stops at the first nonalphanumeric value or underscore ("_") symbol.

Table 71 Value Rules for Object Types

Object Type	Value Rules
INTERFACE_NAME	Finds the first alphanumeric value; stops at the first nonalphanumeric value or a symbol that is not a slash (“/”) or a period (“.”).
L4_PROTO_ID	Finds the first alphanumeric value; stops at the first nonalphanumeric value.
L4_PROTO_ID_RANGE	Finds the first numeric value; stops at the first nonnumeric value.
RULE_IDENTITY	Finds the first alphanumeric value; stops at the colon symbol (“:”).
RULE_IDENTITY_PLATFORM	Finds the first alphanumeric value; stops at the colon symbol (“:”).
SOURCE_SUBJECT DESTINATION_SUBJECT	IPv4: Finds the first numeric value; includes the substring containing number or period (“.’’) ; stops at the first nonnumeric value or nonperiod (“.”); trims the trailing period (“.”), if any. IPv6: Finds the first numeric value; includes the substring containing numbers or periods (“.’’) ; stops at first nonnumeric value or non-period (“.”); trims the trailing period (“.”), if any.
SUBJECT_SERVICE_ID	Finds the first alphanumeric value; stops at the first nonalphanumeric value.
SUBJECT_SERVICE_ID_RANGE	Finds the first numeric value; stops at the first nonnumeric value.
USER_ID	Finds the first alpha symbol; stops at the first nonalphanumeric symbol

Syntax for Search Templates

Search templates for all types of objects are strings enclosed in quotes (“...”). If you provide multiple search templates on the same line, a search is performed for each of the search template in the left-to-right order (by using the logical operation OR).

You can provide arbitrary search templates for all object types except the following: AUDIT_RECORD_DATE, AUDIT_RECORD_TIME, RULE_IDENTITY, and RULE_IDENTITY_PLATFORM.

Search templates of the AUDIT_RECORD_DATE, AUDIT_RECORD_TIME, RULE_IDENTITY, and RULE_IDENTITY_PLATFORM, objects are hard coded because the location and the format of these objects in the Cisco IOS syslog messages are fixed.

The general syntax for the search template is:

```
<object_id>:<logical-expression>
```

For example, the following syntax searches for user:, username, or user in the sylog messages and equates it to USER_ID.

```
USER_ID: "user:" "username" "user"
```

Search Patterns

A search pattern is a regular expression (regexp) for selecting a subset of objects of a given type or a range of values.

Syntax for Search Patterns

Table 72 lists the syntax for search patterns of various types of objects:

Table 72 Syntax for Search Patterns

Object Type	Syntax	Example
AUDIT_RECORD_DATE	YYYY-MM-DD[:YYYY-MM-DD]	AUDIT_RECORD_DATE:2009-01-03 AUDIT_RECORD_DATE:2009-01-03:2009-02-04
AUDIT_RECORD_TIME	HH:MM:SS[-HH:MM:SS]	AUDIT_RECORD_TIME:22:30:33 AUDIT_RECORD_TIME:22:30:33-23:30:00
FW_DROP_PKT_CAUSE	Regular expression with double quotes (“...”)	FW-DROP-PKT_CAUSE: "POLICY"
INTERFACE_NAME	Regular expression with double quotes (“...”)	INTERFACE_NAME: “FastEthernet0/1/2\.1|Gig*”
L4_PROTO_ID	Regular expression with double quotes (“...”)	L4_PROTO_ID: "tcp"
L4_PROTO_ID_RANGE	Numeric value or numeric range without double quotes (“...”)	L4_PROTO_ID_RANGE:6 L4_PROTO_ID_RANGE:8 - 9
RULE_IDENTITY	Regular expression with double quotes (“...”)	RULE_IDENTITY: “SEC_LOGIN\-4\-LOGIN_FAILED|SEC_LOGIN\-5\-LOGIN_SUCCESS”
RULE_IDENTITY_PLATFORM	Regular expression with double quotes (“...”)	RULE_IDENTITY_PLATFORM: "FW\-6\-DROP_PKT"
SOURCE_SUBJECT, DESTINATION_SUBJECT	Regular expression without double quotes (“...”)	SOURCE_SUBJECT: “192\.168\.1\.*|192\.168\.2.\2?”
SUBJECT_SERVICE_ID	Regular expression with double quotes (“...”)	SUBJECT_SERVICE_ID: "telnet|ssh|22"
SUBJECT_SERVICE_ID_RANGE	Numeric value or numeric range without double quotes (“...”)	SUBJECT_SERVICE_ID_RANGE:5 SUBJECT_SERVICE_ID_RANGE:5-122
USER_ID	Case insensitive regular expression with double quotes (“...”)	USER_ID: "alice|Bob"

Sorting Rules

The sorting rules instruct how to sort the selected subset. The sorting rule is specified as a search object ID followed by a sort-order specifier, which is either ASCENDING or DESCENDING.

Syntax for Sorting Rules

The general syntax for the sorting rules is:

```
<object_id>: ASCENDING | DESCENDING
```

For example, the following syntax sorts the user IDs in an ascending order:

```
USER_ID: ASCENDING
```

Search Parameters File

The search parameters file contains a search template, search patterns, and sorting rules. Each section of a search parameters file begins with a header and ends with footer. The general syntax for the search parameters file is as follows:

```
<SEARCH TEMPLATES>
... search-templates here...
</SEARCH TEMPLATES>
<SEARCH PATTERNS>
...search-patterns here...
</SEARCH PATTERNS>
<SORT RULES>
... sort-rules here...
</END SORT RULES>
```

Search Parameters File: Example

The following example shows how to construct search parameters for finding all audit records sorted by the user, between 9/17/2009 and 9/21/2009, captured between 1:00 a.m. and 4:00 a.m. on those dates, which belong to usernames testuser1 or testuser2, and are attempts to initiate a telnet or console connection.

The following syslog messages appear in the output:

*Sep 19 02:46:02.173: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: testuser1] [Source: 172.27.53.101] [localport: 22] at 02:46:02 UTC Wed Sep 19 2001

*Sep 19 02:46:51.359: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: testuser1] [Source: 172.27.53.101] [localport: 22] [Reason: Login Authentication Failed] at 02:46:51 UTC Wed Sep 19 2001

*Sep 19 03:26:28.721: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: testuser2] [Source: 0.0.0.0] [localport: 0] at 03:26:28 UTC Wed Sep 19 2001

The search parameters file for this example is constructed as follows:

```
<SEARCH TEMPLATES>
USER_ID: "user:"
SUBJECT_SERVICE_ID: "localport:"
</SEARCH TEMPLATES>
<SEARCH PATTERNS>
RULE_IDENTITY: "SEC_LOGIN\-5\-LOGIN_SUCCESS" "SEC_LOGIN\-4\-LOGIN_FAILED"
USER_ID: "Alice|Bob"
SUBJECT_SERVICE_ID: "0|22"
AUDIT_RECORD_DATE: 2009-09-17:2009-09-21
AUDIT_RECORD_TIME: 01:00:00 - 03:59:59
</SEARCH PATTERNS>
<SORT RULES>
USER_ID: ASCENDING
</SORT RULES>
```

The **url** *filesystem***:***location* keyword and argument combination specifies the audit folder location. If you do not specify these attributes, a default audit folder location is used. The default audit folder location is defined using the **logging persistent** command.

If you do not specify the **selector-url** *filesystem***:***filename* keyword and argument combination, the viewer displays log files in a chronological order.

Examples

The following is sample output from the **show logging persistent** command:

```
Router# show logging persistent

000070: *Feb 17 01:22:24.147: %PARSER-6-EXPOSEDLOCKACQUIRED: Exclusive configuration lock
acquired by user 'test' from terminal '0'  -Process= "Exec", ipl= 0, pid= 3
000071: *Feb 17 01:22:24.979: %SYS-5-CONFIG_I: Configured from console by ena on console
000072: *Feb 17 01:22:24.979: %PARSER-6-EXPOSEDLOCKRELEASED: Exclusive configuration lock
released from terminal '0' -Process= "Exec", ipl= 0, pid= 3
000073: *Feb 17 02:45:17.201: %PARSER-6-EXPOSEDLOCKACQUIRED: Exclusive configuration lock
acquired by user 'test' from terminal '0'  -Process= "Exec", ipl= 0, pid= 3
Router#
000074: *Feb 18 05:49:19.443: %SYS-6-SHOW_LOGGING_PERSISTENT: User test has activated the
show logging persistent command.
```

The following example shows how to specify the location of the search parameters file “filter_rule_id” from bootflash. The syslog messages are sorted using the search parameters specified in the “filter_rule_id” file and the contents are displayed in the output. In this case, the search parameters specify the system to search for audit records sorted by the “testu1” user for the date 08/31/09.

```
Router# show logging persistent selector-url bootflash:filter_rule_id_pl

*Aug 31 19:35:37.540: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: testu1] [Source:
0.0.0.0] [localport: 0] at 19:35:37 UTC Fri Aug 31 2009

*Aug 31 19:35:54.385: %PARSER-6-EXPOSEDLOCKACQUIRED: Exclusive configuration lock acquired
by user 'testu1' from terminal '0'  -Process= "Exec", ipl= 0, pid= 96 (note: includes
space and apostrophe)
```

The following example shows how to display syslog messages from an audit folder location:

```
Router# show logging persistent url bootflash:test_location

000070: *Feb 17 01:22:24.147: %PARSER-6-EXPOSEDLOCKACQUIRED: Exclusive configuration lock
acquired by user 'test' from terminal '0'  -Process= "Exec", ipl= 0, pid= 3
000071: *Feb 17 01:22:24.979: %SYS-5-CONFIG_I: Configured from console by test onconsole
Router#
000074: *Feb 18 05:49:19.443: %SYS-6-SHOW_LOGGING_PERSISTENT: User test has activated the
show logging persistent command.
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging persistent	Enables the storage of logging messages on the router’s ATA disk.

show management event

To display the Simple Network Management Protocol (SNMP) Event values that have been configured on your routing device through the use of the Event MIB, use the **show management event** command in privileged EXEC mode.

show management event

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The Event MIB allows you to configure your own traps, informs, or set operations through the use of an external network management application. The **show management event** command is used to display the values for the Events configured on your system. For information on Event MIB functionality, see RFC 2981, available at http://www.ietf.org.

Examples

The following example is sample output from the **show management event** command:

```
Router# show management event

Mgmt Triggers:
 (1): Owner: joe_user
  (1): 01, Comment: TestEvent, Sample: Abs, Freq: 120
      Test: Existence Threshold Boolean
         ObjectOwner: aseem, Object: sethi
         OID: ifEntry.10.3, Enabled 1, Row Status 1
      Existence Entry: , Absent, Changed
      StartUp:  Present, Absent
         ObjOwn: , Obj: , EveOwn: aseem, Eve: 09
      Boolean Entry:
         Value: 10, Cmp: 1, Start: 1
         ObjOwn: , Obj: , EveOwn: aseem, Eve: 09
      Threshold Entry:
         Rising: 50000, Falling: 20000
         ObjOwn: ase, Obj: 01 RisEveOwn: ase, RisEve: 09 , FallEveOwn: ase, FallEve: 09
```

```
      Delta Value Table:
  (0): Thresh: Rising, Exis: 1, Read: 0, OID: ifEntry.10.3 , val: 69356097

Mgmt Events:
 (1): Owner: aseem
   (1)Name: 09 , Comment: , Action: Set, Notify, Enabled: 1 Status: 1
      Notification Entry:
         ObjOwn: , Obj: , OID: ifEntry.10.1
      Set:
         OID: ciscoSyslogMIB.1.2.1.0, SetValue: 199, Wildcard: 2 TAG: , ContextName:

 Object Table:
 (1): Owner: aseem
   (1)Name: sethi, Index: 1, OID: ifEntry.10.1, Wild: 1, Status: 1
```

Related Commands

Command	Description
debug management event	Allows real-time monitoring of Event MIB activities for the purposes of debugging.

show management expression

To display the Simple Network Management Protocol (SNMP) Expression values that have been configured on your routing device through the use of the Expression MIB, use the **show management expression** command in user EXEC or privileged EXEC mode.

show management expression

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.2(1)	This command was introduced in a release earlier than Cisco IOS Release 12.2(1).
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.
12.2SR	This command is supported in the Cisco IOS Release 12.2SR train. Support in a specific 12.2SR release of this train depends on your feature set, platform, and platform hardware.
12.2SB	This command is supported in the Cisco IOS Release 12.2SB train. Support in a specific 12.2SB Release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Examples

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

```
Router# show management expression
Expression: 1 is active
  Expression Owner: me
  Expression Name: me
  Expression to be evaluated is $1 + 100 where:
  $1 = ifDescr
  Object Condition is not set
  Sample Type is absolute
  ObjectID is wildcarded
```

The output is self-explanatory.

Related Commands

Command	Description
debug management expression	Monitors the activities of the Expression MIB in real time on your routing device.

show mdf

To display loaded preconfigured Embedded Menu Manager (EMM) Menu Definition Files (MDFs), use the **show mdf** command in user EXEC or privileged EXEC mode.

show mdf

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (#)
Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is sample output from the **show mdf** command when a preconfigured MDF has been loaded on the router:

```
Router# show mdf
Menu Name / URL:
BGP / disk0:bgp.mdf
```

The following is sample output from the **show mdf** command when no MDFs exist on the router:

```
Router# show mdf
No menus configured!
```

Related Commands

Command	Description
debug emm	Debugs MDFs.
emm	Loads and launches preconfigured MDFs or launches loaded preconfigured EMM menus.
emm clear	Changes the terminal clear-screen escape sequence.

show memory

To display statistics about memory when Cisco IOS software or Cisco IOS Software Modularity images are running, use the **show memory** command in user EXEC or privileged EXEC mode.

Cisco IOS software

show memory [*memory-type*] [**free**] [**overflow**] [**summary**] [**poisoning**]

Cisco IOS Software Modularity

show memory

Syntax Description

memory-type	(Optional) Memory type to display (**processor**, **multibus**, **io**, or **sram**). If *memory-type* is not specified, statistics for all memory types present are displayed.
free	(Optional) Displays free memory statistics.
overflow	(Optional) Displays details about memory block header corruption corrections when the **exception memory ignore overflow** global configuration command is configured.
summary	(Optional) Displays a summary of memory usage including the size and number of blocks allocated for each address of the system call that allocated the block.
poisoning	(Optional) Displays memory poisoning details, including the following: • Alloc PID • Alloc Check • Alloc PC • Alloc Name • Corrupt Ptr • Corrupt Val • TotalBytes • MarkedBytes • TIME

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was enhanced with the **overflow** keyword to display details about memory block header corruption corrections.
12.2(25)S	The command output was updated to display information about transient memory pools.

Release	Modification
12.3(14)T	The command output was updated to display information about transient memory pools.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF4	This command was implemented in Cisco IOS Software Modularity images.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	The **poisoning** keyword was added.

Usage Guidelines

Cisco IOS Software

The **show memory** command displays information about memory available after the system image decompresses and loads.

Cisco IOS Software Modularity

No optional keywords or arguments are supported for the **show memory** command when a Cisco IOS Software Modularity image is running. To display details about POSIX and Cisco IOS style system memory information when Software Modularity images are running, use the **show memory detailed** command.

Examples

Example output varies between Cisco IOS software images and Cisco IOS Software Modularity software images. To view the appropriate output, see the following sections:

- Cisco IOS Software
- Cisco IOS Software Modularity

Cisco IOS Software

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

```
Router# show memory

              Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor    B0EE38    5181896    2210036    2971860    2692456    2845368

          Processor memory
Address   Bytes Prev.    Next     Ref  PrevF   NextF   Alloc PC  What
B0EE38     1056 0        B0F280     1                  18F132    List Elements
B0F280     2656 B0EE38   B0FD08     1                  18F132    List Headers
B0FD08     2520 B0F280   B10708     1                  141384    TTY data
B10708     2000 B0FD08   B10F00     1                  14353C    TTY Input Buf
B10F00      512 B10708   B11128     1                  14356C    TTY Output Buf
B11128     2000 B10F00   B11920     1                  1A110E    Interrupt Stack
B11920       44 B11128   B11974     1                  970DE8    *Init*
B11974     1056 B11920   B11DBC     1                  18F132    messages
B11DBC       84 B11974   B11E38     1                  19ABCE    Watched Boolean
B11E38       84 B11DBC   B11EB4     1                  19ABCE    Watched Boolean
B11EB4       84 B11E38   B11F30     1                  19ABCE    Watched Boolean
B11F30       84 B11EB4   B11FAC     1                  19ABCE    Watched Boolean
```

The following is sample output from the **show memory free** command:

```
Router# show memory free

              Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor    B0EE38    5181896    2210076    2971820    2692456    2845368
```

```
          Processor memory
Address   Bytes Prev.    Next     Ref  PrevF   NextF   Alloc PC  What
             24    Free list 1
CEB844       32  CEB7A4 CEB88C      0  0       0       96B894    SSE Manager
             52    Free list 2
             72    Free list 3
             76    Free list 4
             80    Free list 5
D35ED4       80 D35E30   D35F4C     0  0       D27AE8  96B894    SSE Manager
D27AE8       80 D27A48   D27B60     0  D35ED4  0       22585E    SSE Manager
             88    Free list 6
            100    Free list 7
D0A8F4      100 D0A8B0   D0A980     0  0       0       2258DA    SSE Manager
            104    Free list 8
B59EF0      108 B59E8C   B59F84     0  0       0       2258DA    (fragment)
```

The output of the **show memory free** command contains the same types of information as the **show memory** output, except that only free memory is displayed, and the information is ordered by free list.

The first section of the display includes summary statistics about the activities of the system memory allocator.

Table 73 describes the significant fields shown in the first section of the display.

Table 73 show memory Field Descriptions—First Section

Field	Description
Head	Hexadecimal address of the head of the memory allocation chain.
Total(b)	Sum of used bytes plus free bytes.
Used(b)	Amount of memory in use.
Free(b)	Amount of memory not in use.
Lowest(b)	Smallest amount of free memory since last boot.
Largest(b)	Size of largest available free block.

The second section of the display is a block-by-block listing of memory use. Table 74 describes the significant fields shown in the second section of the display.

Table 74 Characteristics of Each Block of Memory—Second Section

Field	Description
Address	Hexadecimal address of block.
Bytes	Size of block (in bytes).
Prev.	Address of previous block (should match the address on previous line).
Next	Address of next block (should match the address on next line).
Ref	Reference count for that memory block, indicating how many different processes are using that block of memory.
PrevF	Address of previous free block (if free).
NextF	Address of next free block (if free).

Table 74 Characteristics of Each Block of Memory—Second Section (continued)

Field	Description
Alloc PC	Address of the system call that allocated the block.
What	Name of process that owns the block, or "(fragment)" if the block is a fragment, or "(coalesced)" if the block was coalesced from adjacent free blocks.

The **show memory io** command displays the free I/O memory blocks. On the Cisco 4000 router, this command quickly shows how much unused I/O memory is available.

The following is sample output from the **show memory io** command:

```
Router# show memory io

Address   Bytes Prev.   Next     Ref  PrevF   NextF   Alloc PC  What
6132DA0   59264 6132664 6141520  0    0       600DDEC  3FCF0     *Packet Buffer*
600DDEC     500 600DA4C 600DFE0  0   6132DA0 600FE68  0
600FE68     376 600FAC8 600FFE0  0   600DDEC 6011D54  0
6011D54     652 60119B4 6011FEO  0   600FE68 6013D54  0
614FCA0     832 614F564 614FFE0  0   601FD54 6177640  0
6177640 2657056 6172E90 0        0   614FCA0 0        0
Total: 2723244
```

The following sample output displays details of a memory block overflow correction when the **exception memory ignore overflow** global configuration command is configured:

```
Router# show memory overflow

Count   Buffer Count     Last corrected      Crashinfo files

1       1                00:11:17            slot0:crashinfo_20030620-075755
Traceback   607D526C 608731A0 607172F8 607288E0 607A5688 607A566C
```

The report includes the amount of time since the last correction was made and the name of the file that logged the memory block overflow details.

The **show memory sram** command displays the free SRAM memory blocks. For the Cisco 4000 router, this command supports the high-speed static RAM memory pool to make it easier for you to debug or diagnose problems with allocation or freeing of such memory.

The following is sample output from the **show memory sram** command:

```
Router# show memory sram

Address   Bytes Prev.   Next     Ref  PrevF   NextF   Alloc PC  What
7AE0      38178 72F0    0        0    0       0       0
Total     38178
```

The following sample output from the **show memory** command used on the Cisco 4000 router includes information about SRAM memory and I/O memory:

```
Router# show memory

              Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor    49C724   28719324    1510864   27208460   26511644   15513908
      I/O   6000000    4194304    1297088    2897216    2869248    2896812
     SRAM      1000      65536      63400       2136       2136       2136

Address   Bytes Prev.   Next     Ref  PrevF   NextF   Alloc PC  What
1000       2032 0       17F0       1                  3E73E     *Init*
17F0       2032 1000    1FE0       1                  3E73E     *Init*
1FE0        544 17F0    2200       1                  3276A     *Init*
```

```
2200          52 1FE0    2234       1                  31D68     *Init*
2234          52 2200    2268       1                  31DAA     *Init*
2268          52 2234    229C       1                  31DF2     *Init*
72F0        2032 6E5C    7AE0       1                  3E73E     Init
7AE0       38178 72F0    0          0    0      0      0
```

The **show memory summary** command displays a summary of all memory pools and memory usage per Alloc PC (address of the system call that allocated the block).

The following is a partial sample output from the **show memory summary** command. This output shows the size, blocks, and bytes allocated. Bytes equal the size multiplied by the blocks. For a description of the other fields, see Table 73 and Table 74.

```
Router# show memory summary

Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor    B0EE38    5181896    2210216    2971680    2692456    2845368

          Processor memory
Alloc PC        Size     Blocks      Bytes    What
0x2AB2           192          1        192    IDB: Serial Info
0x70EC            92          2        184    Init
0xC916           128         50       6400    RIF Cache
0x76ADE         4500          1       4500    XDI data
0x76E84         4464          1       4464    XDI data
0x76EAC          692          1        692    XDI data
0x77764          408          1        408    Init
0x77776          116          1        116    Init
0x777A2          408          1        408    Init
0x777B2          116          1        116    Init
0xA4600           24          3         72    List
0xD9B5C           52          1         52    SSE Manager
.
.
.
0x0                0       3413    2072576    Pool Summary
0x0                0         28    2971680    Pool Summary (Free Blocks)
0x0               40       3441     137640    Pool Summary (All Block Headers)
0x0                0       3413    2072576    Memory Summary
0x0                0         28    2971680    Memory Summary (Free Blocks)
```

Cisco IOS Software Modularity

The following is sample output from the **show memory** command when a Cisco IOS Software Modularity image is running.

```
Router# show memory

System Memory: 262144K total, 116148K used, 145996K free 4000K kernel reserved
```

Table 75 describes the significant fields shown in the display.

Table 75 show memory (Software Modularity Image) Field Descriptions

Field	Description
total	Total amount of memory on the device, in kilobytes.
used	Amount of memory in use, in kilobytes.
free	Amount of memory not in use, in kilobytes.
kernel reserved	Amount of memory reserved by the kernel, in kilobytes.

Related Commands

Command	Description
exception memory ignore overflow	Configures the Cisco IOS software to correct corruptions in memory block headers and allow a router to continue its normal operation.
show memory detailed	Displays POSIX and Cisco IOS style system memory information.
show processes memory	Displays memory used per process.

show memory io

To display the status of the I/O memory, which is used for packet data, use the **show memory io** command in user EXEC or privileged EXEC mode.

show memory io [**allocating-process** [**totals**] | **dead** [**totals**] | **fragment** [**detail**] | **free** [**totals**] | **statistics** [**history** [**table**]]]

Syntax Description

allocating-process	(Optional) Displays the allocating process name.
totals	(Optional) Displays the total allocated memory.
dead	(Optional) Displays memory owned by dead processes.
totals	(Optional) Displays the total dead process memory.
fragment	(Optional) Displays a summary of memory fragment information.
detail	(Optional) Displays detailed memory fragment information.
free	(Optional) Displays free memory statistics.
totals	(Optional) Displays the total free memory.
statistics	(Optional) Displays memory pool statistics.
history	(Optional) Displays memory pool history information.
table	(Optional) Displays a summary of the memory pool history.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was modified. The **fragment**, **detail**, **statistics**, **history**, and **table** keywords were added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 and implemented in Cisco IOS Software Modularity images.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **show memory io** command displays information about I/O memory available after the system image decompresses and loads.

Examples

The following is sample output from the **show memory io fragment** command:

```
Router# show memory io fragment

             I/O memory
Allocator PC Summary for allocated blocks in pool: I/O

    PC          Total   Count  Name
0x60240EE4    2248640      35  FastEthernet0/
0x60395178      12480       3  FastEthernet0/0
0x603950EC       4224       2  FastEthernet0/0
0x6020F588        960       3  *Packet Data*
0x6056B21C        576       1  Init

Allocator PC Summary for free blocks in pool: I/O

    PC          Total   Count  Name
0x6020F588   29854096       3  (fragment)
0x00000000      35632       1  (coalesced)
0x632A3DE8       3072      16  (fragment)
0x60395178        384       2  (fragment)
0x6056B21C        256       1  (fragment)

Free memory size :  29892244 Number of free blocks:       23
```

Table 76 describes the significant fields shown in the display.

Table 76 show memory io fragment Field Descriptions

Field	Description
PC	Program counter.
Total	Total memory allocated by the process (in bytes).
Count	Number of allocations.
Name	Name of the allocating process.

Related Commands

Command	Description
exception memory ignore overflow	Configures the Cisco IOS software to correct corruptions in memory block headers and allow a router to continue its normal operation.
show memory	Displays statistics about memory when Cisco IOS software or Cisco IOS Software Modularity images are running.
show memory detailed	Displays POSIX and Cisco IOS style system memory information.
show processes memory	Displays memory used per process.

show monitor capture

To display the contents of a capture buffer or a capture point, use the **show monitor capture** command in privileged EXEC mode.

show monitor capture {**buffer** {*capture-buffer-name* [**parameters**] | **all parameters** | **merged** *capture-buffer-name1 capture-buffer-name2*}[**dump**] [**filter** *filter-parameters*]} | **point** {**all** | *capture-point-name*}}

Catalyst 6500 Series and Cisco 7600 Series

show monitor capture [**buffer** [*start-index* [*end-index*]] [**brief** [**acl** {*acl-list* | *exp-acl-list*}] | **detail**] [**dump**[**nowrap** *dump-length*] [**acl** {*acl-list* | *exp-acl-list*}] | **status**]

Syntax Description

buffer	Displays the contents of the specified capture buffer.
capture-buffer-name	Name of the capture buffer.
parameters	(Optional) Displays values of parameters for the specified buffers or all buffers.
all	Displays values of parameters for all the buffers.
merged	Displays values of parameters for any two buffers specified.
capture-buffer-name1	Name of the first buffer to be merged.
capture-buffer-name2	Name of the second buffer to be merged.
dump	(Optional) Displays a hexadecimal dump of the captured packet in addition to the metadata.
filter	(Optional) Displays the filter parameters configured for packets stored in the buffer.
filter-parameters	(Optional) Displays the value of the specified parameter applied for defining the filter. Any of the following parameters can be specified: • **direction**—Filters output based on direction. Two types of direction can be specified: **ingress**, **egress**. • **input-interface** *interface-type number*—Filters packets on an input interface. • **l3protocol**—Filters packets with specific L3 protocol. Three types of L3 protocols can be specified: **ipv4**, **ipv6**, **MPLS**. • **output-interface** *interface-type number*—Filters packets on an output interface. • **pak-size** *minimum-size maximum-size*—Filters output based on packet size. The minimum and maximum size for the packets must be specified. The range for the minimum size is from 1 to 2147483647 and the maximum size is from 23 to 2147483647. • **time** *hh***:***mm day month* **duration** *seconds*—Filters packets from a specific date and time. The time is in the hh:mm format. The day, month of the year and duration, in seconds must be specified. Range for duration is from 1 to 2147483647.
point	Displays the contents of the capture point specified.

all	Displays all parameters for all the capture points.
capture-point-name	Displays all parameters for the specified capture point.
start-index	(Optional) The source index. The range is from 1 to 4294967295.
end-index	(Optional) The destination index. The range is from 1 to 4294967295.
brief	(Optional) Provides a brief output of the captured packet information.
acl	(Optional) Displays the output of captured packets for the specified access control list (ACL) only.
acl-list	The IP access list (standard or extended). The range is from 0 to 199.
exp-acl-list	The IP expanded access list (standard or extended). The range is from 1300 to 2699.
detail	(Optional) Provides a detailed output of the captured packet information.
dump	(Optional) Specifies the hexadecimal dump of the captured packets.
nowrap	(Optional) Prevents wrapping of the display output.
dump-length	(Optional) Specifies the hexadecimal dump length of the captured packets. The range is from 14 to 256.
status	(Optional) Displays the capture status.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI on Catalyst 6500 series routers.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD on Cisco 7600 series routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Note The availability of keywords depends on your system and platform.

If you are using Cisco 6500 series routers or Cisco 7600 series, refer to the following usage guidelines:

You can enter the **show monitor capture** command when the capture buffer is not in the running state. You can enter the **show monitor capture status** command even when the capture is enabled to see how many packets are captured.

If you enter the **show monitor capture** command without any keywords or arguments, the output displays the configurations. If you enter the **dump nowrap** keywords, one hexadecimal line is printed per packet. Up to 72 characters of packet bytes is dumped.

If you enter the **dump nowrap** *dump-length* keywords and argument value, the specified length of bytes per line is dumped. If you enter the **brief** keyword, only the src ip, dest ip, src port, dest port, and protocol fields are displayed along with the packet length and item number.

If you enter the **detail** keyword, packets are decoded to the layer 4 protocol level and displayed. If you enter the **dump** keyword, non-IP packets are displayed in hexadecimal dump format. An ACL can be configured as a display filter so that only packets permitted by the ACL are displayed.

Examples

The following example shows how to display all parameters for all capture buffers:

```
Router# show monitor capture buffer all parameters

Capture buffer buff (circular buffer)
Buffer Size : 262144 bytes, Max Element Size : 68 bytes, Packets : 0
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Configuration:
monitor capture buffer buff circular
Capture buffer buff1 (linear buffer)
Buffer Size : 262144 bytes, Max Element Size : 68 bytes, Packets : 0
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Configuration:
```

Table 77 describes the significant fields shown in the display.

Table 77 show monitor capture Field Descriptions

Field	Description
Buffer Size	Size of the buffer defined.
Max Element Size	Specifies the maximum packet size based on which the output has been filtered.
Allow-nth-pak	Specifies that every *n*th packet in the captured data through the buffer is allowed.
Associated Capture Points	Specifies all the capture points that are associated with capture buffers.

The following example shows how to display a hexadecimal dump of the captured packet. The report is self-explanatory and contains the interface type, switching path of the specified buffer, and a hexadecimal dump for the specified buffer.

```
Router# show monitor capture buff pktrace1 dump

11:13:00.593 EDT Mar 21 2007 : IPv4 Turbo      : Fa2/1 Fa0/1
65B6F500: 080020A2 44D90009 E94F8406 08004500  .. "DY..iO....E.
65B6F510: 00400F00 0000FE01 92AF5801 13025801  .@....~../X...X.
65B6F520: 58090800 4D1A1169 00000000 0005326C  X...M..i......2l
65B6F530: 01CCABCD ABCDABCD ABCDABCD ABCDABCD  .L+M+M+M+M+M+M+M
65B6F540: ABCDABCD ABCDABCD ABCDABCD ABCD00    +M+M+M+M+M+M+M.

11:13:20.593 EDT Mar 21 2007 : IPv4 Turbo      : Fa2/1 Fa0/1
65B6F500: 080020A2 44D90009 E94F8406 08004500  .. "DY..iO....E.
65B6F510: 00400F02 0000FE01 92AD5801 13025801  .@....~..-X...X.
65B6F520: 58090800 FEF91169 00000000 0005326C  X...~y.i......2l
65B6F530: 4FECABCD ABCDABCD ABCDABCD ABCDABCD  Ol+M+M+M+M+M+M+M
65B6F540: ABCDABCD ABCDABCD ABCDABCD ABCDFF    +M+M+M+M+M+M+M.
```

The following example shows how to display all the capture points:

```
Router# show monitor capture point all

Status Information for Capture Point ipceffa0/1
IPv4 CEF
Switch Path: IPv4 CEF, Capture Buffer: pktrace1
Status : Inactive
Configuration:
```

```
monitor capture point ip cef ipceffa0/1 FastEthernet0/1 both
Status Information for Capture Point local
IPv4 CEF
Switch Path: IPv4 From Us, Capture Buffer: None
Status : Inactive
```

Table 78 describes the significant fields shown in the display.

Table 78 show monitor capture point all Field Descriptions

Field	Description
IPv4 CEF	Specifies that the capture point contains IPv4 Cisco Express Forwarding (CEF) packets.
Switch Path	Indicates the type of switching path used by the capture point.
Capture Buffer	Specifies the name of the capture buffer configured.
Status	Indicates the status of the capture point.

Catalyst 6500 Series and Cisco 7600 Series

The following example shows how to display the captured packets in a specific access control list (ACL):

```
Router# show monitor capture buffer acl 1

Capture instance [1] :
======================
session status : up
rate-limit value : 10000
buffer-size : 2097152
capture state : ON [running for 00:02:12.736]
capture mode : Linear
capture length : 68
```

Table 79 describes the significant fields shown in the display.

Table 79 show monitor capture buffer acl Field Descriptions

Field	Description
session status	Indicates the status of the capture session.
rate-limit value	Specifies the rate at which packets are captured.
buffer-size	Specifies the capture buffer size, in bytes.
capture state	Indicates the status of the capture buffer.
capture mode	Indicates the shape of the capture buffer.
capture length	Specifies the length of the capture buffer.

The following example shows how to display all the packets in a capture buffer. The report is self-explanatory.

```
Router# show monitor capture buffer

1 IP: s=10.12.0.5 , d=224.0.0.10, len 60
2 346 0180.c200.000e 0012.44d8.5000 88CC 020707526F7
3 60 0180.c200.0000 0004.c099.06c5 0026 42420300000
4 60 ffff.ffff.ffff 0012.44d8.5000 0806 00010800060
5 IP: s=7.0.84.23 , d=224.0.0.5, len 116
```

```
6 IP: s=10.12.0.1 , d=224.0.0.10, len 60
```

The following example shows how to display packets that are decoded to the layer 4 protocol level. The report is self-explanatory.

```
Router# show monitor capture buffer detail

1 Arrival time : 09:44:30 UTC Fri Nov 17 2006
Packet Length : 74 , Capture Length : 68
Ethernet II : 0100.5e00.000a 0008.a4c8.c038 0800
IP: s=10.12.0.5 , d=224.0.0.10, len 60, proto=88
2 Arrival time : 09:44:31 UTC Fri Nov 17 2006
Packet Length : 346 , Capture Length : 68
346 0180.c200.000e 0012.44d8.5000 88CC 020707526F757463031
```

The following example shows how to display the non-IP packets in hexadecimal dump format. The report is self-explanatory.

```
Router# show monitor capture buffer dump

1 IP: s=10.12.0.5 , d=224.0.0.10, len 60
08063810: 0100 5E00000A ..^...
08063820: 0008A4C8 C0380800 45C0003C 00000000 ..$H@8..E@.<....
08063830: 0258CD8F 0A0C0005 E000000A 0205EE6A .XM.....`.....nj
08063840: 00000000 00000000 00000000 00000064 ...............d
08063850: 0001000C 01000100 0000000F 0004 ..............
2 346 0180.c200.000e 0012.44d8.5000 88CC 020707526F757465720415
3 60 0180.c200.0000 0004.c099.06c5 0026 424203000000000800000
4 60 ffff.ffff.ffff 0012.44d8.5000 0806 000108000604000 1001244
5 IP: s=7.0.84.23 , d=224.0.0.5, len 116
0806FCB0: 0100 5E000005 ..^...
0806FCC0: 0015C7D7 AC000800 45C00074 00000000 ..GW,...E@.t....
0806FCD0: 01597D55 07005417 E0000005 0201002C .Y}U..T.`......,
0806FCE0: 04040404 00000000 00000002 00000010 ................
0806FCF0: 455D8A10 FFFF0000 000A1201 0000 E]............
```

The following example shows how to display one hexadecimal line per packet, with up to 72 characters of packet bytes dumped. The report is self-explanatory.

```
Router# show monitor capture buffer dump nowrap

1 74 0100.5e00.000a 0008.a4c8.c038 0800 45C0003C000000
2 346 0180.c200.000e 0012.44d8.5000 88CC 020707526F7574
3 60 0180.c200.0000 0004.c099.06c5 0026 42420300000000
4 60 ffff.ffff.ffff 0012.44d8.5000 0806 00010800060400
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture	Enables and configures monitor packet capturing.
monitor capture buffer	Configures a buffer to capture packet data.
monitor capture point	Defines a monitor capture point and associates it with a capture buffer.

show monitor event-trace

To display event trace messages for Cisco IOS software subsystem components, use the **show monitor event-trace** command in privileged EXEC mode.

show monitor event-trace [**all-traces**] [*component* {**all** | **back** *hour:minute* | **clock** *hour:minute* | **from-boot** *seconds* | **latest** | **parameters**}]

Syntax Description

all-traces	(Optional) Displays all event trace messages in memory to the console.
component	(Optional) Name of the Cisco IOS software subsystem component that is the object of the event trace. To get a list of components that support event tracing in this release, use the **monitor event-trace ?** command.
all	Displays all event trace messages currently in memory for the specified component.
back *hour:minute*	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes. The time argument is specified in hours and minutes format (hh:mm).
clock *hour:minute*	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
from-boot *seconds*	Displays event trace messages starting from a specified number of seconds after booting (uptime). To display the uptime, in seconds, enter the **show monitor event-trace** *component* **from-boot ?** command.
latest	Displays only the event trace messages since the last **show monitor event-trace** command was entered.
parameters	Displays the trace parameters. The only parameter displayed is the size (number of trace messages) of the trace file.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The **show monitor event-trace cef** comand replaced the **show cef events** and **show ip cef events** commands.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. The **spa** component keyword was added to support online insertion and removal (OIR) event messages for shared port adapters (SPAs). The **bfd** keyword was added for the *component* argument to display trace messages relating to the Bidirectional Forwarding Detection (BFD) feature.
12.4(4)T	Support for the **bfd** keyword was added for Cisco IOS Release 12.4(4)T.
12.0(31)S	Support for the **bfd** keyword was added for Cisco IOS Release 12.0(31)S.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.4(9)T	The **cfd** keyword was added as an entry for the *component* argument to display trace messages relating to crypto fault detection.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show monitor event-trace** command to display trace message information.

The trace function is not locked while information is being displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace** command will generate a message indicating that some messages might be lost; however, messages will continue to display on the console. If the number of lost messages is excessive, the **show monitor event-trace** command will stop displaying messages.

Use the **bfd** keyword for the *component* argument to display trace messages relating to the BFD feature.

Use the **cfd** keyword for the *component* argument to display trace messages relating to the crypto fault detection feature. This keyword displays the contents of the error trace buffers in an encryption data path.

Examples

IPC Component Example

The following is sample output from the **show monitor event-trace** *component* command for the interprocess communication (IPC) component. Notice that each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace ipc

3667:  6840.016:Message type:3 Data=0123456789
3668:  6840.016:Message type:4 Data=0123456789
3669:  6841.016:Message type:5 Data=0123456789
3670:  6841.016:Message type:6 Data=0123456
```

BFD Component for Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

Use the **show monitor event-trace bfd all** command to display logged messages for important BFD events in the recent past. The following trace messages show BFD session state changes:

```
Router# show monitor event-trace bfd all

    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], event Session
           create, state Unknown -> Fail
    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Fail -> Down
            (from LC)
    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Down -> Init
            (from LC)
    3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Init -> Up
           (from LC)
    3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], event Session
           create, state Unknown -> Fail
```

```
3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Fail -> Down
        (from LC)
3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Down -> Up
       (from LC)
```

To display trace information for all components configured for event tracing on the networking device, enter the **show monitor event-trace all-traces** command. In this example, separate output is provided for each event, and message numbers are interleaved between the events.

```
Router# show monitor event-trace all-traces

Test1 event trace:
3667: 6840.016:Message type:3 Data=0123456789
3669: 6841.016:Message type:4 Data=0123456789
3671: 6842.016:Message type:5 Data=0123456789
3673: 6843.016:Message type:6 Data=0123456789

Test2 event trace:
3668: 6840.016:Message type:3 Data=0123456789
3670: 6841.016:Message type:4 Data=0123456789
3672: 6842.016:Message type:5 Data=0123456789
3674: 6843.016:Message type:6 Data=0123456789
```

SPA Component Example

The following is sample output from the **show monitor event-trace** *component* **latest** command for the **spa** component:

```
Router# show monitor event-trace spa latest

00:01:15.364: subslot 2/3: 4xOC3 POS SPA, TSM Event:inserted  New state:wait_psm
_ready
     spa type 0x440
00:02:02.308: subslot 2/0: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/0: not present, TSM Event:remove_complete  New state:idle
00:02:02.308: subslot 2/1: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/1: not present, TSM Event:remove_complete  New state:idle
00:02:02.308: subslot 2/2: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/2: not present, TSM Event:remove_complete  New state:idle
00:02:02.312: subslot 2/3: not present(plugin 4xOC3 POS SPA), TSM Event:empty  New
state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.312: subslot 2/3: not present, TSM Event:remove_complete  New state:idle
```

Cisco Express Forwarding Component Examples

If you select Cisco Express Forwarding as the component for which to display event messages, you can use the following additional arguments and keywords: **show monitor event-trace cef** [**events** | **interface** | **ipv6** | **ipv4**][**all**].

The following example shows the IPv6 or IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv6 all

00:00:24.612:  [Default] *::*/*'00             New FIB table          [OK]

Router# show monitor event-trace cef ipv4 all

00:00:24.244:  [Default] 127.0.0.81/32'01       FIB insert             [OK]
```

In the following example, all event trace messages for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all

00:00:18.884: SubSys  fib_ios_chain init
00:00:18.884: Inst    unknown -> RP
00:00:24.584: SubSys  fib init
00:00:24.592: SubSys  fib_ios init
00:00:24.592: SubSys  fib_ios_if init
00:00:24.596: SubSys  ipv4fib init
00:00:24.608: SubSys  ipv4fib_ios init
00:00:24.612: SubSys  ipv6fib_ios init
00:00:24.620: Flag    IPv4 CEF enabled set to yes
00:00:24.620: Flag    0x7BF6B62C set to yes
00:00:24.620: Flag    IPv4 CEF switching enabled set to yes
00:00:24.624: GState  CEF enabled
00:00:24.628: SubSys  ipv4fib_les init
00:00:24.628: SubSys  ipv4fib_pas init
00:00:24.632: SubSys  ipv4fib_util init
00:00:25.304: Process Background created
00:00:25.304: Flag    IPv4 CEF running set to yes
00:00:25.304: Process Background event loop enter
00:00:25.308: Flag    IPv4 CEF switching running set to yes
```

The following example shows Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all

00:00:24.624: <empty>      (sw  4) Create   new
00:00:24.624: <empty>      (sw  4) SWIDBLnk FastEthernet0/0(4)
00:00:24.624: Fa0/0        (sw  4) NameSet
00:00:24.624: <empty>      (hw  1) Create   new
00:00:24.624: <empty>      (hw  1) HWIDBLnk FastEthernet0/0(1)
00:00:24.624: Fa0/0        (hw  1) NameSet
00:00:24.624: <empty>      (sw  3) Create   new
00:00:24.624: <empty>      (sw  3) SWIDBLnk FastEthernet0/1(3)
00:00:24.624: Fa0/1        (sw  3) NameSet
00:00:24.624: <empty>      (hw  2) Create   new
```

Cisco Express Forwarding Component Examples for Cisco 10000 Series Routers Only

The following example shows the IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv4 all

00:00:48.244:  [Default] 127.0.0.81/32'01      FIB insert               [OK]
```

In the following example, all event trace message for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all

00:00:18.884: SubSys  fib_ios_chain init
00:00:18.884: Inst    unknown -> RP
00:00:24.584: SubSys  fib init
00:00:24.592: SubSys  fib_ios init
00:00:24.592: SubSys  fib_ios_if init
00:00:24.596: SubSys  ipv4fib init
00:00:24.608: SubSys  ipv4fib_ios init
00:00:24.620: Flag    IPv4 CEF enabled set to yes
00:00:24.620: Flag    0x7BF6B62C set to yes
00:00:24.620: Flag    IPv4 CEF switching enabled set to yes
00:00:24.624: GState  CEF enabled
00:00:24.628: SubSys  ipv4fib_les init
00:00:24.628: SubSys  ipv4fib_pas init
00:00:24.632: SubSys  ipv4fib_util init
00:00:25.304: Process Background created
00:00:25.304: Flag    IPv4 CEF running set to yes
00:00:25.304: Process Background event loop enter
00:00:25.308: Flag    IPv4 CEF switching running set to yes
```

The following examples show Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all

00:00:24.624: <empty>      (sw  4) Create   new
00:00:24.624: <empty>      (sw  4) SWIDBLnk FastEthernet1/0/0(4)
00:00:24.624: Fa0/0        (sw  4) NameSet
00:00:24.624: <empty>      (hw  1) Create   new
00:00:24.624: <empty>      (hw  1) HWIDBLnk FastEthernet1/0/0(1)
00:00:24.624: Fa0/0        (hw  1) NameSet
00:00:24.624: <empty>      (sw  3) Create   new
00:00:24.624: <empty>      (sw  3) SWIDBLnk FastEthernet1/1/0(3)
00:00:24.624: Fa0/1        (sw  3) NameSet
00:00:24.624: <empty>      (hw  2) Create   new
```

CFD Component for Cisco IOS Release 12.4(9)T

To troubleshoot errors in an encryption datapath, enter the **show monitor event-trace cfd all** command. In this example, events are shown separately, each beginning with a time stamp, followed by data from the error trace buffer. Cisco Technical Assistence Center (TAC) engineers can use this information to diagnose the cause of the errors.

Note If no packets have been dropped, this command does not display any output.

```
Router# show monitor event-trace cfd all

00:00:42.452: 450000B4 00060000 FF33B306 02020203 02020204 32040000 F672999C
        00000001 7A7690C2 A0A4F8BC E732985C D6FFDCC8 00000001 C0902BD0
        A99127AE 8EAA22D4

00:00:44.452: 450000B4 00070000 FF33B305 02020203 02020204 32040000 F672999C
        00000002 93C01218 2325B697 3C384CF1 D6FFDCC8 00000002 BFA13E8A
        D21053ED 0F62AB0E

00:00:46.452: 450000B4 00080000 FF33B304 02020203 02020204 32040000 F672999C
        00000003 7D2E11B7 A0BA4110 CC62F91E D6FFDCC8 00000003 7236B930
        3240CA8C 9EBB44FF

00:00:48.452: 450000B4 00090000 FF33B303 02020203 02020204 32040000 F672999C
        00000004 FB6C80D9 1AADF938 CDE57ABA D6FFDCC8 00000004 E10D8028
```

```
        6BBD748F 87F5E253

00:00:50.452: 450000B4 000A0000 FF33B302 02020203 02020204 32040000 F672999C
        00000005 697C8D9D 35A8799A 2A67E97B D6FFDCC8 00000005 BC21669D
        98B29FFF F32670F6

00:00:52.452: 450000B4 000B0000 FF33B301 02020203 02020204 32040000 F672999C
        00000006 CA18CBC4 0F387FE0 9095C27C D6FFDCC8 00000006 87A54811
        AE3A0517 F8AC4E64
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls event trace functions for a specified Cisco IOS software subsystem component.
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.

show monitor event-trace cpu-report

To display event trace messages for the CPU, use the **show monitor event-trace cpu-report** command in user EXEC or privileged EXEC mode.

show monitor event-trace cpu-report {**brief** {**all** [**detail**] | **back** *time* | **clock** *time* | **from-boot** *seconds* | [**detail**] | **latest** [**detail**]} | **handle** *handle-number*}

Syntax Description

brief	Displays a brief CPU report.
all	Displays all event trace messages currently in memory for the CPU.
detail	(Optional) Displays detailed event trace information.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
time	Integer value that is the length of time, in hours and minutes. The format is hh:mm.
clock	Displays event trace messages starting from a specific clock time.
from-boot	Displays event trace messages starting from a specified number of seconds after booting.
seconds	Number of seconds since the networking device was last booted (uptime).
latest	Displays only the event trace messages since the last **show monitor event-trace** command was entered.
handle	Displays a detailed CPU report for a specified handle number.
handle-number	Handle number. Valid values are from 1 to 255.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **show monitor event-trace cpu-report** command with the **brief** keyword to display the CPU report details. To see individual snapshots, use the **show monitor event-trace cpu-report handle** *handle-number* command.

To view the uptime, in seconds, enter the **show monitor event-trace cpu-report from-boot ?** command.

Examples

To view CPU report details for event tracing on a networking device, enter the **show monitor event-trace cpu-report brief all** command:

```
Router# show monitor event-trace cpu-report brief all

Timestamp   : Handle Name               Description
00:01:07.320:  1     CPU                None
```

To view CPU report details for event tracing on a networking device for the handle number 1, enter the **show monitor event-trace cpu-report handle 1** command:

```
Router# show monitor event-trace cpu-report handle 1

00:01:07.320:  1     CPU                None
################################################################################
Global Statistics
-----------------
5 sec CPU util 0%/0% Timestamp 21:03:56
Queue Statistics
----------------
             Exec Count  Total CPU    Response Time         Queue Length
                                       (avg/max)              (avg/max)
Critical           1          0          0/0                    1/1
High               5          0          0/0                    1/1
Normal           178          0          0/0                    2/9
Low               15          0          0/0                    2/3
Common Process Information
------------------------------
 PID Name             Prio Style
------------------------------
  10 AAA high-capacit M  New
 133 RADIUS TEST CMD  M  New
  47 VNM DSPRM MAIN   H  New
  58 TurboACL         M  New
  97 IP Background    M  New
  99 CEF: IPv4 proces L  New
 112 X.25 Background  M  New
 117 LFDp Input Proc  M  New
   3 Init             M  Old
CPU Intensive processes
--------------------------------------------------------------------------------
 PID Total       Exec    Quant         Burst  Burst size  Schedcall  Schedcall
     CPUms      Count   avg/max        Count avg/max(ms)      Count Per avg/max
--------------------------------------------------------------------------------
   3   820          6   136/236         1     24/24              18  887/15172
Priority Suspends
-----------------------------------
 PID Exec Count Prio-Susps
-----------------------------------
   3          6          1
Latencies
-------------------------
 PID Exec Count   Latency
                  avg/max
-------------------------
  10          1 15192/15192
 133          1 15192/15192
  58          1 15192/15192
 112          1 15192/15192
 117          1 15192/15192
  99          1 15172/15172
  47          1 15172/15172
  97          1 15172/15172
```

```
################################################################################
Global Statistics
-----------------
5 sec CPU util 0%/0% Timestamp 00:00:00
Queue Statistics
----------------
        Exec Count  Total CPU     Response Time            Queue Length
                                     (avg/max)                (avg/max)
Critical      0          0              0/0                    0/0
High          0          0              0/0                    0/0
Normal        0          0              0/0                    0/0
Low           0          0              0/0                    0/0

Common Process Information
------------------------------
 PID Name             Prio Style
------------------------------

CPU Intensive processes
--------------------------------------------------------------------------------
 PID Total       Exec    Quant         Burst  Burst size  Schedcall  Schedcall
     CPUms      Count   avg/max        Count avg/max(ms)      Count Per avg/max
--------------------------------------------------------------------------------
Priority Suspends
-----------------------------------
 PID Exec Count Prio-Susps
-----------------------------------
Latencies
-------------------------
 PID Exec Count   Latency
                  avg/max
-------------------------
################################################################################
```

Related Commands

Command	Description
monitor event-trace cpu-report (EXEC)	Monitors event tracing of the CPU reports.
monitor event-trace cpu-report (global)	Monitors the collection of CPU report traces.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.

show netconf

To display network configuration protocol (NETCONF) information, use the **show netconf** command in privileged EXEC mode.

show netconf {**counters** | **session** | **schema**}

Syntax Description

counters	Displays NETCONF statistics and informational counters.
session	Displays the current state of all connected NETCONF sessions across all transports and any resources and locks in use by the session.
schema	Displays the NETCONF schema.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.4(20)T	This command was modified. The schema keyword was added.

Examples

The following is sample output from the **show netconf counters** command:

```
Router# show netconf counters

NETCONF Counters
Connection Attempts:0: rejected:0 no-hello:0 success:0
Transactions
        total:0, success:0, errors:0
detailed errors:
        in-use 0        invalid-value 0         too-big 0
        missing-attribute 0     bad-attribute 0         unknown-attribute 0
        missing-element 0       bad-element 0   unknown-element 0
        unknown-namespace 0     access-denied 0         lock-denied 0
        resource-denied 0       rollback-failed 0       data-exists 0
        data-missing 0  operation-not-supported 0       operation-failed 0
        partial-operation 0
```

The following is sample output from the **show netconf session** command:

```
Router# show netconf session

(Current | max) sessions:   3 | 4
Operations received: 100              Operation errors: 99
Connection Requests: 5                Authentication errors: 2   Connection Failures: 0
ACL dropped : 30
Notifications  Sent: 20
```

The output of the **show netconf schema** command describes the element structure for a NETCONF request and the resulting reply. This schema can be used to construct proper NETCONF requests and parse the resulting replies. The nodes in the schema are defined in RFC 4741. The following is sample output from the **show netconf schema** command:

```
Router# show netconf schema

New Name Space 'urn:ietf:params:xml:ns:netconf:base:1.0'
<VirtualRootTag> [0, 1] required
  <rpc-reply> [0, 1] required
    <ok> [0, 1] required
    <data> [0, 1] required
    <rpc-error> [0, 1] required
      <error-type> [0, 1] required
      <error-tag> [0, 1] required
      <error-severity> [0, 1] required
      <error-app-tag> [0, 1] required
      <error-path> [0, 1] required
      <error-message> [0, 1] required
      <error-info> [0, 1] required
        <bad-attribute> [0, 1] required
        <bad-element> [0, 1] required
        <ok-element> [0, 1] required
        <err-element> [0, 1] required
        <noop-element> [0, 1] required
        <bad-namespace> [0, 1] required
        <session-id> [0, 1] required
  <hello> [0, 1] required
    <capabilities> 1 required
      <capability> 1+ required
  <rpc> [0, 1] required
    <close-session> [0, 1] required
    <commit> [0, 1] required
      <confirmed> [0, 1] required
      <confirm-timeout> [0, 1] required
    <copy-config> [0, 1] required
      <source> 1 required
        <config> [0, 1] required
          <cli-config-data> [0, 1] required
            <cmd> 1+ required
          <cli-config-data-block> [0, 1] required
          <xml-config-data> [0, 1] required
            <Device-Configuration> [0, 1] required
              <> any subtree is allowed
        <candidate> [0, 1] required
        <running> [0, 1] required
        <startup> [0, 1] required
        <url> [0, 1] required
      <target> 1 required
        <candidate> [0, 1] required
        <running> [0, 1] required
        <startup> [0, 1] required
        <url> [0, 1] required
    <delete-config> [0, 1] required
      <target> 1 required
        <candidate> [0, 1] required
        <running> [0, 1] required
        <startup> [0, 1] required
        <url> [0, 1] required
    <discard-changes> [0, 1] required
    <edit-config> [0, 1] required
      <target> 1 required
        <candidate> [0, 1] required
```

```
    <running> [0, 1] required
    <startup> [0, 1] required
    <url> [0, 1] required
  <default-operation> [0, 1] required
  <test-option> [0, 1] required
  <error-option> [0, 1] required
  <config> 1 required
    <cli-config-data> [0, 1] required
      <cmd> 1+ required
    <cli-config-data-block> [0, 1] required
    <xml-config-data> [0, 1] required
      <Device-Configuration> [0, 1] required
        <> any subtree is allowed
<get> [0, 1] required
  <filter> [0, 1] required
    <config-format-text-cmd> [0, 1] required
      <text-filter-spec> [0, 1] required
    <config-format-text-block> [0, 1] required
      <text-filter-spec> [0, 1] required
    <config-format-xml> [0, 1] required
    <oper-data-format-text-block> [0, 1] required
      <show> 1+ required
    <oper-data-format-xml> [0, 1] required
      <show> 1+ required
<get-config> [0, 1] required
  <source> 1 required
    <config> [0, 1] required
      <cli-config-data> [0, 1] required
        <cmd> 1+ required
      <cli-config-data-block> [0, 1] required
      <xml-config-data> [0, 1] required
        <Device-Configuration> [0, 1] required
          <> any subtree is allowed
    <candidate> [0, 1] required
    <running> [0, 1] required
    <startup> [0, 1] required
    <url> [0, 1] required
  <filter> [0, 1] required
    <config-format-text-cmd> [0, 1] required
      <text-filter-spec> [0, 1] required
    <config-format-text-block> [0, 1] required
      <text-filter-spec> [0, 1] required
    <config-format-xml> [0, 1] required
<kill-session> [0, 1] required
  <session-id> [0, 1] required
<lock> [0, 1] required
  <target> 1 required
    <candidate> [0, 1] required
    <running> [0, 1] required
    <startup> [0, 1] required
    <url> [0, 1] required
<unlock> [0, 1] required
  <target> 1 required
    <candidate> [0, 1] required
    <running> [0, 1] required
    <startup> [0, 1] required
    <url> [0, 1] required
<validate> [0, 1] required
  <source> 1 required
    <config> [0, 1] required
      <cli-config-data> [0, 1] required
        <cmd> 1+ required
      <cli-config-data-block> [0, 1] required
      <xml-config-data> [0, 1] required
```

```
        <Device-Configuration> [0, 1] required
          <> any subtree is allowed
      <candidate> [0, 1] required
      <running> [0, 1] required
      <startup> [0, 1] required
      <url> [0, 1] required
  <notification-on> [0, 1] required
  <notification-off> [0, 1] required
```

Table 80 describes the significant fields shown in the displays.

Table 80 show netconf Field Descriptions

Field	Description
Connection Attempts	Number of NETCONF connection attempts.
rejected	Number of rejected NETCONF sessions.
no-hello	Number of NETCONF sessions that were dropped because Hello messages were not received.
success	Number of successful NETCONF sessions.
in-use 0	The request requires a resource that is already in use.
invalid-value 0	The request specifies an invalid value for one or more parameters.
too-big 0	The request or response that would be generated would be too large for the implementation to handle.
missing-attribute 0	An expected attribute is missing.
bad-attribute 0	An attribute value is incorrect. An attribute that is the incorrect type, out of range, or contains a pattern mismatch will be displayed as a bad attribute.
unknown-attribute 0	An unexpected attribute is present.
missing-element 0	An expected element is missing.
bad-element 0	An element value is not correct. An element that is the incorrect type, out of range, or contains a pattern mismatch will be displayed as a bad element.
unknown-element 0	An unexpected element is present.
unknown-namespace 0	An unexpected name space is present.
access-denied 0	Access to a requested NETCONF session is denied because authorization failed.
lock-denied 0	Access to a requested lock is denied because the lock is currently in use.
resource-denied 0	A request could not be completed because of insufficient resources.
rollback-failed 0	A request to roll back a configuration change was not completed.
data-exists 0	A request could not be completed because the relevant content already exists.
data-missing 0	A request could not be completed because the relevant content does not exist.

Table 80 show netconf Field Descriptions (continued)

Field	Description
operation-not-supported 0	A request could not be completed because the requested operation is not supported.
operation-failed 0	A request could not be completed because the requested operation failed for a reason not specified by another error notice.
partial-operation 0	Part of a requested operation failed or was not attempted.
(Current | max) sessions: 3 | 4	Number of current NETCONF sessions and the maximum number of concurrent NETCONF sessions allowed.
Operations received: 100	Number of NETCONF operations received.
Operation errors: 99	Number of NETCONF operation errors.
Connection Requests: 5	Number of NETCONF connection requests.
Authentication errors: 2	Number of NETCONF authentication errors.
Connection Failures: 0	Number of unsuccessful NETCONF session connections.
ACL dropped: 30	Number of NETCONF sessions dropped due to an access list.
Notifications Sent: 20	Number of NETCONF notifications sent.

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
netconf ssh	Enables NETCONF over SSHv2.

show ntp associations

To display the status of Network Time Protocol (NTP) associations, use the **show ntp associations** command in user EXEC or privileged EXEC mode.

show ntp associations [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about each NTP association.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	Support for IPv6 was added.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Examples

Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

The following is sample output from the **show ntp associations** command:

```
Router> show ntp associations

     address         ref clock     st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Table 81 describes the significant fields shown in the display.

Table 81 show ntp associations Field Descriptions

Field	Description
address	Address of the peer.
ref clock	Address of the reference clock of the peer.
st	Stratum of the peer.
when	Time since the last NTP packet was received from the peer (in seconds).

Table 81 show ntp associations Field Descriptions (continued)

Field	Description
poll	Polling interval (in seconds).
reach	Peer reachability (bit string, in octal).
delay	Round-trip delay to the peer (in milliseconds).
offset	Relative time of the peer clock to the local clock (in milliseconds).
disp	Dispersion.
*	Synchronized to this peer.
#	Almost synchronized to this peer.
+	Peer selected for possible synchronization.
-	Peer is a candidate for selection.
~	Peer is statically configured.

The following is sample output from the **show ntp associations detail** command:

```
Router> show ntp associations detail

172.31.32.2 configured, insane, invalid, stratum 5
ref ID 172.31.32.1, time AFE252C1.6DBDDFF2 (00:12:01.428 PDT Mon Jul 5 1993)
our mode active, peer mode active, our poll intvl 1024, peer poll intvl 64
root delay 137.77 msec, root disp 142.75, reach 376, sync dist 215.363
delay 4.23 msec, offset -8.587 msec, dispersion 1.62
precision 2**19, version 3
org time AFE252E2.3AC0E887 (00:12:34.229 PDT Mon Jul 5 1993)
rcv time AFE252E2.3D7E464D (00:12:34.240 PDT Mon Jul 5 1993)
xmt time AFE25301.6F83E753 (00:13:05.435 PDT Mon Jul 5 1993)
filtdelay =     4.23    4.14    2.41    5.95    2.37    2.33    4.26    4.33
filtoffset =   -8.59   -8.82   -9.91   -8.42  -10.51  -10.77  -10.13  -10.11
filterror =     0.50    1.48    2.46    3.43    4.41    5.39    6.36    7.34

192.168.13.33 configured, selected, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE24F0E.14283000 (23:56:14.078 PDT Sun Jul 4 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 83.72 msec, root disp 217.77, reach 377, sync dist 264.633
delay 4.07 msec, offset 3.483 msec, dispersion 2.33
precision 2**6, version 3
org time AFE252B9.713E9000 (00:11:53.442 PDT Mon Jul 5 1993)
rcv time AFE252B9.7124E14A (00:11:53.441 PDT Mon Jul 5 1993)
xmt time AFE252B9.6F625195 (00:11:53.435 PDT Mon Jul 5 1993)
filtdelay =     6.47    4.07    3.94    3.86    7.31    7.20    9.52    8.71
filtoffset =    3.63    3.48    3.06    2.82    4.51    4.57    4.28    4.59
filterror =     0.00    1.95    3.91    4.88    5.84    6.82    7.80    8.77

192.168.13.57 configured, our_master, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE252DC.1F2B3000 (00:12:28.121 PDT Mon Jul 5 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 125.50 msec, root disp 115.80, reach 377, sync dist 186.157
delay 7.86 msec, offset 11.176 msec, dispersion 3.62
precision 2**6, version 2
org time AFE252DE.77C29000 (00:12:30.467 PDT Mon Jul 5 1993)
rcv time AFE252DE.7B2AE40B (00:12:30.481 PDT Mon Jul 5 1993)
xmt time AFE252DE.6E6D12E4 (00:12:30.431 PDT Mon Jul 5 1993)
filtdelay =    49.21    7.86    8.18    8.80    4.30    4.24    7.58    6.42
filtoffset =   11.30   11.18   11.13   11.28    8.91    9.09    9.27    9.57
```

```
filterror =     0.00    1.95    3.91    4.88    5.78    6.76    7.74    8.71
```

Table 82 describes the significant fields shown in the display.

Table 82 show ntp associations detail Field Descriptions

Field	Descriptions
configured	Peer was statically configured.
insane	Peer fails basic checks.
invalid	Peer time is believed to be invalid.
ref ID	Address of the machine the peer is synchronized to.
time	Last time stamp the peer received from its master.
our mode	Mode of the source relative to the peer (active/passive/client/server/bdcast/bdcast client).
peer mode	Peer's mode relative to the source.
our poll intvl	Source poll interval to the peer.
peer poll intvl	Peer's poll interval to the source.
root delay	Delay (in milliseconds) along the path to the root (ultimate stratum 1 time source).
root disp	Dispersion of the path to the root.
reach	Peer reachability (bit string in octal).
sync dist	Peer synchronization distance.
delay	Round-trip delay to the peer (in milliseconds).
offset	Offset of the peer clock relative to the system clock.
dispersion	Dispersion of the peer clock.
precision	Precision of the peer clock in Hertz.
version	NTP version number that the peer is using.
org time	Originate time stamp.
rcv time	Receive time stamp.
xmt time	Transmit time stamp.
filtdelay	Round-trip delay (in milliseconds) of each sample.
filtoffset	Clock offset (in milliseconds) of each sample.
filterror	Approximate error of each sample.
sane	Peer passes basic checks.
selected	Peer is selected for possible synchronization.
valid	Peer time is believed to be valid.
our_master	Local machine is synchronized to this peer.

Related Commands

Command	Description
show ntp status	Displays the status of the NTP.

show ntp status

To display the status of the Network Time Protocol (NTP), use the **show ntp status** command in user EXEC or privileged EXEC mode.

show ntp status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	Support for IPv6 was added.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Examples

The following is sample output from the **show ntp status** command:

```
Router> show ntp status

Clock is synchronized, stratum 4, reference is 192.168.13.57
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is AFE2525E.70597B34 (00:10:22.438 PDT Mon Jul 5 1993)
clock offset is 7.33 msec, root delay is 133.36 msec
root dispersion is 126.28 msec, peer dispersion is 5.98 msec
```

Table 83 describes the significant fields shown in the display.

Table 83 show ntp status Field Descriptions

Field	Description
synchronized	System is synchronized to an NTP peer.
stratum	NTP stratum of this system.
reference	Address of the peer the system is synchronized to.
nominal freq	Nominal frequency of the system hardware clock (in Hertz).
actual freq	Measured frequency of the system hardware clock (in Hertz).
precision	Precision of the clock of this system (in Hertz).

Table 83 show ntp status Field Descriptions (continued)

Field	Description
reference time	Reference time stamp.
clock offset	Offset of the system clock to the synchronized peer (in milliseconds).
root delay	Total delay along the path to the root clock (in milliseconds).
root dispersion	Dispersion of the root path.
peer dispersion	Dispersion of the synchronized peer.

Related Commands

Command	Description
show ntp associations	Displays the status of the NTP associations.