Customizing the Display of CEF Event Trace Messages

This module contains information about and instructions for customizing the display of recorded Cisco Express Forwarding events.

You can customize the Cisco Express Forwarding event-tracing message display by specifying the size of the file stored in memory or by choosing to display event trace messages by prefix and mask, by a specified interface, or by a Cisco Express Forwarding Virtual Private Network (VPN) routing and forwarding instance (VRF) for an IPv4 or IPv6 address family.

Cisco Express Forwarding is an advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks: those that carry small amounts of traffic and those that carry large amounts of traffic in complex patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for the Display of CEF Event Trace Messages

Cisco Express Forwarding must be running on the networking device before you can customize the display of recorded Cisco Express Forwarding events.

Restrictions for the Display of CEF Event Trace Messages

If you enable Cisco Express Forwarding and then create an access list that uses the **log** keyword, the packets that match the access list are not Cisco Express Forwarding switched. They are process switched. Logging disables Cisco Express Forwarding.

Information About the Display of CEF Event Trace Messages

Cisco Platform Support for Central CEF and dCEF

Cisco Express Forwarding is enable by default on the Cisco ASR 1000 Series Aggregation Services Routers.

To find out if Cisco Express Forwarding is enabled on your platform, enter the **show ip cef**command. If Cisco Express Forwarding is enabled, you receive output that looks like this:

```
Router# show ip cef
Prefix              Next Hop            Interface
[...]
10.2.61.8/24        192.168.100.1       FastEthernet1/0/0
                    192.168.101.1       FastEthernet2/1/0
[...]
```

If Cisco Express Forwarding is not enabled on your platform, the output for the **show ip cef**command looks like this:

```
Router# show ip cef
%CEF not running
```

If Cisco Express Forwarding is not enabled on your platform, use the **ip cef**command to enable (central) Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

Overview of CEF Event Trace Function

The Cisco Express Forwarding event trace function collects Cisco Express Forwarding events as they occur, even when debugging is not enabled. This function allows the tracing of an event immediately after it occurs. Cisco technical personnel can use the event trace function to help resolve any problems with the Cisco Express Forwarding feature.

Cisco Express Forwarding event trace messages are saved in memory on the device. When the event trace messages exceed the configured size, the newest message in the trace will begin to overwrite the older messages. You can use the following commands to change the capacity of the Cisco Express Forwarding event message file:

- The **monitor event-trace cef events size**global configuration command allows you to increase or decrease the number of messages that can be written to memory for a single instance of a trace. To display the size parameter, use the **show monitor event-trace events parameters** command.
- The **monitor event-trace cef events clear** privileged EXEC command allows you to clear existing trace messages.
- The **monitor event-trace cef**(global) command configures event tracing for Cisco Express Forwarding events. To monitor and control the event trace function for Cisco Express Forwarding events, use the **monitor event-trace cef** (EXEC) command.

You can use the following commands to display Cisco Express Forwarding events:

- The **show monitor event-trace cef all**command displays all event trace messages currently in memory for Cisco Express Forwarding.
- The **debug ip cef** command and the **events** keyword record general Cisco Express Forwarding events as they occur.
- The **debug ip cef table**command enables the real-time collection of events that affect entries in the Cisco Express Forwarding tables.

CEF Event Tracing Defaults and Options

Event tracing for distributed Cisco Express Forwarding events is enabled by default. The Cisco IOS XE software allows Cisco Express Forwarding to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value in one of two ways: using the **monitor event-trace cef**command in privileged EXEC mode or using the **monitor event-trace cef**command in global configuration mode.

To configure the file in which you want to save trace information, use the **monitor event-trace cef**command in global configuration mode. By default, the trace messages are saved in a binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the **monitor event-trace cef dump pretty** command in privileged EXEC mode. The amount of data collected from a trace depends on the trace message size configured using the **monitor event-trace cef**command in global configuration mode for each instance of a trace.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

CEF Event Tracing for IPv4 Events

Event tracing for Cisco Express Forwarding IPv4 events is enabled by default. The software allows Cisco Express Forwarding to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value in one of two ways: using the **monitor event-trace cef ipv4**command in privileged EXEC mode or using the **monitor event-trace cef ipv4**command in global configuration mode.

To configure the file in which you want to save trace information for Cisco Express Forwarding IPv4 events, use the **monitor event-trace cef ipv4**command in global configuration mode. By default, the trace messages are saved in a binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the **monitor event-trace cef ipv4 dump pretty** command in privileged EXEC mode. The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace cef ipv4**command for each instance of a trace.

To determine whether event tracing is enabled by default for Cisco Express Forwarding, use the **show monitor event-trace cef ipv4**command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

CEF Event Tracing for IPv6 Events

Event tracing for Cisco Express Forwarding IPv6 events is enabled by default.The Cisco IOS XE software allows Cisco Express Forwarding to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value in one of two ways: using the **monitor event-trace cef ipv6**command in privileged EXEC mode or using the **monitor event-trace cef ipv6**command in global configuration mode.

To configure the file in which you want to save trace information for Cisco Express Forwarding IPv6 events, use the **monitor event-trace cef ipv6**command in global configuration mode. By default, the trace messages are saved in a binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the **monitor event-trace cef ipv6 dump pretty** command in privileged EXEC mode. The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace cef ipv6**command for each instance of a trace.

To determine whether event tracing is enabled by default for Cisco Express Forwarding, use the **show monitor event-trace cef ipv6**command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

How to Customize the Display of CEF Event Trace Messages

Perform the following tasks to customize the Cisco Express Forwarding event tracing function and to display event trace messages:

Customizing CEF Event Tracing

Perform the following task to customize Cisco Express Forwarding event tracing. Event trace messages can be used to monitor Cisco Express Forwarding and to help resolve any issues with the Cisco Express Forwarding feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor event-trace cef** {**dump-file** *dump-file-name* | {**events** | **interface**} {**disable** | **dump-file** *dump-file-name*| **enable** | **size** *number* | **stacktrace** [*depth*]}}
4. **exit**
5. **monitor event-trace cef** {**dump** [**merged pretty** | **pretty**] | {**events** | **interface** | **ipv4** | **ipv6**} {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}}
6. **disable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**monitor event-trace cef** {**dump-file** *dump-file-name* | {**events** | **interface**} {**disable** | **dump-file** *dump-file-name*| **enable** | **size** *number* | **stacktrace** [*depth*]}} **Example:** `Router(config)# monitor event-trace cef dump-file tftp://172.16.10.5/cef-events`	Configures event tracing for Cisco Express Forwarding. • The **dump-file** *dump-file-name* keyword and argument pair specify the file to which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server. • The **events**keyword turns on event tracing for Cisco Express Forwarding events. • The **interface** keyword turns on event tracing for Cisco Express Forwarding interface events. • The **disable** keyword turns off event tracing for Cisco Express Forwarding events. • The **enable** keyword turns on event tracing for Cisco Express Forwarding events if it had been enabled with the **monitor event-trace cef** privileged EXEC command. • The **size** *number* keyword and argument pair sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536. **Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace cef events parameters** command. • The **stacktrace** keyword enables the stack trace at tracepoints. • The *depth* argument specifies the depth of the stack trace stored. Range: 1 to 16.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**monitor event-trace cef** {**dump** [**merged pretty** | **pretty**] | {**events** | **interface** | **ipv4** | **ipv6**} {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}} **Example:** `Router# monitor event-trace cef events dump pretty`	Monitors and controls the event trace function for Cisco Express Forwarding. • The **dump** keyword writes the event trace results to the file configured with the **monitor event-trace cef**global configuration command. The trace messages are saved in binary format. • The **merged pretty** keywords sort all event trace entries by time and write the entries to a file in ASCII format. • The **pretty** keyword saves the event trace message in ASCII format. • The **events** keyword monitors Cisco Express Forwarding events. • The **interface**keyword monitors Cisco Express Forwarding interface events. • The **ipv4**keyword monitors Cisco Express Forwarding IPv4 events. • The **ipv6** keyword monitors Cisco Express Forwarding IPv6 events. • The **clear** keyword clears existing trace messages for Cisco Express Forwarding from memory on the networking device. • The **continuous** keyword continuously displays the latest event trace entries. • The **cancel** keyword cancels the continuous display of the latest trace entries. • The **disable** keyword turns off Cisco Express Forwarding event tracing. • The **enable** keyword turns on Cisco Express Forwarding event tracing. • The **one-shot** keyword Clears any existing trace information from memory, starts event tracing again, and disables the trace when the size of the trace message file configured in the global configuration command is exceeded.
Step 6	**disable** **Example:** `Router# disable`	Exits to user EXEC mode.

Customizing CEF Event Tracing for IPv4 Events

Perform the following task to customize Cisco Express Forwarding event tracing for Cisco Express Forwarding IPv4 events. Use event tracing to monitor Cisco Express Forwarding IPv4 events as they occur and to help resolve any issues with Cisco Express Forwarding and related IPv4 events.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor event-trace cef ipv4** {**disable** | **distribution** |**dump-file** *dump-file-name*| **enable** | **match** {**global** | *ip-address mask*} | **size** *number* | **stacktrace** [*depth*] | **vrf** *vrf-name* [**distribution** | **match** {**global** | *ip-address mask*}]}
4. **exit**
5. **monitor event-trace cef ipv4** {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}
6. **disable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**monitor event-trace cef ipv4** {**disable**	**distribution** |**dump-file** *dump-file-name*| **enable**	**match** {**global**	*ip-address mask*}	**size** *number*	**stacktrace** [*depth*]	**vrf** *vrf-name* [**distribution**	**match** {**global**	*ip-address mask*}]} **Example:** `Router(config)# monitor event-trace cef ipv4 size 10000`	Configures event-tracing for Cisco Express Forwarding IPv4 events. • The **disable** keyword turns off event tracing for Cisco Express Forwarding IPv4 events. • The **distribution** keyword logs events related to the distribution of Cisco Express Forwarding Forwarding Information Base (FIB) tables to the line cards • The **dump-file** *dump-file-name* keyword and argument pair specify the file to which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server. • The **enable** keyword turns on event tracing for Cisco Express Forwarding IPv4 events if it had been enabled with the **monitor event-trace cef** privileged EXEC command. • The **match**keyword turns on event tracing for Cisco Express Forwarding IPv4 events that matches global events or events that match a specific network address • The **global**keyword specifies global events. • The *ip-address mask*argumentsspecify an IP address in A.B.C.D format and a subnet mask in A.B.C.D format.

	Command or Action	Purpose
		• The **size** *number* keyword and argument pair sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536. **Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace cef ipv4 parameters** command. • The **stacktrace** keyword enables the stack trace at tracepoints. • The *depth* argument specifies the depth of the stack trace stored. Range: 1 to 16. • The **vrf** *vrf-name* keyword and argument pair turns on event tracing for a Cisco Express Forwarding IPv4 VRF table. The *vrf-name* argument specifies the name of the VRF
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.
Step 5	**monitor event-trace cef ipv4** {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**} **Example:** `Router# monitor event-trace cef ipv4 continuous`	Monitors and controls the event trace function for Cisco Express Forwarding IPv4 events. • The **clear** keyword clears existing trace messages for Cisco Express Forwarding from memory on the networking device. • The **continuous** keyword continuously displays the latest event trace entries. • The **cancel** keyword cancels the continuous display of the latest trace entries. • The **disable** keyword turns off Cisco Express Forwarding event tracing. • The **dump** keyword writes the event trace results to the file configured with the global configuration **monitor event-trace cef** command. The trace messages are saved in binary format. • The **pretty** keyword saves the event trace message in ASCII format. • The **enable** keyword turns on Cisco Express Forwarding event tracing. • The **one-shot** keyword clears any existing trace information from memory, starts event tracing again, and disables the trace when the size of the trace message file configured in the global configuration command is exceeded.
Step 6	**disable** **Example:** `Router# disable`	Exits to user EXEC mode.

Customizing CEF Event Tracing for IPv6 Events

Perform the following task to customize Cisco Express Forwarding event tracing for Cisco Express Forwarding IPv6 events.Use event tracing to monitor Cisco Express Forwarding IPv6 events as they occur and to help resolve any issues with Cisco Express Forwarding and related IPv6 events.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor event-trace cef ipv4** {**disable** | **distribution** | **dump-file** *dump-file-name*| **enable** | **match** {**global** | *ipv6-address/n*} | **size** *number* | **stacktrace** [*depth*] | **vrf** *vrf-name* [**distribution** | **match** {**global** | *ipv6-address/n}*]}
4. **exit**
5. **monitor event-trace cef ipv6** {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}}
6. **disable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**monitor event-trace cef ipv4** {**disable**	**distribution**	**dump-file** *dump-file-name*| **enable**	**match** {**global**	*ipv6-address/n*}	**size** *number*	**stacktrace** [*depth*]	**vrf** *vrf-name* [**distribution**	**match** {**global**	*ipv6-address/n}*]} **Example:** `Router(config)# monitor event-trace cef ipv6 match global`	Configures event-tracing for Cisco Express Forwarding IPv6 events. • The **disable** keyword turns off event tracing for Cisco Express Forwarding IPv6 events. • The **distribution** keyword logs events related to the distribution of Cisco Express Forwarding FIB tables to the line cards. • The **dump-file** *dump-file-name* keyword and argument pair specify the file to which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server. • The **enable** keyword turns on event tracing for Cisco Express Forwarding IPv6 events if it had been enabled with the **monitor event-trace cef** privileged EXEC command.

	Command or Action	Purpose
		• The **match**keyword turns on event tracing for Cisco Express Forwarding IPv6 events that matches global events or events that match a specific network address. • The **global**keyword specifies global events. • The *ipv6-address* / *n*argument specifies an IPv6 address. This address must be in the form documented in RFC 2373: the address is specified in hexadecimals using 16-bit values between colons. The slash followed by a number (/ *n*) indicates the number of bits that do not change. Range: 0 to 128 • The **size** *number* keyword and argument pair sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536. **Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace cef ipv6 parameters** command. • The **stacktrace** keyword enables the stack trace at tracepoints. • The *depth* argument specifies the depth of the stack trace stored. Range: 1 to 16. • The **vrf** *vrf-name* keyword and argument pair turns on event tracing for a Cisco Express Forwarding IPv6 VRF table. The *vrf-name* argument specifies the name of the VRF
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.
Step 5	**monitor event-trace cef ipv6** {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}} **Example:** `Router# monitor event-trace cef ipv6 one-shot`	Monitors and controls the event trace function for Cisco Express Forwarding IPv6 events. • The **clear** keyword clears existing trace messages for Cisco Express Forwarding from memory on the networking device. • The **continuous** keyword continuously displays the latest event trace entries. • The **cancel** keyword cancels the continuous display of the latest trace entries. • The **disable** keyword turns off Cisco Express Forwarding event tracing. • The **dump** keyword writes the event trace results to the file configured with the global configuration **monitor event-trace cef** command. The trace messages are saved in binary format. • The **pretty** keyword saves the event trace message in ASCII format. • The **enable** keyword turns on Cisco Express Forwarding event tracing. • The **one-shot** keyword Clears any existing trace information from memory, starts event tracing again, and disables the trace when the size of the trace message file configured in the global configuration command is exceeded.

	Command or Action	Purpose
Step 6	**disable** **Example:** `Router# disable`	Exits to privileged EXEC mode.

Displaying CEF Event Trace Information

Perform the following task to display Cisco Express Forwarding event trace information.

SUMMARY STEPS

1. **enable**
2. **monitor event-trace cef events clear**
3. **debug ip cef table**
4. **show monitor events-trace cef all**
5. **show monitor event-trace cef latest**
6. **show monitor event-trace cef events all**
7. **show monitor event-trace cef interface latest**
8. **show monitor event-trace cef ipv4 all**
9. **show monitor event-trace cef ipv6 parameters**
10. **disable**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

Example:

```
Router> enable
Router#
```

Step 2 **monitor event-trace cef events clear**

Use this command to clear the Cisco Express Forwarding event trace buffer. For example:

```
Router# monitor event-trace cef clear
```

Example:

Step 3 **debug ip cef table**

Use this command to display events that affect entries in the Cisco Express Forwarding tables. For example:

Example:

```
Router# debug ip cef table
01:25:46:CEF-Table:Event up, 10.1.1.1/32 (rdbs:1, flags:1000000)
01:25:46:CEF-IP:Checking dependencies of 0.0.0.0/0
01:25:47:CEF-Table:attempting to resolve 10.1.1.1/32
01:25:47:CEF-IP:resolved 10.1.1.1/32 via 10.9.104.1 to 10.9.104.1 Ethernet2/0/0
01:26:02:CEF-Table:Event up, default, 0.0.0.0/0 (rdbs:1, flags:400001)
01:26:02:CEF-IP:Prefix exists - no-op change
```

Step 4 **show monitor events-trace cef all**

Use this command to display event trace messages for Cisco Express Forwarding. For example:

Example:

```
Router# show monitor event-trace cef all
cef_events:
*Jul 22 20:14:58.999: SubSys  ipv4fib_ios_def_cap init
*Jul 22 20:14:58.999: SubSys  ipv6fib_ios_def_cap init
*Jul 22 20:14:58.999: Inst    unknown -> RP
*Jul 22 20:14:58.999: SubSys  fib_ios_chain init
*Jul 22 20:14:59.075: SubSys  fib init
*Jul 22 20:14:59.075: SubSys  ipv4fib init
*Jul 22 20:14:59.075: SubSys  fib_ios init
*Jul 22 20:14:59.075: SubSys  fib_ios_if init
*Jul 22 20:14:59.075: SubSys  ipv4fib_ios init
*Jul 22 20:14:59.075: Flag    Common CEF enabled set to yes
*Jul 22 20:14:59.075: Flag    IPv4 CEF enabled set to yes
*Jul 22 20:14:59.075: Flag    IPv4 CEF switching enabled set to yes
*Jul 22 20:14:59.075: GState  CEF enabled
*Jul 22 20:14:59.075: SubSys  ipv6fib_ios init
*Jul 22 20:14:59.075: SubSys  ipv4fib_util init
*Jul 22 20:14:59.075: SubSys  ipv4fib_les init
*Jul 22 20:15:02.907: Process Background created
*Jul 22 20:15:02.907: Flag    IPv4 CEF running set to yes
*Jul 22 20:15:02.907: Process Background event loop enter
*Jul 22 20:15:02.927: Flag    IPv4 CEF switching running set to yes

cef_interface:
*Jul 22 20:14:58.999: Et0/0        (hw  3) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/1        (hw  4) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/2        (hw  5) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/3        (hw  6) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et1/0        (hw  7) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et1/1        (hw  8) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et1/2        (hw  9) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et1/3        (hw 10) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Se2/0        (hw 11) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Se2/1        (hw 12) SWvecLES <unknown> (0x01096A3C)
.
.
.
```

The output is in table format where the first column contains a time stamp, the second column lists the type of event, and the third column lists the detail for the event.

Step 5 **show monitor event-trace cef latest**

Use this command to display only the event trace message that have been sent since the last instance of the **show monitor event-trace cef** command. For example:

Example:

```
Router# show monitor event-trace cef latest
cef_events:
cef_interface:
*Jul 22 20:14:59.075: Se3/0        (sw 15) FlagCha  0x60C1 add puntLC
*Jul 22 20:14:59.075: <empty>      (hw 16) State    down -> up
*Jul 22 20:14:59.075: <empty>      (hw 16) Create   new
*Jul 22 20:14:59.075: Se3/1        (hw 16) NameSet
*Jul 22 20:14:59.075: Se3/1        (hw 16) HWIDBLnk Serial3/1(16)
*Jul 22 20:14:59.075: Se3/1        (hw 16) RCFlags  None -> Fast
*Jul 22 20:14:59.075: <empty>      (sw 16) VRFLink  IPv4:id0 - success
*Jul 22 20:14:59.075: <empty>      (sw 16) State    deleted -> down
*Jul 22 20:14:59.075: <empty>      (sw 16) Create   new
*Jul 22 20:14:59.075: Se3/1        (sw 16) NameSet
*Jul 22 20:14:59.075: Se3/1        (sw 16) FIBHWLnk Serial3/1(16)
*Jul 22 20:14:59.075: Se3/1        (sw 16) SWIDBLnk Serial3/1(16)
*Jul 22 20:14:59.075: Se3/1        (sw 16) FlagCha  0x6001 add p2p|input|first
*Jul 22 20:14:59.075: Se3/1        (sw 16) FlagCha  0x6041 add auto_adj
*Jul 22 20:14:59.075: Se3/1        (sw 16) Impared  lc rea Queueing configuration
*Jul 22 20:14:59.075: Se3/1        (sw 16) FlagCha  0x60C1 add puntLC
*Jul 22 20:14:59.075: <empty>      (hw 17) State    down -> up
*Jul 22 20:14:59.075: <empty>      (hw 17) Create   new
*Jul 22 20:14:59.075: Se3/2        (hw 17) NameSet
```

Step 6 **show monitor event-trace cef events all**

Use this command to display information about Cisco Express Forwarding events. For example:

Example:

```
Router# show monitor event-trace cef events all
*Jul 13 17:38:27.999: SubSys  ipv4fib_ios_def_cap init
*Jul 13 17:38:27.999: SubSys  ipv6fib_ios_def_cap init
*Jul 13 17:38:27.999: Inst    unknown -> RP
*Jul 13 17:38:27.999: SubSys  fib_ios_chain init
*Jul 13 17:38:28.199: SubSys  fib init
*Jul 13 17:38:28.199: SubSys  ipv4fib init
*Jul 13 17:38:28.199: SubSys  fib_ios init
*Jul 13 17:38:28.199: SubSys  fib_ios_if init
*Jul 13 17:38:28.199: SubSys  ipv4fib_ios init
*Jul 13 17:38:28.199: Flag    Common CEF enabled set to yes
*Jul 13 17:38:28.199: Flag    IPv4 CEF enabled set to yes
*Jul 13 17:38:28.199: Flag    IPv4 CEF switching enabled set to yes
*Jul 13 17:38:28.199: GState  CEF enabled
*Jul 13 17:38:28.199: SubSys  ipv6fib_ios init
*Jul 13 17:38:28.199: SubSys  ipv4fib_util init
*Jul 13 17:38:28.199: SubSys  ipv4fib_les init
*Jul 13 17:38:34.059: Process Background created
*Jul 13 17:38:34.059: Flag    IPv4 CEF running set to yes
*Jul 13 17:38:34.059: Process Background event loop enter
*Jul 13 17:38:34.079: Flag    IPv4 CEF switching running set to yes
```

The output is in table format where the first column contains a time stamp, the second column lists the type of event, and the third column lists the detail for the event.

For example, the Subsys event type is related to the initialization of a subset of Cisco Express Forwarding functionality. The "ipv4fib_ios_def_cap init" entry is the initialization of IPv4 Cisco Express Forwarding default capabilities.

Step 7 **show monitor event-trace cef interface latest**

Use this command to display only the event trace messages generated since the last **show monitor event-trace cef interface**command was entered. For example:

Example:

```
Router# show monitor event-trace cef interface latest
*Jul 22 20:14:58.999: Et0/0        (hw  3) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/1        (hw  4) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/2        (hw  5) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/3        (hw  6) SWvecLES <unknown> (0x01096A3C)
.
.
.
*Jul 22 20:14:59.075: <empty>      (hw  3) State    down -> up
*Jul 22 20:14:59.075: <empty>      (hw  3) Create   new
*Jul 22 20:14:59.075: Et0/0        (hw  3) NameSet
*Jul 22 20:14:59.075: Et0/0        (hw  3) HWIDBLnk Ethernet0/0(3)
*Jul 22 20:14:59.075: Et0/0        (hw  3) RCFlags  None -> Fast
*Jul 22 20:14:59.075: <empty>      (sw  3) VRFLink  IPv4:id0 - success
*Jul 22 20:14:59.075: <empty>      (sw  3) State    deleted -> down
*Jul 22 20:14:59.075: <empty>      (sw  3) Create   new
*Jul 22 20:14:59.075: Et0/0        (sw  3) NameSet
*Jul 22 20:14:59.075: Et0/0        (sw  3) FIBHWLnk Ethernet0/0(3)
*Jul 22 20:14:59.075: Et0/0        (sw  3) SWIDBLnk Ethernet0/0(3)
*Jul 22 20:14:59.075: Et0/0        (sw  3) FlagCha  0x6000 add input|first
*Jul 22 20:14:59.075: Et0/0        (sw  3) State    down -> up
*Jul 22 20:14:59.075: <empty>      (hw  4) State    down -> up
*Jul 22 20:14:59.075: <empty>      (hw  4) Create   new
*Jul 22 20:14:59.075: Et0/1        (hw  4) NameSet
*Jul 22 20:14:59.075: Et0/1        (hw  4) HWIDBLnk Ethernet0/1(4)
*Jul 22 20:14:59.075: Et0/1        (hw  4) RCFlags  None -> Fast
*Jul 22 20:14:59.075: <empty>      (sw  4) VRFLink  IPv4:id0 - success
*Jul 22 20:14:59.075: <empty>      (sw  4) State    deleted -> down
*Jul 22 20:14:59.075: <empty>      (sw  4) Create   new
*Jul 22 20:14:59.075: Et0/1        (sw  4) NameSet
*Jul 22 20:14:59.075: Et0/1        (sw  4) FIBHWLnk Ethernet0/1(4)
*Jul 22 20:14:59.075: Et0/1        (sw  4) SWIDBLnk Ethernet0/1(4)
*Jul 22 20:14:59.075: Et0/1        (sw  4) FlagCha  0x6000 add input|first
*Jul 22 20:14:59.075: Et0/1        (sw  4) State    down -> up
.
.
.
```

Step 8 **show monitor event-trace cef ipv4 all**

Use this command to display information about Cisco Express Forwarding IPv4 events. For example:

Example:

```
Router# show monitor event-trace cef ipv4 all
*Jul 22 20:14:59.075:  [Default] *.*.*.*/*             Allocated FIB table
                      [OK]
*Jul 22 20:14:59.075:  [Default] *.*.*.*/*'00          Add source Default table
                      [OK]
*Jul 22 20:14:59.075:  [Default] 0.0.0.0/0'00          FIB add src DRH (ins)
                      [OK]
*Jul 22 20:14:59.075:  [Default] *.*.*.*/*'00          New FIB table
                      [OK]
*Jul 22 20:15:02.927:  [Default] *.*.*.*/*'00          FIB refresh start
                      [OK]
.
.
.
```

Step 9 **show monitor event-trace cef ipv6 parameters**

Use this commands to display parameters configured for Cisco Express Forwarding IPv6 events. For example:

Example:

```
Router# show monitor event-trace cef ipv6 parameters
Trace has 1000 entries
Stacktrace is disabled by default
Matching all events
```

Step 10 **disable**

Use this command to exit to user EXEC mode. For example:

Example:

```
Router# disable
Router>
```

Configuration Examples for the Display of CEF Event Trace Messages

Customizing CEF Event Tracing Examples

The following example shows how to enable event tracing for Cisco Express Forwarding and configure the buffer size to 2500 messages. The trace messages file is set to cef-dump in slot0 (flash memory).

```
configure terminal
!
monitor event-trace cef events enable
monitor event-trace cef dump-file slot0:cef-dump
monitor event-trace cef events size 2500
exit
The following example shows what happens when you try to enable event tracing for Cisco
Express Forwarding events when it is already enabled:
configure terminal
!
monitor event-trace cef events enable
00:04:33: %EVENT_TRACE-6-ENABLE: Trace already enabled.
```

The following example shows the privileged EXEC commands that stop event tracing, clear the current contents of memory, and reenable the trace function for Cisco Express Forwarding events. This example assumes that the tracing function is configured and enabled on the networking device.

```
enable
!
monitor event-trace cef events disable
monitor event-trace cef events clear
monitor event-trace cef events enable
disable
```

Example Customizing CEF Event Tracing for IPv4 Events

The following example shows how to enable event tracing for Cisco Express Forwarding IPv4 events and configure the buffer size to 5000 messages:

```
configure terminal
!
monitor event-trace cef ipv4 enable
monitor event-trace cef ipv4 size 5000
exit
The following example shows how to enable event tracing for events that match Cisco Express
 Forwarding IPv4 VRF vpn1:
configure terminal
!
monitor event-trace cef ipv4 enable
monitor event-trace cef ipv4 vrf vpn1
exit
```

The following example shows the privileged EXEC commands to configure the continuous display of the latest Cisco Express Forwarding event trace entries for IPv4 events:

```
enable
!
monitor event-trace cef ipv4 continuous
disable
```

The following example shows how to stop the continuous display of the latest trace entries:

```
enable
!
monitor event-trace cef ipv4 continuous cancel
disable
```

Example Customizing CEF Event Tracing for IPv6 Events

The following example shows how to enable event tracing for Cisco Express Forwarding IPv6 events and configure the buffer size to 10000:

```
configure terminal
!
monitor event-trace cef ipv6 enable
monitor event-trace cef ipv6 size 10000
exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Commands for configuring and managing Cisco Express Forwarding	*Cisco IOS IP Switching Command Reference*
Overview of the Cisco Express Forwarding feature	Cisco Express Forwarding Overview

Related Topic	Document Title
Tasks for verifying basic Cisco Express Forwarding and distributed Cisco Express Forwarding operation	Configuring Basic Cisco Express Forwarding for Improved Performance, Scalability, and Resiliency in Dynamic Networks
Tasks for enabling or disabling Cisco Express Forwarding or distributed Cisco Express Forwarding	Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding to Customize Switching and Forwarding for Dynamic Networks
Tasks for configuring load-balancing schemes for Cisco Express Forwarding	Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic
Tasks for configuring Cisco Express Forwarding consistency checkers	Configuring Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards
Tasks for configuring epochs for Cisco Express Forwarding tables	Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables
Tasks for configuring and verifying Cisco Express Forwarding network accounting	Configuring Cisco Express Forwarding Network Accounting

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the Display of CEF Event Trace Messages

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring the Display of Cisco Express Forwarding Event Trace Messages

Feature Name	Releases	Feature Configuration Information
This table is intentionally left blank because no features were introduced or modified in Cisco IOS XE Release 2.1 or later. This table will be updated when feature information is added to this module.	--	--

Glossary

adjacency --A relationship formed between selected neighboring routers and end nodes for the purpose of exchanging routing information. Adjacency is based upon the use of a common media segment by the routers and nodes involved.

Cisco Express Forwarding --A Layer 3 switching technology. Cisco Express Forwarding can also refer to central Cisco Express Forwarding mode, one of two modes of Cisco Express Forwarding operation. Cisco Express Forwarding enables a Route Processor to perform express forwarding. Distributed Cisco Express Forwarding is the other mode of Cisco Express Forwarding operation.

distributed Cisco Express Forwardin g--A mode of Cisco Express Forwarding operation in which line cards maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Processor of involvement in the switching operation.

FIB --forwarding information base. A component of Cisco Express Forwarding that is conceptually similar to a routing table or information base. The router uses the FIB lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The router maintains a mirror image of the forwarding information in an IP routing table.

line card --A general term for an interface processor that can be used in various Cisco products.

prefix --The network address portion of an IP address. A prefix is specified by a network and mask and is generally represented in the format network/mask. The mask indicates which bits are the network bits. For example, 1.0.0.0/16 means that the first 16 bits of the IP address are masked, making them the network bits. The remaining bits are the host bits. In this example, the network number is 10.0.

VPN --Virtual Private Network. The result of a router configuration that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

VRF --A Virtual Private Network (VPN) routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.