

# ip cache-invalidate-delay

To control the invalidation rate of the IP route cache, use the **ip cache-invalidate-delay** command in global configuration mode. To allow the IP route cache to be immediately invalidated, use the **no** form of this command.

**ip cache-invalidate-delay** [*minimum maximum quiet threshold*]

**no ip cache-invalidate-delay**

## Syntax Description

<i>minimum</i>	(Optional) Minimum time (in seconds) between invalidation request and actual invalidation. The default is 2 seconds.
<i>maximum</i>	(Optional) Maximum time (in seconds) between invalidation request and actual invalidation. The default is 5 seconds.
<i>quiet</i>	(Optional) Length of quiet period (in seconds) before invalidation. The default is 3 seconds with no more than zero invalidation requests.
<i>threshold</i>	(Optional) Maximum number of invalidation requests considered to be quiet.

## Command Default

The invalidation rate of the IP route cache is not controlled.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

After you enter the **ip cache-invalidate-delay** command all cache invalidation requests are honored immediately.



### Caution

This command should only be used under the guidance of technical support personnel. Incorrect settings can seriously degrade network performance. The command-line-interface (CLI) will not allow you to enter the **ip cache-invalidate-delay** command until you configure the **service internal** command in global configuration mode.

The IP fast-switching and autonomous-switching features maintain a cache of IP routes for rapid access. When a packet is to be forwarded and the corresponding route is not present in the cache, the packet is process switched and a new cache entry is built. However, when routing table changes occur (such as when a link or an interface goes down), the route cache must be flushed so that it can be rebuilt with up-to-date routing information.

This command controls how the route cache is flushed. The intent is to delay invalidation of the cache until after routing has settled down. Because route table changes tend to be clustered in a short period of time, and the cache may be flushed repeatedly, a high CPU load might be placed on the router.

When this feature is enabled, and the system requests that the route cache be flushed, the request is held for at least *minimum* seconds. Then the system determines whether the cache has been “quiet” (that is, less than *threshold* invalidation requests in the last *quiet* seconds). If the cache has been quiet, the cache is then flushed. If the cache does not become quiet within *maximum* seconds after the first request, it is flushed unconditionally.

Manipulation of these parameters trades off CPU utilization versus route convergence time. Timing of the routing protocols is not affected, but removal of stale cache entries is affected.

### Examples

The following example shows how to set a minimum delay of 5 seconds, a maximum delay of 30 seconds, and a quiet threshold of no more than 5 invalidation requests in the previous 10 seconds:

```
Router(config)# service internal
Router(config)# ip cache-invalidate-delay 5 30 10 5
```

### Related Commands

Command	Description
<b>ip route-cache</b>	Configures the high-speed switching caches for IP routing.

# ip cef

To enable Cisco Express Forwarding on the route processor card, use the **ip cef** command in global configuration mode. To disable Cisco Express Forwarding, use the **no** form of this command.

**Cisco IAD2420 Series Routers, Cisco 2600 Series Routers, Cisco 3600 Series Routers, Cisco 3700 Series Routers, Cisco 7200 Series Routers**

**ip cef [distributed]**

**no ip cef [distributed]**

**Cisco ASR 1000 Series Aggregation Services Routers**

**ip cef distributed**

**no ip cef distributed**

<b>Syntax Description</b>	<b>distributed</b>	(Optional) Enables distributed Cisco Express Forwarding operation. Distributes Cisco Express Forwarding information to line cards. Line cards perform express forwarding.
---------------------------	--------------------	---

<b>Command Default</b>	Cisco Express Forwarding is enabled by default on most platforms. To find out if Cisco Express Forwarding is enabled by default on your platform, enter the <b>show ip cef</b> command.
------------------------	---

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.1CC	This command was introduced.
	12.2	The default for Cisco 7200 series routers was changed from disabled to enabled.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the following platforms: Cisco IAD2420 series, Cisco 2600 series, Cisco 3620 routers, Cisco 3640 routers, Cisco 3660 routers, Cisco 3700 series routers, and Cisco MC3810 multiservice access concentrators.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	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(20T)	This command was integrated into Cisco IOS Release 12.4(20)T.

**Usage Guidelines**

The **ip cef** command is not available on the Cisco 12000 series because that router series operates only in distributed Cisco Express Forwarding mode. Distributed Cisco Express Forwarding is enabled also on the Cisco 6500 series router.

Cisco Express Forwarding is advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

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 fast switched. Logging disables Cisco Express Forwarding.

The following example shows how to enable standard Cisco Express Forwarding operation:

```
Router(config)# ip cef
```

The following example shows how to enable distributed Cisco Express Forwarding operation:

```
Router(config)# ip cef distributed
```

**Related Commands**

Command	Description
<b>ip route-cache</b>	Controls the use of high-speed switching caches for IP routing.
<b>ip cef accounting</b>	Enables Cisco Express Forwarding network accounting.
<b>ip cef load-sharing algorithm</b>	Selects a Cisco Express Forwarding load balancing algorithm.
<b>ip cef table adjacency-prefix override</b>	Enables Cisco Express Forwarding adjacency prefixes to override static host glean routes.
<b>cef table consistency-check</b>	Enables Cisco Express Forwarding table consistency checker types and parameters.
<b>show ip cef</b>	Displays entries or a summary of the FIB table.

# ip cef accounting

To enable Cisco Express Forwarding network accounting, use the **ip cef accounting** command in global configuration mode or interface configuration mode. To disable network accounting of Cisco Express Forwarding, use the **no** form of this command.

**ip cef accounting** *accounting-types*

**no ip cef accounting** *accounting-types*

## Specific Cisco Express Forwarding Accounting Information Through Interface Configuration Mode

**ip cef accounting non-recursive** { **external** | **internal** }

**no ip cef accounting non-recursive** { **external** | **internal** }

Syntax Description		
<i>accounting-types</i>		The <i>accounting-types</i> argument must be replaced with at least one of the following keywords. Optionally, you can follow this keyword by any or all of the other keywords, but you can use each keyword only once. <ul style="list-style-type: none"> <li>• <b>load-balance-hash</b>—Enables load balancing hash bucket counters.</li> <li>• <b>non-recursive</b>—Enables accounting through nonrecursive prefixes.</li> <li>• <b>per-prefix</b>—Enables express forwarding of the collection of the number of packets and bytes to a destination (or prefix).</li> <li>• <b>prefix-length</b>—Enables accounting through prefix length.</li> </ul>
<b>non-recursive</b>		Enables accounting through nonrecursive prefixes.  This keyword is optional when used in global configuration mode after another keyword is entered. See the <i>accounting-types</i> argument.
<b>external</b>		Counts input traffic in the nonrecursive external bin.
<b>internal</b>		Counts input traffic in the nonrecursive internal bin.

**Command Default** Accounting is disabled by default.

**Command Modes** Global configuration (config)  
Interface configuration (config-if)

Command History	Release	Modification
	11.2GS	This command was introduced.
	11.1CC	Multiple platform support was added and the <b>prefix-length</b> keyword was added.

Release	Modification
12.2(2)T	The <b>ip cef accounting non-recursive</b> command in interface configuration mode was added.
12.2(25)S	The <b>load-balance-hash</b> keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

### Usage Guidelines

Collecting statistics can help you better understand Cisco Express Forwarding patterns in your network.

When you enable network accounting for Cisco Express Forwarding from global configuration mode, accounting information is collected at the Route Processor (RP) when Cisco Express Forwarding mode is enabled and at the line cards when distributed Cisco Express Forwarding mode is enabled. You can then display the collected accounting information using the **show ip cef** privileged EXEC command.

For prefixes with directly connected next hops, the **non-recursive** keyword enables express forwarding of the collection of packets and bytes through a prefix. This keyword is optional when this command is used in global configuration mode.

This command in interface configuration mode must be used in conjunction with the global configuration command. The interface configuration command allows a user to specify two different bins (internal or external) for the accumulation of statistics. The internal bin is used by default. The statistics are displayed through the **show ip cef detail** command.

Per-destination load balancing uses a series of 16 hash buckets into which the set of available paths are distributed. A hash function operating on certain properties of the packet is applied to select a bucket that contains a path to use. The source and destination IP addresses are the properties used to select the bucket for per-destination load balancing. Use the **load-balance-hash** keyword with the **ip cef accounting** command to enable per-hash-bucket counters. Enter the **show ip cef prefix internal** command to display the per-hash-bucket counters.



#### Note

The **ip cef accounting** command is not supported on the Cisco 7600 series router.

### Examples

The following example shows how to enable the collection of Cisco Express Forwarding accounting information for prefixes directly connected to the next hops:

```
Router(config)# ip cef accounting non-recursive
```

### Related Commands

Command	Description
<b>ipv6 cef accounting</b>	Enables Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) network accounting.
<b>show cef</b>	Displays information about packets forwarded by Cisco Express Forwarding.
<b>show ip cef</b>	Displays entries or a summary of the FIB table.

# ip cef linecard ipc memory

To configure the line card memory pool for the Cisco Express Forwarding queuing messages, use the **ip cef linecard ipc memory** command in global configuration mode. To return to the default Inter-process Communications (IPC) memory allocation, use the **no** form of this command.

**ip cef linecard ipc memory** *kbps*

**no ip cef linecard ipc memory** *kbps*

<b>Syntax Description</b>	<i>kbps</i>	Kilobytes of line card memory allocated. Range is 0 to 12800. The default IPC memory allocation is 25 messages. However, this value depends on the switching platform.
---------------------------	-------------	--

**Command Default** If you do not configure a line card memory pool for the Cisco Express Forwarding queuing messages, the default is the IPC memory allocation for the switching platform.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)T	This command was introduced.

**Usage Guidelines** This command is available only on distributed switching platforms.

If you are expecting large routing updates to the Route Processor (RP), use this command to allocate a larger memory pool on the line cards for queuing Cisco Express Forwarding routing update messages. The memory pool reduces the transient memory requirements on the RP.

To display and monitor the current size of the Cisco Express Forwarding message queues, use the **show cef linecard** command. Also, the peak size is recorded and displayed when you use the **detail** keyword.

**Examples** The following example shows how to configure the Cisco Express Forwarding line card memory queue to 128000 kilobytes per second:

```
Router(config)# ip cef linecard ipc memory 128000
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show cef linecard</b>	Displays detailed Cisco Express Forwarding information for the specified line card.

# ip cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm, use the **ip cef load-sharing algorithm** command in global configuration mode. To return to the default universal load-balancing algorithm, use the **no** form of this command.

```
ip cef load-sharing algorithm { original | tunnel [id] | universal [id] | include-ports { source [id]
| [destination] [id] | source [id] destination [id]} }
```

```
no ip cef load-sharing algorithm
```

## Syntax Description

<b>original</b>	Sets the load-balancing algorithm to the original algorithm based on a source and destination hash.
<b>tunnel</b>	Sets the load-balancing algorithm for use in tunnel environments or in environments where there are only a few IP source and destination address pairs.
<i>id</i>	(Optional) Fixed identifier.
<b>universal</b>	Sets the load-balancing algorithm to the universal algorithm that a src ip, a dest ip, a source port, a dest port, an L4 protocol and an ID hash.



### Note

Any changes in these fields can result in the load balance based on the available links. Fragmented packets will be forwarded to two different links by this algorithm.

<b>include-ports source</b>	Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 source port.
<b>include-ports destination</b>	Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 destination port.
<b>include-ports source destination</b>	Sets the load balancing algorithm to the include-ports algorithm that uses Layer 4 source and destination ports.

## Command Default

The universal load-balancing algorithm is selected. If you do not configure the fixed identifier for a load-balancing algorithm, the router automatically generates a unique ID.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.0(12)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.



Release	Modification
12.4(11)T	The <b>include-ports source</b> , <b>include-ports destination</b> , and the <b>include-ports source destination</b> keywords were added for the command.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

### Usage Guidelines

The original Cisco Express Forwarding load-balancing algorithm produced distortions in load sharing across multiple routers because of the use of the same algorithm on every router. When the load-balancing algorithm is set to universal mode, each router on the network can make a different load sharing decision for each source-destination address pair, and that resolves load-balancing distortions.

The tunnel algorithm is designed to share the load more fairly when only a few source-destination pairs are involved.

The include-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal-cost paths that are not loadshared because the majority of the traffic is between peer addresses that use different port numbers, such as Real-Time Protocol (RTP) streams. The include-ports algorithm is available in Cisco IOS Release 12.4(11)T and later releases.

### Examples

The following example shows how to enable the Cisco Express Forwarding load-balancing algorithm for tunnel environments:

```
configure terminal
!
ip cef load-sharing algorithm tunnel
exit
```

### Related Commands

Command	Description
<b>debug ip cef hash</b>	Records Cisco Express Forwarding load-balancing hash algorithm events
<b>ip load-sharing</b>	Enables load balancing for Cisco Express Forwarding.

# ip cef optimize neighbor resolution

To configure address resolution optimization from Cisco Express Forwarding for IPv4 for directly connected neighbors, use the **ip cef optimize neighbor resolution** command in global configuration mode. To disable address resolution optimization from Cisco Express Forwarding for directly connected neighbors, use the **no** form of this command.

**ip cef optimize neighbor resolution**

**no ip cef optimize neighbor resolution**

**Syntax Description** This command has no arguments or keywords.

**Command Default** If this command is not configured, Cisco Express Forwarding does not optimize the address resolution of directly connected neighbors for IPv4.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.2(25)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	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.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

**Usage Guidelines** The **ip cef optimize neighbor resolution** command is very similar to the **ipv6 cef optimize neighbor resolution** command, except that it is IPv4-specific.

Use this command to trigger Layer 2 address resolution of neighbors directly from Cisco Express Forwarding for IPv4.

**Examples** The following example shows how to optimize address resolution from Cisco Express Forwarding for directly connected neighbors:

```
Router(config)# ip cef optimize neighbor resolution
```

Related Commands	Command	Description
	<b>ipv6 cef optimize neighbor resolution</b>	Configures address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors.

# ip cef table adjacency-prefix

To modify how Cisco Express Forwarding adjacency prefixes are managed, use the **ip cef table adjacency-prefix** command in global configuration mode. To disable Cisco Express Forwarding adjacency prefix management, use the **no** form of this command.

**ip cef table adjacency-prefix [override | validate]**

**no ip cef table adjacency-prefix [override | validate]**

## Syntax Description

<b>override</b>	(Optional) Enables Cisco Express Forwarding adjacency prefixes to override static host glean routes.
<b>validate</b>	(Optional) Enables the periodic validation of Cisco Express Forwarding adjacency prefixes.

## Defaults

All Cisco Express Forwarding adjacency prefix management is disabled by default.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.0(16)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.1(13)E07	The <b>validate</b> keyword was added.
12.1(19.02)E	The default behavior for <b>ip cef table adjacency-prefix override</b> was changed to disabled.
12.3(04)XG	
12.3(04)XK	
12.3(06.01)PI03	
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

## Usage Guidelines

When Cisco Express Forwarding is configured, the forwarding information base (FIB) table may conflict with static host routes that are specified in terms of an output interface or created by a Layer 2 address resolution protocols such as Address Resolution Protocol (ARP), map lists, and so on.

The Layer 2 address resolution protocol adds adjacencies to Cisco Express Forwarding, which in turn creates a corresponding host route entry in the FIB table. This entry is called an adjacency prefix.

### override

If the Cisco Express Forwarding adjacency prefix entries are also configured by a static host route, a conflict occurs.

This command ensures that adjacency prefixes can override static host glean routes, and correctly restore routes when the adjacency prefix is deleted.

#### **validate**

When you add a /31 netmask route, the new netmask does not overwrite an existing /32 Cisco Express Forwarding entry. This problem is resolved by configuring the **validate** keyword to periodically validate prefixes derived from adjacencies in the FIB against prefixes originating from the RIB.

---

## **Examples**

#### **override**

The following example shows how to enable Cisco Express Forwarding table adjacency prefix override:

```
Router(config)# ip cef table adjacency-prefix override
```

#### **validate**

The following example shows how to enable Cisco Express Forwarding table adjacency prefix validation:

```
Router(config)# ip cef table adjacency-prefix validate
```

## ip cef table adjacency-prefix

The **override** keyword for the **ip cef table adjacency-prefix** command is no longer documented as a separate command.

The information for using the **override** keyword for the **ip cef table adjacency-prefix** command has been incorporated into the **ip cef table adjacency-prefix** command documentation. See the **ip cef table adjacency-prefix** command documentation for more information.

# ip cef table consistency-check



## Note

Effective with Cisco IOS Release 12.4(20)T, the **ip cef table consistency-check** command is not available in Cisco IOS software.

To enable consistency checker types and parameters for Cisco Express Forwarding tables, use the **ip cef table consistency-check** command in global configuration mode. To disable consistency checkers, use the **no** form of this command.

```
ip cef table consistency-check [type {lc-detect | scan-lc | scan-rib | scan-rp}] [count
  count-number] [period seconds]
```

```
no ip cef table consistency-check [type {lc-detect | scan-lc | scan-rib | scan-rp}] [count
  count-number] [period seconds]
```

## Suppressing Errors During Route Updates

```
ip cef table consistency-check [settle-time seconds]
```

```
no ip cef table consistency-check [settle-time seconds]
```

## Syntax Description

<b>type</b>	(Optional) Specifies the type of consistency check to configure.
<b>lc-detect</b>	(Optional) Specifies that the line card or the module detects a missing prefix. On the line card, a missing prefix is confirmed by Route Processor (RP).
<b>scan-lc</b>	(Optional) Specifies a passive scan check of tables on the line card or module.
<b>scan-rib</b>	(Optional) Specifies a passive scan check of tables on the RP against the Routing Information Base (RIB). For the Cisco 7600 series router, the <b>scan-rib</b> keyword specifies a passive scan check of tables on the rendezvous point against the RIB.
<b>scan-rp</b>	(Optional) Specifies a passive scan check of tables on the RP or on the rendezvous point for the Cisco 7600 series router.
<b>count</b> <i>count-number</i>	(Optional) Specifies the maximum number of prefixes to check per scan. Valid values are from 1 to 225.
<b>period</b> <i>seconds</i>	(Optional) Specifies the period of time between scans. Valid values are from 30 to 3600 seconds.
<b>settle-time</b> <i>seconds</i>	(Optional) Specifies the amount of time that elapsed during which updates for a candidate prefix are ignored as inconsistencies. Valid values are from 1 to 3600 seconds. This keyword is used during route updates.

## Command Default

All consistency checkers are disabled by default.

## Command Modes

Global configuration (config)

**Command History**

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(14)SX	Support for this command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Release 12.2(17d)SXB.
12.2(25)S	This command was replaced by the <b>cef table consistency-check</b> command.
12.2(28)SB	This command was replaced by the <b>cef table consistency-check</b> command.
12.2(33)SRA	This command was replaced by the <b>cef table consistency-check</b> command.
12.2(33)SXH	This command was replaced by the <b>cef table consistency-check</b> command.
12.4(20)T	This command was removed.

**Usage Guidelines**

This command configures Cisco Express Forwarding table consistency checkers and parameters for the detection mechanism types that are listed in [Table 2](#).

**Table 2** CEF Detection Mechanism Types

Detection Mechanism	Where Operates	Description
lc-detect	Line Card or Module	Operates on the line card or module detecting and retrieving IP prefixes that are missing from its FIB table. If IP prefixes are missing, the line card or module cannot forward packets for these addresses. The lc-detect mechanism sends IP prefixes to the RP or rendezvous point for confirmation. If the RP or rendezvous point detects that it has the relevant entry, an inconsistency is identified and an error message is displayed. Also, the RP or rendezvous point sends a signal back to the line card or module confirming that the IP prefix is an inconsistency.
scan-lc	Line Card or Module	Operates on the line card or module by looking through the FIB table for a configurable time period and sending the next <i>n</i> prefixes to the RP or rendezvous point. The RP or rendezvous point performs an exact lookup. If it finds the prefix missing, the RP or rendezvous point reports an inconsistency. Finally, the RP or rendezvous point sends a signal back to the line card or module for confirmation.

**Table 2** CEF Detection Mechanism Types (continued)

Detection Mechanism	Where Operates	Description
scan-rp	Route Processor	Operates on the RP or rendezvous point (opposite of the scan-lc) by looking through the FIB table for a configurable time period and sending the next <i>n</i> prefixes to the line card or module. The line card or module performs an exact lookup. If it finds the prefix missing, the line card or module reports an inconsistency and finally signals the RP or rendezvous point for confirmation.
scan-rib	Route Processor	Operates on all RPs or rendezvous points (even nondistributed) and scans the RIB to ensure that prefix entries are present in the RP or rendezvous point FIB table.

**Examples**

The following example shows how to enable the Cisco Express Forwarding consistency checkers:

```
Router(config)# ip cef table consistency-check
```

**Related Commands,**

Command	Description
<b>clear ip cef inconsistency</b>	Clears Cisco Express Forwarding inconsistency statistics and records found by the Cisco Express Forwarding consistency checkers.
<b>debug ip cef</b>	Displays various Cisco Express Forwarding table query and check events.
<b>show ip cef inconsistency</b>	Displays Cisco Express Forwarding IP prefix inconsistencies.



# ip cef table event-log



## Note

The **ip cef table event-log** command is not available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases.

To control Cisco Express Forwarding table event-log characteristics, use the **ip cef table event-log** command in global configuration mode.

```
ip cef table event-log [size event-number] [match ip-prefix mask]
```

```
no ip cef table event-log [size event-number] [match ip-prefix mask]
```

### Specific to Virtual Private Network (VPN) Event Log

```
ip cef table event-log [size event-number] [vrf vrf-name] [match ip-prefix mask]
```

```
no ip cef table event-log [size event-number] [vrf vrf-name] [match ip-prefix mask]
```

## Syntax Description

<b>size</b> <i>event-number</i>	(Optional) Number of event entries. The range is from 1 to 4294967295. The default is 10000.
<b>match</b>	(Optional) Log events matching specified prefix and mask.
<i>ip-prefix</i>	(Optional) IP prefixes matched, in dotted decimal format (A.B.C.D).
<i>mask</i>	(Optional) Network mask written as A.B.C.D.
<b>vrf</b> <i>vrf-name</i>	(Optional) Virtual Private Network (VPN) routing and forwarding instance (VRF) Cisco Express Forwarding table and VRF name.

## Defaults

Default size for event log is 10000 entries.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(25)S	This command was removed. It is not available in Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
12.2(28)SB	This command was removed. It is not available in Cisco IOS Release 12.2(28)SB and later Cisco IOS 12.2SB releases.
12.2(33)SRA	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRA and later Cisco IOS 12.2SR releases.

Release	Modification
12.2(33)SXH	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXH and later Cisco IOS 12.2SX releases.
12.4(20)T	This command was removed. It is not available in Cisco IOS Release 12.4(20)T and later Cisco IOS 12.4T releases.

### Usage Guidelines

This command is used to troubleshoot inconsistencies that occur in the Cisco Express Forwarding event log between the routes in the Routing Information Base (RIB), Route Processor (RP) Cisco Express Forwarding tables, and line card Cisco Express Forwarding tables.

The Cisco Express Forwarding event log collects Cisco Express Forwarding events as they occur without debugging enabled. This process allows the tracing of an event immediately after it occurs. Cisco technical personnel may ask for information from this event log to aid in resolving problems with the Cisco Express Forwarding feature.

When the Cisco Express Forwarding table event log has reached its capacity, the oldest event is written over by the newest event until the event log size is reset using this command or cleared using the **clear ip cef event-log** command.

### Examples

The following example shows how to set the Cisco Express Forwarding table event log size to 5000 entries:

```
Router(config)# ip cef table event-log size 5000
```

### Related Commands

Command	Description
<b>cef table consistency-check</b>	Enables Cisco Express Forwarding table consistency checker types and parameters.

# ip cef table resolution-timer



## Note

The **ip cef table resolution-timer** command is not available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T and later releases.

To change the Cisco Express Forwarding background resolution timer, use the **ip cef table resolution-timer** command in global configuration mode.

**ip cef table resolution-timer** *seconds*

**no ip cef table resolution-timer** *seconds*

## Syntax Description

<i>seconds</i>	Timer value in seconds. Range is from 0 to 30 seconds; 0 is for the automatic exponential backoff scheme.
----------------	---

## Defaults

The default configuration value is 0 seconds for automatic exponential backoff.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(25)S	This command was removed. It is not available in Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
12.2(28)SB	This command was removed. It is not available in Cisco IOS Release 12.2(28)SB and later Cisco IOS 12.2SB releases.
12.2(33)SRA	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRA and later Cisco IOS 12.2SR releases.
12.2(33)SXH	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXH and later Cisco IOS 12.2SX releases.
12.4(20)T	This command was removed. It is not available in Cisco IOS Release 12.4(20)T and later Cisco IOS 12.4T releases.

## Usage Guidelines

The Cisco Express Forwarding background resolution timer can use either a fixed time interval or an exponential backoff timer that reacts to the amount of resolution work required. The exponential backoff timer starts at 1 second, increasing to 16 seconds when a network flap is in progress. When the network recovers, the timer returns to 1 second.

The default is used for the exponential backoff timer. During normal operation, the default configuration value set to 0 results in re-resolution occurring much sooner than when the timer is set at a higher fixed interval.

**Examples**

The following example show how to set the Cisco Express Forwarding background resolution timer to 3 seconds:

```
Router(config)# ip cef table resolution-timer 3
```

## ip cef traffic-statistics

To change the time interval that controls when Next Hop Resolution Protocol (NHRP) sets up or tears down a switched virtual circuit (SVC), use the **ip cef traffic-statistics** command in global configuration mode. To restore the default values, use the **no** form of this command.

**ip cef traffic-statistics** [**load-interval** *seconds*] [**update-rate** *seconds*]

**no ip cef traffic-statistics**

### Syntax Description

<b>load-interval</b> <i>seconds</i>	(Optional) Length of time (in 30-second increments) during which the average <i>trigger-threshold</i> and <i>teardown-threshold</i> intervals are calculated before an SVC setup or teardown action is taken. (These thresholds are configured in the <b>ip nhrp trigger-svc</b> command.) The <b>load-interval</b> range is from 30 seconds to 300 seconds, in 30-second increments. The default value is 30 seconds.
<b>update-rate</b> <i>seconds</i>	(Optional) Frequency that the port adapter sends the accounting statistics to the Route Processor (RP). When the route processor is using NHRP in distributed Cisco Express Forwarding switching mode, this value must be set to 5 seconds. The default value is 10 seconds.

### Defaults

Load interval: 30 seconds  
Update rate: 10 seconds

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

The **ip nhrp trigger-svc** command sets the threshold by which NHRP sets up and tears down a connection. The threshold is the Cisco Express Forwarding traffic load statistics. The thresholds in the **ip nhrp trigger-svc** command are measured during a sampling interval of 30 seconds, by default. To change that interval over which that threshold is determined, use the **load-interval** *seconds* option of the **ip cef traffic-statistics** command.

When NHRP is configured on a Cisco Express Forwarding switching node with a Versatile Interface Processor (VIP2) adapter, you must make sure the **update-rate** keyword is set to 5 seconds.

Other Cisco IOS features could also use the **ip cef traffic-statistics** command; this NHRP feature relies on it.

---

**Examples**

In the following example, the triggering and teardown thresholds are calculated based on an average over 120 seconds:

```
ip cef traffic-statistics load-interval 120
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip nhrp trigger-svc</b>	Configures when NHRP will set up and tear down an SVC based on aggregate traffic rates.

---

# ip load-sharing

To enable load balancing for Cisco Express Forwarding on an interface, use the **ip load-sharing** command in interface configuration mode. To disable load balancing for Cisco Express Forwarding on the interface, use the **no** form of this command.

**ip load-sharing { per-packet | per-destination }**

**no ip load-sharing per-packet**

## Syntax Description

<b>per-packet</b>	Enables per-packet load balancing for Cisco Express Forwarding on the interface. This functionality and keyword are not supported on all platforms. See “Usage Guidelines” for more information.
<b>per-destination</b>	Enables per-destination load balancing for Cisco Express Forwarding on the interface.

## Command Default

Per-destination load balancing is enabled by default when you enable Cisco Express Forwarding.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
11.2GS	This command was introduced.
11.1CC	This command was modified. Multiple platform support was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

## Usage Guidelines

Per-packet load balancing allows the router to send data packets over successive equal-cost paths without regard to individual destination hosts or user sessions. Path utilization is good, but packets destined for a given destination host might take different paths and might arrive out of order.



### Note

Per-packet load balancing via Cisco Express Forwarding is not supported on Engine 2 Cisco 12000 series Internet router line cards (LCs).

Per-destination load balancing allows the router to use multiple, equal-cost paths to achieve load sharing. Packets for a given source-destination host pair are guaranteed to take the same path, even if multiple, equal-cost paths are available. Traffic for different source-destination host pairs tends to take different paths.

**Note**

If you want to enable per-packet load sharing to a particular destination, then all interfaces that can forward traffic to the destination must be enabled for per-packet load sharing.

**Note**

Per-packet load balancing can result in out-of-sequence (OOS) packet delivery errors on some routers, which can cause applications such as VoIP to malfunction. Therefore, per-packet load balancing is not recommended. For more information, see the release notes and caveats for your platform and software release.

**Cisco ASR 1000 Series Aggregation Services Routers**

The **ip load-sharing** command is not supported on the Cisco ASR 1000 Series Aggregation Services Router. Per-packet load balancing is not supported. On the Cisco ASR 1000 Series Aggregation Services Router, per-destination load balancing is enabled by default and cannot be disabled.

**Examples**

The following example shows how to enable per-packet load balancing:

```
Router(config)# interface E0
Router(config-if)# ip load-sharing per-packet
```

The following example shows how to enable per-destination load balancing:

```
Router(config)# interface E0
Router(config-if)# ip load-sharing per-destination
```

**Related Commands**

Command	Description
<b>ip cef</b>	Enables CEF on the RP card.



# ip route-cache

To control the use of switching methods for forwarding IP packets, use the **ip route-cache** command in interface configuration mode. To disable any of these switching methods, use the **no** form of this command.

**ip route-cache** [**cef** | **distributed** | **flow** | **policy** | **same-interface**]

**no ip route-cache** [**cef** | **distributed** | **flow** | **policy** | **same-interface**]

## Syntax Description

<b>cef</b>	(Optional) Enables Cisco Express Forwarding operation on an interface.
<b>distributed</b>	(Optional) Enables distributed switching on the interface. (This keyword is not supported on the Cisco 7600 routers.) Distributed switching is disabled by default.
<b>flow</b>	(Optional) Enables NetFlow accounting for packets that are received by the interface. The default is disabled.
<b>policy</b>	(Optional) Enables fast-switching for packets that are forwarded using policy-based routing (PBR). Fast Switching for PBR (FSPBR) is disabled by default.
<b>same-interface</b>	(Optional) Enables fast-switching of packets onto the same interface on which they arrived.

## Command Default

The switching method is not controlled.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
10.0	This command was introduced.
11.1	The <b>flow</b> keyword was added.
11.2GS	The <b>cef</b> and <b>distributed</b> keywords were added.
11.1CC	<b>cef</b> keyword support was added for multiple platforms.
12.0	The <b>policy</b> keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The <b>ip route-cache flow</b> command is automatically remapped to the <b>ip flow ingress</b> command.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. This command is not supported on the Cisco 10000 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

---

**Usage Guidelines****IP Route Cache****Note**

---

The Cisco 10000 series routers do *not* support the **ip route-cache** command.

---

Using the route cache is often called *fast switching*. The route cache allows outgoing packets to be load-balanced on a *per-destination* basis rather than on a per-packet basis. The **ip route-cache** command with no additional keywords enables fast switching.

Entering the **ip route-cache** command has no effect on a subinterface. Subinterfaces accept the **no** form of the command; however, this disables Cisco Express Forwarding or distributed Cisco Express Forwarding on the physical interface and all subinterfaces associated with the physical interface

The default behavior for Fast Switching varies by interface and media.

**Note**

---

IPv4 fast switching is removed with the implementation of the Cisco Express Forwarding infrastructure enhancements for Cisco IOS 12.2(25)S-based releases and Cisco IOS Release 12.4(20)T. For these and later Cisco IOS releases, switching path are Cisco Express Forwarding switched or process switched.

---

**IP Route Cache Same Interface**

You can enable IP fast switching when the input and output interfaces are the same interface, using the **ip route-cache same-interface** command. This configuration normally is not recommended, although it is useful when you have partially meshed media, such as Frame Relay or you are running Web Cache Communication Protocol (WCCP) redirection. You could use this feature on other interfaces, although it is not recommended because it would interfere with redirection of packets to the optimal path.

**IP Route Cache Flow**

The flow caching option can be used in conjunction with Cisco Express Forwarding switching to enable NetFlow, which allows statistics to be gathered with a finer granularity. The statistics include IP subprotocols, well-known ports, total flows, average number of packets per flow, and average flow lifetime.

**Note**

---

The **ip route-cache flow** command has the same functionality as the **ip flow ingress** command, which is the preferred command for enabling NetFlow. If either the **ip route-cache flow** command or the **ip flow ingress** command is configured, both commands will appear in the output of the **show running-config** command.

---

**IP Route Cache Distributed**

The distributed option is supported on Cisco routers with line cards and Versatile Interface Processors (VIPs) that support Cisco Express Forwarding switching.

On Cisco routers with Route/Switch Processor (RSP) and VIP controllers, the VIP hardware can be configured to switch packets received by the VIP with no per-packet intervention on the part of the RSP. When VIP distributed switching is enabled, the input VIP interface tries to switch IP packets instead of forwarding them to the RSP for switching. Distributed switching helps decrease the demand on the RSP.

If the **ip route-cache distributed**, **ip cef distributed**, and **ip route-cache flow** commands are configured, the VIP performs distributed Cisco Express Forwarding switching and collects a finer granularity of flow statistics.

### IP Route-Cache Cisco Express Forwarding

In some instances, you might want to disable Cisco Express Forwarding or distributed Cisco Express Forwarding on a particular interface because that interface is configured with a feature that Cisco Express Forwarding or distributed Cisco Express Forwarding does not support. Because all interfaces that support Cisco Express Forwarding or distributed Cisco Express Forwarding are enabled by default when you enable Cisco Express Forwarding or distributed Cisco Express Forwarding operation globally, you must use the **no** form of the **ip route-cache distributed** command in the interface configuration mode to turn Cisco Express Forwarding or distributed Cisco Express Forwarding operation off a particular interface.

Disabling Cisco Express Forwarding or distributed Cisco Express Forwarding on an interface disables Cisco Express Forwarding or distributed Cisco Express Forwarding switching for packets forwarded to the interface, but does not affect packets forwarded out of the interface.

Additionally, when you disable distributed Cisco Express Forwarding on the RSP, Cisco IOS software switches packets using the next-fastest switch path (Cisco Express Forwarding).

Enabling Cisco Express Forwarding globally disables distributed Cisco Express Forwarding on all interfaces. Disabling Cisco Express Forwarding or distributed Cisco Express Forwarding globally enables process switching on all interfaces.



#### Note

On the Cisco 12000 series Internet router, you must not disable distributed Cisco Express Forwarding on an interface.

### IP Route Cache Policy

If Cisco Express Forwarding is already enabled, the **ip route-cache route** command is not required because PBR packets are Cisco Express Forwarding-switched by default.

Before you can enable fast-switched PBR, you must first configure PBR.

FSPBR supports all of PBR's **match** commands and most of PBR's **set** commands, with the following restrictions:

- The **set ip default next-hop** and **set default interface** commands are not supported.
- The **set interface** command is supported only over point-to-point links, unless a route cache entry exists using the same interface specified in the **set interface** command in the route map. Also, at the process level, the routing table is consulted to determine if the interface is on a reasonable path to the destination. During fast switching, the software does not make this check. Instead, if the packet matches, the software blindly forwards the packet to the specified interface.



#### Note

Not all switching methods are available on all platforms. Refer to the *Cisco Product Catalog* for information about features available on the platform you are using.

### Examples

#### Configuring Fast Switching and Disabling Cisco Express Forwarding Switching

The following example shows how to enable fast switching and disable Cisco Express Forwarding switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache
```

The following example shows that fast switching is enabled:

```
Router# show ip interface fastEthernet 0/0/0
```

```

FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.224
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Distributed switching is disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled

```

The following example shows that Cisco Express Forwarding switching is disabled:

```

Router# show cef interface fastEthernet 0/0/0

FastEthernet0/0/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
  Internet address is 10.1.1.254/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is FastEthernet0/0/0
  Fast switching type 1, interface type 18
  IP CEF switching disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 1(1)
  Slot 0 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A02 (0x48001A02)
  IP MTU 1500

```

The following example shows the configuration information for FastEthernet interface 0/0/0:

```

Router# show running-config
.
.
!
interface FastEthernet0/0/0
  ip address 10.1.1.254 255.255.255.0
  no ip route-cache cef
  no ip route-cache distributed
!

```

The following example shows how to enable Cisco Express Forwarding (and to disable distributed Cisco Express Forwarding if it is enabled):

```
Router(config-if)# ip route-cache cef
```

The following example shows how to enable VIP distributed Cisco Express Forwarding and per-flow accounting on an interface (regardless of the previous switching type enabled on the interface):

```
Router(config)# interface e0
Router(config-if)# ip address 10.252.245.2 255.255.255.0
Router(config-if)# ip route-cache distributed
Router(config-if)# ip route-cache flow
```

The following example shows how to enable Cisco Express Forwarding on the router globally (which also disables distributed Cisco Express Forwarding on any interfaces that are running distributed Cisco Express Forwarding), and disable Cisco Express Forwarding (which enables process switching) on Ethernet interface 0:

```
Router(config)# ip cef
Router(config)# interface e0
Router(config-if)# no ip route-cache cef
```

The following example shows how to enable distributed Cisco Express Forwarding operation on the router (globally), and disable Cisco Express Forwarding operation on Ethernet interface 0:

```
Router(config)# ip cef distributed
Router(config)# interface e0
Router(config-if)# no ip route-cache cef
```

The following example shows how to reenabling distributed Cisco Express Forwarding operation on Ethernet interface 0:

```
Router(config)# ip cef distributed
Router(config)# interface e0
Router(config-if)# ip route-cache distributed
```

### Configuring Fast Switching for Traffic That Is Received and Transmitted over the Same Interface

The following example shows how to enable fast switching and disable Cisco Express Forwarding switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache same-interface
```

The following example shows that fast switching on the same interface is enabled for interface fastethernet 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
 Internet address is 10.1.1.254/24
 Broadcast address is 255.255.255.224
 Address determined by non-volatile memory
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.10
 Outgoing access list is not set
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
```

```

ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is enabled
IP Flow switching is disabled
IP Distributed switching is disabled
IP Feature Fast switching turbo vector
IP Null turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
IP multicast multilayer switching is disabled

```

The following example shows the configuration information for FastEthernet interface 0/0/0:

```

Router# show running-config
.
.
!
interface FastEthernet0/0/0
 ip address 10.1.1.254 255.255.255.0
 ip route-cache same-interface
 no ip route-cache cef
 no ip route-cache distributed
!

```

### Enabling NetFlow Accounting

The following example shows how to enable NetFlow switching:

```

Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache flow

```

The following example shows that NetFlow accounting is enabled for FastEthernet interface 0/0/0:

```

Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
 Internet address is 10.1.1.254/24
 Broadcast address is 255.255.255.224
 Address determined by non-volatile memory
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.10
 Outgoing access list is not set
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is enabled

```

```

IP fast switching on the same interface is disabled
IP Flow switching is enabled
IP Distributed switching is disabled
IP Flow switching turbo vector
IP Null turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, Flow
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
IP multicast multilayer switching is disabled

```

### Configuring Distributed Switching

The following example shows how to enable distributed switching:

```

Router(config)# ip cef distributed
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache distributed

```

The following example shows that distributed Cisco Express Forwarding switching is for FastEthernet interface 0/0/0:

```

Router# show cef interface fastEthernet 0/0/0

FastEthernet0/0/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
  Internet address is 10.1.1.254/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is FastEthernet0/0/0
  Fast switching type 1, interface type 18
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 1(1)
  Slot 0 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A02 (0x48001A02)
  IP MTU 1500

```

### Configuring Fast Switching for PBR

The following example shows how to configure a simple policy-based routing scheme and to enable FSPBR:

```

Router(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)# route-map mypbrtag permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set ip next-hop 10.1.1.195

```

```
Router(config-route-map)# exit
Router(config)# interface fastEthernet 0/0/0
Router(config-if)# ip route-cache policy
Router(config-if)# ip policy route-map mypbrtag
```

The following example shows that FSPBR is enabled for FastEthernet interface 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Distributed switching is enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, Distributed, Policy, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is enabled, using route map my_pbr_tag
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  IP multicast multilayer switching is disabled
```



**Related Commands**

<b>Command</b>	<b>Description</b>
<b>exit</b>	Leaves aggregation cache mode.
<b>ip cef</b>	Enables Cisco Express Forwarding on the RP card.
<b>ip cef distributed</b>	Enables distributed Cisco Express Forwarding operation.
<b>ip flow ingress</b>	Configures NetFlow on a subinterface.
<b>set default interface</b>	Configures a default interface for PBR.
<b>set interface</b>	Configures a specified interface for PBR.
<b>set ip default next-hop</b>	Configures a default IP next hop for PBR.
<b>show cef interface</b>	Displays detailed Cisco Express Forwarding information for interfaces.
<b>show ip interface</b>	Displays the usability status of interfaces configured for IP.
<b>show mpoa client</b>	Displays the routing table cache used to fast switch IP traffic.

## ip route-cache policy

The **policy** keyword for the **ip route-cache** command is no longer documented as a separate command.

The information for using the **policy** keyword for the **ip route-cache** command has been incorporated into the **ip route-cache** command documentation. See the **ip route-cache** command documentation for more information.

# ip verify unicast notification threshold

To configure the threshold value used to determine whether to send a Unicast Reverse Path Forwarding (RPF) drop rate notification, use the **ip verify unicast notification threshold** command in interface configuration mode. To set the notification threshold back to the default value, use the **no** form of this command.

**ip verify unicast notification threshold** *packets-per-second*

**no ip verify unicast notification threshold**

## Syntax Description

*packets-per-second* Threshold value, in packets per second, used to determine whether to send a Unicast RPF drop rate notification. The range is from 0 to 4294967295. The default is 1000.

## Command Default

No notifications are sent.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SX12	This command was integrated into Cisco IOS Release 12.2(33)SX12.

## Usage Guidelines

This command configures the threshold Unicast RPF drop rate which, when exceeded, triggers a notification. Configuring a value of 0 means that any Unicast RPF packet drop triggers a notification.

## Examples

The following example shows how to configure a notification threshold value of 900 on Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 3/0
Router(config-if)# ip verify unicast notification threshold 900
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip verify drop-rate compute interval</b>	Configures the interval of time between Unicast RPF drop rate computations.
<b>ip verify drop-rate compute window</b>	Configures the interval of time during which the Unicast RPF drop count is collected for the drop rate computation.
<b>ip verify drop-rate notify hold-down</b>	Configures the minimum time between Unicast RPF drop rate notifications.

# ip verify unicast reverse-path



## Note

This command was replaced by the **ip verify unicast source reachable-via** command effective with Cisco IOS Release 12.0(15)S. The **ip verify unicast source reachable-via** command allows for more flexibility and functionality, such as supporting asymmetric routing, and should be used for any Reverse Path Forward implementation. The **ip verify unicast reverse-path** command is still supported.

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast reverse-path** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

**ip verify unicast reverse-path** [*list*]

**no ip verify unicast reverse-path** [*list*]

## Syntax Description

<i>list</i>	(Optional) Specifies a numbered access control list (ACL) in the following ranges: <ul style="list-style-type: none"> <li>• 1 to 99 (IP standard access list)</li> <li>• 100 to 199 (IP extended access list)</li> <li>• 1300 to 1999 (IP standard access list, expanded range)</li> <li>• 2000 to 2699 (IP extended access list, expanded range)</li> </ul>
-------------	--

## Command Default

Unicast RPF is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
11.1(CC) 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3
12.1(2)T	Added ACL support using the <i>list</i> argument. Added per-interface statistics on dropped or suppressed packets.
12.0(15)S	The <b>ip verify unicast source reachable-via</b> command replaced this command, and the following keywords were added to the <b>ip verify unicast source reachable-via</b> command: <b>allow-default</b> , <b>allow-self-ping</b> , <b>rx</b> , and <b>any</b> .
12.1(8a)E	The <b>ip verify unicast reverse-path</b> command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	The <b>ip verify unicast reverse-path</b> command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(14)SX	The <b>ip verify unicast reverse-path</b> command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(33)SRA	The <b>ip verify unicast reverse-path</b> command was integrated into Cisco IOS Release 12.2(33)SRA.

### Usage Guidelines

Use the **ip verify unicast reverse-path interface** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that are received by a router. Malformed or forged source addresses can indicate denial of service (DoS) attacks on the basis of source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to ensure that the source address appears in the Forwarding Information Base (FIB) and that it matches the interface on which the packet was received. This “look backwards” ability is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.

To use Unicast RPF, enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching in the router. There is no need to configure the input interface for Cisco Express Forwarding switching. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.



#### Note

It is very important for Cisco Express Forwarding to be configured globally in the router. Unicast RPF will not work without Cisco Express Forwarding.



#### Note

Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

The Unicast Reverse Path Forwarding feature checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this by doing a reverse lookup in the Cisco Express Forwarding table. If Unicast RPF does not find a reverse path for the packet, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast Reverse Path Forwarding command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast Reverse Path Forwarding command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast Reverse Path Forwarding command. Log information can be used to gather information about the attack, such as source address, time, and so on.

### Where to Use RPF in Your Network

Unicast RPF may be used on interfaces in which only one path allows packets from valid source networks (networks contained in the FIB). Unicast RPF may also be used in cases for which a router has multiple paths to a given network, as long as the valid networks are switched via the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an

Internet service provider (ISP) are likely to have symmetrical reverse paths. Unicast RPF may still be applicable in certain multi-homed situations, provided that optional Border Gateway Protocol (BGP) attributes such as weight and local preference are used to achieve symmetric routing.

With Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

For example, routers at the edge of the network of an ISP are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. In this scenario, you should use the new form of the command, **ip verify unicast source reachable-via**, if there is a chance of asymmetrical routing.

## Examples

The following example shows that the Unicast Reverse Path Forwarding feature has been enabled on a serial interface:

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
 ip verify unicast reverse-path
```

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 192.168.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 192.168.200.225 255.255.255.255
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 192.168.202.128 10.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 10.0.0.0 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 10.0.0.0 255.255.255.255 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 192.168.0.0 255.255.255.255 any log
access-list 111 deny ip 209.165.202.129 10.0.0.31 any log
access-list 111 permit ip any any
```

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on Ethernet interface 0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at Ethernet interface 0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at Ethernet interface 0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.255
 ip verify unicast reverse-path 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.255
!
access-list 197 deny ip 192.168.201.0 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 10.0.0.63 any log-input
access-list 197 deny ip 192.168.201.128 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 10.0.0.63 any log-input
access-list 197 deny ip host 10.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 255.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 192.168.0.0 255.255.255.255 any log-input
```

#### Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.




# ip verify unicast source reachable-via

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast source reachable-via** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

```
ip verify unicast source reachable-via {any | rx [I2-src]} [allow-default] [allow-self-ping]
    [access-list]
```

```
no ip verify unicast source reachable-via
```

Syntax Description		
<b>any</b>	Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet if the source is reachable through any interface (sometimes referred to as loose mode).	
<b>rx</b>	Examines incoming packets to determine whether the source address is in the FIB and permits the packet only if the source is reachable through the interface on which the packet was received (sometimes referred to as strict mode).	
<b>I2-src</b>	(Optional) Enables source IPv4 and source MAC address binding.	
<b>allow-default</b>	(Optional) Allows the use of the default route for RPF verification.	
<b>allow-self-ping</b>	(Optional) Allows a router to ping its own interface or interfaces.	
		
	<b>Caution</b>	Use caution when enabling the <b>allow-self-ping</b> keyword. This keyword opens a denial-of-service (DoS) hole.
<i>access-list</i>	(Optional) Specifies a numbered access control list (ACL) in the following ranges:	<ul style="list-style-type: none"> <li>• 1 to 99 (IP standard access list)</li> <li>• 100 to 199 (IP extended access list)</li> <li>• 1300 to 1999 (IP standard access list, expanded range)</li> <li>• 2000 to 2699 (IP extended access list, expanded range)</li> </ul>

Command Default	
	Unicast RPF is disabled. Source IPv4 and source MAC address binding is disabled.

Command Modes	
	Interface configuration (config-if)

Command History	Release	Modification
	11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3.
	12.1(2)T	Added access control list (ACL) support using the <i>access-list</i> argument. Added per-interface statistics on dropped or suppressed packets.

Release	Modification
12.0(15)S	This command replaced the <b>ip verify unicast reverse-path</b> command, and the following keywords were added: <b>allow-default</b> , <b>allow-self-ping</b> , <b>rx</b> , and <b>any</b> .
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified. The <b>I2-src</b> keyword was added to support the source IPv4 and source MAC address binding feature on platforms that support the Cisco Express Forwarding software switching path.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

### Usage Guidelines

Use the **ip verify unicast source reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate DoS attacks based on source IP address spoofing.

To use Unicast RPF, enable Cisco Express Forwarding or distributed Cisco Express Forwarding in the router. There is no need to configure the input interface for Cisco Express Forwarding. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.



#### Note

It is important for Cisco Express Forwarding to be configured globally on the router. Unicast RPF does not work without Cisco Express Forwarding.



#### Note

Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to make sure that the source address appears in the FIB. If the **rx** keyword is selected, the source address must match the interface on which the packet was received. If the **any** keyword is selected, the source address must be present only in the FIB. This ability to “look backwards” is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.



#### Note

If the source address of an incoming packet is resolved to a null adjacency, the packet will be dropped. The null interface is treated as an invalid interface by the new form of the Unicast RPF command. The older form of the command syntax did not exhibit this behavior.

Unicast RPF checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement

in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ip verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately, and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries that are used by the **ip verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

### Strict Mode RPF

If the source address is in the FIB and reachable only through the interface on which the packet was received, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via rx**.

### Exists-Only (or Loose Mode) RPF

If the source address is in the FIB and reachable through any interface on the router, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via any**.

Because this Unicast RPF option passes packets regardless of which interface the packet enters, it is often used on Internet service provider (ISP) routers that are “peered” with other ISP routers (where asymmetrical routing typically occurs). Packets using source addresses that have not been allocated on the Internet, which are often used for spoofed source addresses, are dropped by this Unicast RPF option. All other packets that have an entry in the FIB are passed.

### allow-default

Normally, sources found in the FIB but only by way of the default route will be dropped. Specifying the **allow-default** keyword option will override this behavior. You must specify the **allow-default** keyword in the command to permit Unicast RPF to successfully match on prefixes that are known through the default route to pass these packets.

### allow-self-ping

This keyword allows the router to ping its own interface or interfaces. By default, when Unicast RPF is enabled, packets that are generated by the router and destined to the router are dropped, thereby, making certain troubleshooting and management tasks difficult to accomplish. Issue the **allow-self-ping** keyword to enable self-pinging.



### Caution

Caution should be used when enabling the **allow-self-ping** keyword because this option opens a potential DoS hole.

### Using RPF in Your Network

Use Unicast RPF strict mode on interfaces where only one path allows packets from valid source networks (networks contained in the FIB). Also, use Unicast RPF strict mode when a router has multiple paths to a given network, as long as the valid networks are switched through the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an ISP are likely to have symmetrical reverse paths. Unicast RPF strict mode is applicable in certain multihomed situations, provided that optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, are used to achieve symmetric routing.

**Note**

With Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

Use Unicast RPF loose mode on interfaces where asymmetric paths allow packets from valid source networks (networks contained in the FIB). Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.

**IP and MAC Address Spoof Prevention**

In Release 15.0(1)M and later, you can use the **l2-src** keyword to enable source IPv4 and source MAC address binding. To disable source IPv4 and source MAC address binding, use the **no** form of the **ip verify unicast source reachable-via** command.

If an inbound packet fails this security check, it will be dropped and the Unicast RPF dropped-packet counter will be incremented. The only exception occurs if a numbered access control list has been specified as part of the Unicast RPF command in strict mode, and the ACL permits the packet. In this case the packet will be forwarded and the Unicast RPF suppressed-drops counter will be incremented.

**Note**

The **l2-src** keyword cannot be used with the loose uRPF command, **ip verify unicast source reachable-via any** command.

Not all platforms support the **l2-src** keyword. Therefore, not all the possible keyword combinations for strict Unicast RPF in the following list will apply to your platform:

Possible keyword combinations for strict Unicast RPF include the following:

```
allow-default
allow-self-ping
l2-src
<ACL-number>
allow-default allow-self-ping
allow-default l2-src
allow-default <ACL-number>
allow-self-ping l2-src
allow-self-ping <ACL-number>
l2-src <ACL-number>
allow-default allow-self-ping l2-src
allow-default allow-self-ping <ACL-number>
allow-default l2-src <ACL-number>
allow-self-ping l2-src <ACL-number>
allow-default allow-self-ping l2-src <ACL-number>
```

**Examples****Single-Homed ISP Connection with Unicast RPF**

The following example uses a very simple single-homed ISP connection to demonstrate the concept of Unicast RPF. In this example, an ISP peering router is connected through a single serial interface to one upstream ISP. Hence, traffic flows into and out of the ISP will be symmetric. Because traffic flows will be symmetric, a Unicast RPF strict-mode deployment can be configured.

```
ip cef
! or "ip cef distributed" for Route Switch Processor+Versatile Interface Processor-
```

```
(RSP+VIP-) based routers.
!
interface Serial5/0/0
  description - link to upstream ISP (single-homed)
  ip address 192.168.200.225 255.255.255.252
  no ip redirects
  no ip directed-broadcasts
  no ip proxy-arp
  ip verify unicast source reachable-via
```

### ACLs and Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/1/1 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0/1/1 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet 0/1/2 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
  ip address 192.168.200.1 255.255.255.0
  ip verify unicast source reachable-via rx 197
!
int eth0/1/2
  ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input
```

### MAC Address Binding on Software Switching Platforms Like the Cisco 7200 Series Routers

The following example shows how to enable source IPv4 and source MAC address binding on Ethernet 0/0:

```
Router# configure terminal
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip verify unicast source reachable-via rx 12-src
```

#### Related Commands

Command	Description
<b>ip cef</b>	Enables Cisco Express Forwarding on the route processor card.
<b>ip cef distributed</b>	Enables Cisco Express Forwarding on the line card.

## ip verify unicast vrf

To enable Unicast Reverse Path Forwarding (Unicast RPF) verification for a specified VRF, use the **ip verify unicast vrf** command in interface configuration mode. To disable the Unicast RPF check for a VRF, use the **no** form of this command.

```
ip verify unicast vrf vrf-name {deny | permit}
```

```
no ip verify unicast vrf vrf-name {deny | permit}
```

### Syntax Description

<i>vrf-name</i>	Virtual Private Network (VPN) routing and forwarding (VRF) instance name.
<b>deny</b>	Specifies that traffic associated with the specified VRF is dropped after it passes the Unicast RPF verification.
<b>permit</b>	Specifies that traffic associated with the specified VRF is forwarded after it passes the Unicast RPF verification.

### Command Default

Unicast RPF verification is disabled.

### Command Modes

Interface configuration (config-if)

### Command History

Release	Modification
12.0(29)S	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 integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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.

### Usage Guidelines

Unicast RPF is configured to verify that the source address is in the Forwarding Information Base (FIB). The **ip verify unicast vrf** command is configured in interface configuration mode and is enabled for each VRF. This command has **permit** and **deny** keywords that are used to determine if traffic is forwarded or dropped after Unicast RPF verification.

### Examples

The following example configures Unicast RPF verification for VRF1 and VRF2. VRF1 traffic is forwarded. VRF2 traffic is dropped.

```
Router(config)# interface Ethernet 0
Router(config-if)# ip verify unicast vrf vrf1 permit
Router(config-if)# ip verify unicast vrf vrf2 deny
Router(config-if)# end
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>import ipv4</b>	Configures an import map to import IPv4 prefixes from the global routing table to a VRF table.
<b>ip vrf</b>	Configures a VRF routing table.
<b>rd</b>	Creates routing and forwarding tables for a VRF.
<b>show ip bgp</b>	Displays entries in the BGP routing table.
<b>show ip bgp vpnv4</b>	Displays VPN address information from the BGP table.
<b>show ip vrf</b>	Displays the set of defined VRFs and associated interfaces.

# ipv6 cef

To enable Cisco Express Forwarding for IPv6, use the **ipv6 cef** command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the **no** form of this command.

**ipv6 cef**

**no ipv6 cef**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Cisco Express Forwarding for IPv6 is disabled by default.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The **ipv6 cef** command is similar to the **ip cef** command, except that it is IPv6-specific.

The **ipv6 cef** command is not available on the Cisco 12000 series Internet routers because this distributed platform operates only in distributed Cisco Express Forwarding for IPv6 mode.



### Note

The **ipv6 cef** command is not supported in interface configuration mode.



### Note

Some distributed architecture platforms, such as the Cisco 7500 series routers, support both Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6. When Cisco Express Forwarding for IPv6 is configured on distributed platforms, Cisco Express Forwarding switching is performed by the Route Processor (RP).





**Note**

You must enable Cisco Express Forwarding for IPv4 by using the **ip cef** global configuration command before enabling Cisco Express Forwarding for IPv6 by using the **ipv6 cef** global configuration command.

Cisco Express Forwarding for IPv6 is advanced Layer 3 IP switching technology that functions the same and offer the same benefits as Cisco Express Forwarding for IPv4. Cisco Express Forwarding for IPv6 optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

**Examples**

The following example enables standard Cisco Express Forwarding for IPv4 operation and then standard Cisco Express Forwarding for IPv6 operation globally on the router.

```
ip cef
ipv6 cef
```

**Related Commands**

Command	Description
<b>ip route-cache</b>	Controls the use of high-speed switching caches for IP routing.
<b>ipv6 cef accounting</b>	Enables Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting.
<b>ipv6 cef distributed</b>	Enables distributed Cisco Express Forwarding for IPv6.
<b>show cef</b>	Displays which packets the line cards dropped or displays which packets were not express-forwarded.
<b>show ipv6 cef</b>	Displays entries in the IPv6 FIB.

# ipv6 cef accounting

To enable Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting, use the **ipv6 cef accounting** command in global configuration mode or interface configuration mode. To disable Cisco Express Forwarding for IPv6 network accounting, use the **no** form of this command.

**ipv6 cef accounting** *accounting-types*

**no ipv6 cef accounting** *accounting-types*

## Specific Cisco Express Forwarding Accounting Information Through Interface Configuration Mode

**ipv6 cef accounting non-recursive** { **external** | **internal** }

**no ipv6 cef accounting non-recursive** { **external** | **internal** }

### Syntax Description

<i>accounting-types</i>	The <i>accounting-types</i> argument must be replaced with at least one of the following keywords. Optionally, you can follow this keyword by any or all of the other keywords, but you can use each keyword only once. <ul style="list-style-type: none"> <li>• <b>load-balance-hash</b>—Enables load balancing hash bucket counters.</li> <li>• <b>non-recursive</b>—Enables accounting through nonrecursive prefixes.</li> <li>• <b>per-prefix</b>—Enables express forwarding of the collection of the number of packets and bytes to a destination (or prefix).</li> <li>• <b>prefix-length</b>—Enables accounting through prefix length.</li> </ul>
<b>non-recursive</b>	Enables accounting through nonrecursive prefixes.  This keyword is optional when used in global configuration mode after another keyword is entered. See the <i>accounting-types</i> argument.
<b>external</b>	Counts input traffic in the nonrecursive external bin.
<b>internal</b>	Counts input traffic in the nonrecursive internal bin.

### Command Default

Cisco Express Forwarding for IPv6 network accounting is disabled by default.

### Command Modes

Global configuration (config)  
Interface configuration (config-if)

### Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(25)S	The <b>non-recursive</b> and <b>load-balance-hash</b> keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

### Usage Guidelines

The **ipv6 cef accounting** command is similar to the **ip cef accounting** command, except that it is IPv6-specific.

Configuring Cisco Express Forwarding for IPv6 network accounting enables you to collect statistics on Cisco Express Forwarding for IPv6 traffic patterns in your network.

When you enable network accounting for Cisco Express Forwarding for IPv6 by using the **ipv6 cef accounting** command in global configuration mode, accounting information is collected at the Route Processor (RP) when Cisco Express Forwarding for IPv6 mode is enabled and at the line cards when distributed Cisco Express Forwarding for IPv6 mode is enabled. You can then display the collected accounting information using the **show ipv6 cef EXEC** command.

For prefixes with directly connected next hops, the **non-recursive** keyword enables express forwarding of the collection of packets and bytes through a prefix. This keyword is optional when this command is used in global configuration mode after you enter another keyword on the **ipv6 cef accounting** command.

This command in interface configuration mode must be used in conjunction with the global configuration command. The interface configuration command allows a user to specify two different bins (internal or external) for the accumulation of statistics. The internal bin is used by default. The statistics are displayed through the **show ipv6 cef detail** command.

Per-destination load balancing uses a series of 16 hash buckets into which the set of available paths are distributed. A hash function operating on certain properties of the packet is applied to select a bucket that contains a path to use. The source and destination IP addresses are the properties used to select the bucket for per-destination load balancing. Use the **load-balance-hash** keyword with the **ipv6 cef accounting** command to enable per-hash-bucket counters. Enter the **show ipv6 cef prefix internal** command to display the per-hash-bucket counters.

### Examples

The following example enables the collection of Cisco Express Forwarding for IPv6 accounting information for prefixes with directly connected next hops:

```
Router(config)# ipv6 cef accounting non-recursive
```

### Related Commands

Command	Description
<b>ip cef accounting</b>	Enable Cisco Express Forwarding network accounting (for IPv4).
<b>show cef</b>	Displays information about packets forwarded by Cisco Express Forwarding.
<b>show ipv6 cef</b>	Displays entries in the IPv6 FIB.

# ipv6 cef distributed

To enable distributed Cisco Express Forwarding for IPv6, use the **ipv6 cef distributed** command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the **no** form of this command.

**ipv6 cef distributed**

**no ipv6 cef distributed**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Distributed Cisco Express Forwarding for IPv6 is disabled on the Cisco 7500 series routers and enabled on the Cisco 12000 series Internet routers.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.0(22)S	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
	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.
	Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** The **ipv6 cef distributed** command is similar to the **ip cef distributed** command, except that it is IPv6-specific.

Enabling distributed Cisco Express Forwarding for IPv6 globally on the router by using the **ipv6 cef distributed** in global configuration mode distributes the Cisco Express Forwarding processing of IPv6 packets from the Route Processor (RP) to the line cards of distributed architecture platforms.



**Note**

The **ipv6 cef distributed** command is not supported on the Cisco 12000 series Internet routers because distributed Cisco Express Forwarding for IPv6 is enabled by default on this platform.



**Note**

To forward distributed Cisco Express Forwarding for IPv6 traffic on the router, configure the forwarding of IPv6 unicast datagrams globally on your router by using the **ipv6 unicast-routing** global configuration command, and configure an IPv6 address and IPv6 processing on an interface by using the **ipv6 address** interface configuration command.



**Note**

You must enable distributed Cisco Express Forwarding for IPv4 by using the **ip cef distributed** global configuration command before enabling distributed Cisco Express Forwarding for IPv6 by using the **ipv6 cef distributed** global configuration command.

Cisco Express Forwarding is advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

**Examples**

The following example enables distributed Cisco Express Forwarding for IPv6 operation:

```
ipv6 cef distributed
```

**Related Commands**

Command	Description
<b>ip route-cache</b>	Controls the use of high-speed switching caches for IP routing.
<b>show ipv6 cef</b>	Displays entries in the IPv6 FIB.

# ipv6 cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm for IPv6, use the **ipv6 cef load-sharing algorithm** command in global configuration mode. To return to the default universal load-balancing algorithm, use the **no** form of this command.

```
ipv6 cef load-sharing algorithm { original | universal [id] | include-ports { source [id] |
destination [id] | source [id] destination [id]} }
```

```
no ipv6 cef load-sharing algorithm
```

Syntax Description		
<b>original</b>		Sets the load-balancing algorithm to the original algorithm based on a source and destination hash.
<b>universal</b>		Sets the load-balancing algorithm to the universal algorithm that uses a source and destination and an ID hash.
<i>id</i>		(Optional) Fixed identifier in hexadecimal format.
<b>include-ports source</b>		Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 source port.
<b>include-ports destination</b>		Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 destination port.
<b>include-ports source destination</b>		Sets the load balancing algorithm to the include-ports algorithm that uses Layer 4 source and destination ports.

**Command Default** The universal load-balancing algorithm is selected. If you do not configure the fixed identifier for a load-balancing algorithm, the router automatically generates a unique ID.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.2(25)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
	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	This command was integrated into Cisco IOS Release 12.4(20)T.

**Usage Guidelines**

The **ipv6 cef load-sharing algorithm** command is similar to the **ip cef load-sharing algorithm** command, except that it is IPv6-specific.

When the Cisco Express Forwarding for IPv6 load-balancing algorithm is set to universal mode, each router on the network can make a different load-sharing decision for each source-destination address pair.

The include-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal-cost paths that are not load-shared because the majority of the traffic is between peer addresses that use different port numbers, such as Real-Time Protocol (RTP) streams.

**Examples**

The following example shows how to enable the Cisco Express Forwarding load-balancing algorithm for IPv6 for Layer-4 source and destination ports:

```
Router(config)# ipv6 cef load-sharing algorithm include-ports source destination
```

The router automatically generates fixed IDs for the algorithm.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug ipv6 cef hash</b>	Displays debug messages for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 load-sharing hash algorithm events.
<b>ip cef load-sharing algorithm</b>	Selects a Cisco Express Forwarding load-balancing algorithm (for IPv4).

# ipv6 cef optimize neighbor resolution

To configure address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the **ipv6 cef optimize neighbor resolution** command in global configuration mode. To disable address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the **no** form of this command.

**ipv6 cef optimize neighbor resolution**

**no ipv6 cef optimize neighbor resolution**

**Syntax Description** This command has no arguments or keywords.

**Command Default** If this command is not configured, Cisco Express Forwarding for IPv6 does not optimize the address resolution of directly connected neighbors.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.2(25)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	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.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

**Usage Guidelines** The **ipv6 cef optimize neighbor resolution** command is very similar to the **ip cef optimize neighbor resolution** command, except that it is IPv6-specific.

Use this command to trigger Layer 2 address resolution of neighbors directly from Cisco Express Forwarding for IPv6.

**Examples** The following example shows how to optimize address resolution from Cisco Express Forwarding for IPv6 for directly connected neighbors:

```
Router(config)# ipv6 cef optimize neighbor resolution
```

Related Commands	Command	Description
	<b>ip cef optimize neighbor resolution</b>	Configures address resolution optimization from Cisco Express Forwarding for IPv4 for directly connected neighbors.



# ipv6 verify unicast reverse-path

To enable Unicast Reverse Path Forwarding (Unicast RPF) for IPv6, use the **ipv6 verify unicast reverse-path** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

**ipv6 verify unicast reverse-path** [*access-list name*]

**no ipv6 verify unicast reverse-path** [*access-list name*]

## Syntax Description

<b>access-list name</b>	(Optional) Specifies the name of the access list.
<b>Note</b>	This keyword and argument are not supported on the Cisco 12000 series Internet router.

## Command Default

Unicast RPF is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S and introduced on the 10G Engine 5 SPA Interface Processor in the Cisco 12000 series Internet router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## Usage Guidelines

The **ipv6 verify unicast reverse-path** command is used to enable Unicast RPF for IPv6 in strict checking mode. The Unicast RPF for IPv6 feature requires that Cisco Express Forwarding for IPv6 is enabled on the router.



### Note

Beginning in Cisco IOS Release 12.0(31)S, the Cisco 12000 series Internet router supports both the **ipv6 verify unicast reverse-path** and **ipv6 verify unicast source reachable-via rx** commands to enable Unicast RPF to be compatible with the Cisco IOS Release 12.3T and 12.2S software trains.

Use the **ipv6 verify unicast reverse-path** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source IPv6 address appears in the routing table and that it is reachable by a path through the interface on which the packet was received. Unicast RPF is an input feature and is applied only on the input interface of a router at the upstream end of a connection.

The Unicast RPF feature performs a reverse lookup in the CEF table to check if any packet received at a router interface has arrived on a path identified as a best return path to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast RPF command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast RPF command. Log information can be used to gather information about the attack, such as source address, time, and so on.

**Note**

When you configure Unicast RPF for IPv6 on the Cisco 12000 series Internet router, the most recently configured checking mode is not automatically applied to all interfaces as on other platforms. You must enable Unicast RPF for IPv6 separately on each interface.

When you configure a SPA on the Cisco 12000 series Internet router, the interface address is in the format *slot/subslot/port*.

The optional **access-list** keyword for the **ipv6 verify unicast reverse-path** command is not supported on the Cisco 12000 series Internet router. For information about how Unicast RPF can be used with ACLs on other platforms to mitigate the transmission of invalid IPv4 addresses (perform egress filtering) and to prevent (deny) the reception of invalid IPv4 addresses (perform ingress filtering), refer to the “Configuring Unicast Reverse Path Forwarding” chapter in the “Other Security Features” section of the *Cisco IOS Security Configuration Guide*.

**Note**

When using Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on).

Do not use Unicast RPF on core-facing interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, meaning that there are multiple routes to the source of a packet. Apply Unicast RPF only where there is natural or configured symmetry.

For example, routers at the edge of the network of an Internet service provider (ISP) are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing. It is simplest to place Unicast RPF only at the edge of a network or, for an ISP, at the customer edge of the network.

**Examples****Unicast Reverse Path Forwarding on a Serial Interface**

The following example shows how to enable the Unicast RPF feature on a serial interface:

```
interface serial 5/0/0
  ipv6 verify unicast reverse-path
```

### Unicast Reverse Path Forwarding on a Cisco 12000 Series Internet Router

The following example shows how to enable Unicast RPF for IPv6 with strict checking on a 10G SIP Gigabit Ethernet interface 2/1/2:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# interface gigabitEthernet 2/1/2

Router(config-if)# ipv6 verify unicast reverse-path
Router(config-if)# exit
```

### Unicast Reverse Path Forwarding on a Single-Homed ISP

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 209.165.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
interface Serial 5/0/0
description Connection to Upstream ISP
ipv6 address FE80::260:3EFF:FE11:6770/64
no ipv6 redirects
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
permit ipv6 host 2::1 any
deny ipv6 FEC0::/10 any
    ipv6 access-group abc in
    ipv6 access-group jkl out
!
access-list abc permit ip FE80::260:3EFF:FE11:6770/64 2001:0DB8:0000:0001::0001any
access-list abc deny ipv6 any any log
access-list jkl deny ipv6 host 2001:0DB8:0000:0001::0001 any log
access-list jkl deny ipv6 2001:0DB8:0000:0001:FFFF:1234::5.255.255.255 any log
access-list jkl deny ipv6 2002:0EF8:002001:0DB8:0000:0001:FFFF:1234::5172.16.0.0
0.15.255.255 any log
access-list jkl deny ipv6 2001:0CB8:0000:0001:FFFF:1234::5 0.0.255.255 any log
access-list jkl deny ipv6 2003:0DB8:0000:0001:FFFF:1234::5 0.0.0.31 any log
access-list jkl permit ipv6
```

### ACL Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL abc provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/0 to check packets arriving at that interface.

For example, packets with a source address of 8765:4321::1 arriving at Ethernet interface 0 are dropped because of the deny statement in ACL “abc.” In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 1234:5678::1 arriving at Ethernet interface 0/0 are forwarded because of the permit statement in ACL abc. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
interface ethernet 0/0
ipv6 address FE80::260:3EFF:FE11:6770/64 link-local
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
```

```
permit ipv6 1234:5678::/64 any log-input  
deny ipv6 8765:4321::/64 any log-input
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip cef</b>	Enables Cisco Express Forwarding on the route processor card.
<b>ip verify unicast reverse-path</b>	Enables Unicast RPF for IPv4 traffic.
<b>ipv6 cef</b>	Enables Cisco Express Forwarding for IPv6 interfaces.

# ipv6 verify unicast source reachable-via

To verify that a source address exists in the FIB table and enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ipv6 verify unicast source reachable-via** command in interface configuration mode. To disable URPF, use the **no** form of this command.

```
ipv6 verify unicast source reachable-via {rx | any} [allow-default] [allow-self-ping]
    [access-list-name]
```

```
no ipv6 verify unicast
```

## Syntax Description

<b>rx</b>	Source is reachable through the interface on which the packet was received.
<b>any</b>	Source is reachable through any interface.
<b>allow-default</b>	(Optional) Allows the lookup table to match the default route and use the route for verification.
<b>allow-self-ping</b>	(Optional) Allows the router to ping a secondary address.
<i>access-list-name</i>	(Optional) Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeral.

## Command Default

Unicast RPF is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

## Usage Guidelines

The **ipv6 verify unicast reverse-path** command is used to enable Unicast RPF for IPv6 in loose checking mode.

Use the **ipv6 verify unicast source reachable-via** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through an IPv6 router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IPv6 address spoofing.

The URPF feature checks to see if any packet received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this by doing a reverse lookup in the CEF table. If URPF does not find a reverse path for the packet, U RPF can drop or forward the packet, depending on whether an access control list (ACL) is specified in the **ipv6 verify unicast source reachable-via** command. If an ACL is specified in the command, then when (and only when) a packet fails the URPF check, the ACL is checked to see if the packet should be dropped (using a deny statement in the ACL)

or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for U RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ipv6 verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

U RPF events can be logged by specifying the logging option for the ACL entries used by the **ipv6 verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

**Examples**

The following example enables Unicast RPF on any interface:

```
ipv6 verify unicast source reachable-via any
```

**Related Commands**

Command	Description
<b>ipv6 access-list</b>	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
<b>show ipv6 interface</b>	Displays the usability status of interfaces configured for IPv6.

## mls cef maximum-routes

To limit the maximum number of the routes that can be programmed in the hardware allowed per protocol, use the **mls cef maximum-routes** command in global configuration mode. To return to the default settings, use the **no** form of this command.

```
mls cef maximum-routes {ip | ip-multicast | ipv6 | mpls} maximum-routes
```

```
no mls cef maximum-routes {ip | ip-multicast | ipv6 | mpls}
```

### Syntax Description

<b>ip</b>	Specifies the maximum number of IP routes.
<i>maximum-routes</i>	Maximum number of the routes that can be programmed in the hardware allowed per protocol.
<b>ip-multicast</b>	Specifies the maximum number of multicast routes.
<b>ipv6</b>	Specifies the maximum number of IPv6 routes.
<b>mpls</b>	Specifies the maximum number of Multiprotocol Label Switching (MPLS) labels.

### Command Default

The defaults are as follows:

- For XL-mode systems:
  - IPv4 unicast and MPLS—512,000 routes
  - IPv6 unicast and IPv4 multicast—256,000 routes
- For non-XL mode systems:
  - IPv4 unicast and MPLS—192,000 routes
  - IPv6 unicast and IPv4 multicast—32,000 routes



### Note

See the “Usage Guidelines” section for information on XL and non-XL mode systems.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
12.2(17b)SXA	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

## Usage Guidelines



### Note

If you copy a configuration file that contains the multilayer switching (MLS) Cisco Express Forwarding maximum routes into the startup-config file and reload the Cisco 7600 series router, the Cisco 7600 series router reloads after it reboots.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **mls cef maximum-routes** command limits the maximum number of the routes that can be programmed in the hardware. If routes are detected that exceed the limit for that protocol, an exception condition is generated.

The determination of XL and non-XL mode is based on the type of Policy Feature Card (PFC) or Distributed Forwarding Card (DFC) modules that are installed in your system. For additional information on systems running Cisco IOS software release 12.2SXF and earlier releases see:

[http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL\\_4164.html#Policy\\_Feature\\_Card\\_Guidelines\\_and\\_Restrictions](http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html#Policy_Feature_Card_Guidelines_and_Restrictions)

For additional information on systems running Cisco IOS software release 12.2SXH and later releases see:

[http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/ol\\_14271.html#Policy\\_Feature\\_Card\\_Guidelines\\_and\\_Restrictions](http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/ol_14271.html#Policy_Feature_Card_Guidelines_and_Restrictions)

The valid values for the *maximum-routes* argument depend on the system mode—XL mode or non-XL mode. The valid values are as follows:

- XL mode
  - IP and MPLS—Up to 1,007,000 routes
  - IP multicast and IPv6—Up to 503,000 routes
- Non-XL mode
  - IP and MPLS—Up to 239,000 routes
  - IP multicast and IPv6—Up to 119,000 routes



### Note

The maximum values that you are permitted to configure is not fixed but varies depending on the values that are allocated for other protocols.

An example of how to enter the maximum routes argument is as follows:

```
mls cef maximum-routes ip 4
```

where 4 is 4096 IP routes (1024 x 4 = 4096).

The new configurations are applied after a system reload only and do not take effect if a switchover occurs.



### Note

A switchover might lead to a crash when you have a VSS in a dual supervisor setup due to a lack of synchronization between the TCAM.



In RPR mode, if you change and save the maximum-routes configuration, the redundant supervisor engine reloads when it becomes active from either a switchover or a system reload. The reload occurs 5 minutes after the supervisor engine becomes active.

Use the **show mls cef maximum-routes** command to display the current maximum routes system configuration.

**Examples**

This example shows how to set the maximum number of routes that are allowed per protocol:

```
Router(config)# mls cef maximum-routes ip 100
```

This example shows how to return to the default setting for a specific protocol:

```
Router(config)# no mls cef maximum-routes ip
```

**Related Commands**

Command	Description
<b>show mls cef maximum-routes</b>	Displays the current maximum-route system configuration.

# mls cef tunnel fragment

To allow tunnel fragmentation, use the **mls cef tunnel fragment** command. To return to the default settings, use the **no** form of this command.

**mls cef tunnel fragment**

**no mls cef tunnel fragment**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Tunnel fragmentation is not enabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.2(18)SXF	This command was introduced.
	12.2(33)SXH	This command was modified. Support was added for PCF3BXL, PFC3C, and PFC3CXL modes only.
	12.2(33)SXI	This command was modified. Support was added for PCF3BXL, PFC3C, and PFC3CXL modes only.
	12.2(33)SXI2	This command was modified. Support was added for all PFC3 modes.

**Usage Guidelines** When you enable tunnel fragmentation, if the size of the packets that are going into a tunnel interface exceed the MTU, the packet is fragmented. The packets that are fragmented are reassembled at the destination point.

**Examples** This example shows how to allow tunnel fragmentation:

```
Router(config)# mls cef tunnel fragment
```

This example shows how to return to the default setting:

```
Router(config)# no mls cef tunnel fragment
```

Related Commands	Command	Description
	<b>show mls cef tunnel fragment</b>	Displays the operational status of tunnel fragmentation.

# mls erm priority

To assign the priorities to define an order in which protocols attempt to recover from the exception status, use the **mls erm priority** command in global configuration mode. To return to the default settings, use the **no** form of this command.



**Note**

The **mls erm priority** command is not available in Cisco IOS Release 12.2(33)SXJ and later Cisco IOS 12.2SX releases.

**mls erm priority ipv4** *value* **ipv6** *value* **mpls** *value*

**no mls erm priority ipv4** *value* **ipv6** *value* **mpls** *value*

**Syntax Description**

<b>ipv4</b>	Prioritizes the IPv4 protocol. The default priority is 1.
<i>value</i>	Priority value; valid values are from 1 to 3.
<b>ipv6</b>	Prioritizes the IPv6 protocol. The default priority is 2.
<b>mpls</b>	Prioritizes the Multiprotocol Label Switching (MPLS) protocol. The default priority is 3.

**Command Default**

The default priority settings are used.

**Command Modes**

Global configuration (config)

**Command History**

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to support the <b>ipv6</b> keyword.
12.2(17b)SXA	This command was changed to support the <b>mpls</b> keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXJ	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXJ and later Cisco IOS 12.2SX releases.

**Usage Guidelines**

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

A lower *value* indicates a higher priority.

When a protocol sees a Forwarding Information Base (FIB) table exception, the protocol notifies the FIB Embedded Resource Manager (ERM). The FIB ERM periodically polls the FIB table exception status and decides which protocol gets priority over another protocol when multiple protocols are running under the exception. Only one protocol can attempt to recover from an exception at any time.

If there is sufficient FIB space, the protocol with the highest priority tries to recover first. Other protocols under the exception do not start to recover until the previous protocol completes the recovery process by reloading the appropriate FIB table.

---

**Examples**

This example shows how to set the ERM exception-recovery priority:

```
Router(config)# mls erm priority ipv4 2 ipv6 1 mpls 3
```

This example shows how to return to the default setting:

```
Router(config)# no mls erm priority ipv4 2 ipv6 1 mpls 3
```

---

**Related Commands**

Command	Description
<b>show mls cef exception</b>	Displays information about the Cisco Express Forwarding exception.

# mls ip

To enable multilayer switching (MLS) IP for the internal router on the interface, use the **mls ip** command in interface configuration mode. To disable MLS IP on the interface use the **no** form of this command.

**mls ip**

**no mls ip**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Multicast is disabled.

**Command Modes** Interface configuration (config-if)

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

**Usage Guidelines** This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

**Examples** This example shows how to enable MLS IP:

```
Router(config-if)# mls ip
```

Related Commands	Command	Description
	<b>mls rp ip (interface configuration)</b>	Allows the external systems to enable MLS IP on a specified interface.
	<b>show mls ip multicast</b>	Displays the MLS IP information.

# mls ip cef accounting per-prefix

To enable Multilayer Switching (MLS) per-prefix accounting, use the **mls ip cef accounting per-prefix** command in global configuration mode. To disable MLS per-prefix accounting, use the **no** form of this command

```
mls ip cef accounting per-prefix prefix-entry prefix-entry-mask [instance-name]
```

```
no mls ip cef accounting per-prefix
```

## Syntax Description

<i>prefix-entry</i>	Prefix entry in the format A.B.C.D.
<i>prefix-entry-mask</i>	Prefix entry mask in the format A.B.C.D.
<i>instance-name</i>	(Optional) Virtual Private Network (VPN) routing and forwarding instance name.

## Command Default

MLS per-prefix accounting is disabled by default.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXF	Support for this command was implemented on the Supervisor Engine 32.

## Usage Guidelines

Per-prefix accounting collects the adjacency counters used by the prefix. When the prefix is used for accounting, the adjacency cannot be shared with other prefixes. You can use per-prefix accounting to account for the packets sent to a specific destination.

## Examples

This example shows how to enable MLS per-prefix accounting:

```
Router(config)# mls ip cef accounting per-prefix 172.20.52.18 255.255.255.255
```

This example shows how to disable MLS per-prefix accounting:

```
Router(config)# no mls ip cef accounting per-prefix
```

## Related Commands

Command	Description
<b>show mls cef ip</b>	Displays all the prefixes that are configured for the statistic collection.

# mls ip cef load-sharing

To configure the Cisco Express Forwarding load balancing, use the **mls ip cef load-sharing** command in global configuration mode. To return to the default settings, use the **no** form of this command.

**mls ip cef load-sharing [full] [exclude-port { destination | source }] [simple]**

**no mls ip cef load-sharing**

## Syntax Description

<b>full</b>	(Optional) Sets the Cisco Express Forwarding load balancing to include source and destination Layer 4 ports and source and destination IP addresses (Layer 3).
<b>exclude-port destination</b>	(Optional) Excludes the destination Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm.
<b>exclude-port source</b>	(Optional) Excludes the source Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm.
<b>simple</b>	(Optional) Sets the Cisco Express Forwarding load balancing for single-stage load sharing.

## Defaults

Source and destination IP address and universal identification

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was introduced in Release 12.2(17d)SXB.
12.2(17d)SXB2	This command was changed as follows: <ul style="list-style-type: none"> <li>The <b>simple</b> keyword was added.</li> <li>Support for this command was introduced on the Supervisor Engine 720.</li> </ul>
12.2(18)SXE	This command was changed to include the <b>exclude-port</b> , <b>destination</b> , and <b>source</b> keywords on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

## Usage Guidelines

The **mls ip cef load-sharing** command affects the IPv4, the IPv6, and the Multiprotocol Label Switching (MPLS) forwardings.

The **mls ip cef load-sharing** command is structured as follows:

- **mls ip cef load-sharing full**—Uses Layer 3 and Layer 4 information with multiple adjacencies.
- **mls ip cef load-sharing full simple**—Uses Layer 3 and Layer 4 information without multiple adjacencies.
- **mls ip cef load-sharing simple**—Uses Layer 3 information without multiple adjacencies.

For additional guidelines, refer to the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

### Examples

This example shows how to set load balancing to include Layer 3 and Layer 4 ports with multiple adjacencies:

```
Router(config)# mls ip cef load-sharing full
```

This example shows how to set load balancing to exclude the destination Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm:

```
Router(config)# mls ip cef load-sharing full exclude-port destination
```

This example shows how to set load balancing to exclude the source Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm:

```
Router(config)# mls ip cef load-sharing full exclude-port source
```

This example shows how to return to the default setting:

```
Router(config)# no mls ip cef load-sharing
```

### Related Commands

Command	Description
<code>show mls cef ip</code>	Displays the IP entries in the MLS-hardware Layer 3-switching table.



# mls ip cef rate-limit

To rate-limit Cisco Express Forwarding-punted data packets, use the **mls ip cef rate-limit** command in global configuration mode. To disable the rate-limited Cisco Express Forwarding-punted data packets, use the **no** form of this command.

**mls ip cef rate-limit** *packets-per-second*

**no mls ip cef rate-limit**

<b>Syntax Description</b>	<i>packets-per-second</i> Number of data packets per second; see the “Usage Guidelines” section for the valid values.
---------------------------	---

<b>Defaults</b>	No rate limit is configured.
-----------------	------------------------------

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

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

<b>Usage Guidelines</b>	<p>The valid values for the number of data packets per second are as follows:</p> <ul style="list-style-type: none"> <li>For Cisco 7600 series routers that are configured with a Supervisor Engine 2, the valid values are from 1 to 1000000.</li> <li>For Cisco 7600 series routers that are configured with a Supervisor Engine 720, the valid values are from 0 to 1000000.</li> </ul>
-------------------------	--

Certain denial-of-service attacks target the route processing engines of routers. Certain packets that cannot be forwarded by the Policy Feature Card (PFC) are directed to the Multilayer Switch Feature Card (MSFC) for processing. Denial-of-service attacks can overload the route processing engine and cause routing instability when running dynamic routing protocols. You can use the **mls ip cef rate-limit** command to limit the amount of traffic that is sent to the MSFC to prevent denial-of-service attacks against the route processing engine.

This command rate limits all Cisco Express Forwarding-punted data packets including the following:

- Data packets going to the local interface IP address
- Data packets requiring Address Resolution Protocol (ARP)

Setting the rate to a low value could impact the packets that are destined to the IP addresses of the local interfaces and the packets that require ARP.

You should use this command to limit these packets to a normal rate and to avoid abnormal incoming rates.

For additional guidelines, see the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

---

**Examples**

This example shows how to enable and set rate limiting:

```
Router(config)# mls ip cef rate-limit 50000
```

---

**Related Commands**

Command	Description
<code>show mls cef ip</code>	Displays the IP entries in the MLS-hardware Layer 3-switching table.

# mls ip cef rpf hw-enable-rpf-acl

To enable hardware unicast Reverse Path Forwarding (uRPF) for packets matching the deny Access Control List (ACL) when uRPF with ACL is enabled, use the **mls ip cef rpf hw-enable-rpf-acl** command in global configuration mode. To disable hardware uRPF when RPF and ACL are enabled, use the **no** form of this command.

**mls ip cef rpf hw-enable-rpf-acl**

**no mls ip cef rpf hw-enable-rpf-acl**

**Syntax Description** This command has no arguments or keywords.

**Command Default** uRPF is disabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.2(18)SXF6	This command was introduced.

**Usage Guidelines** This command is supported on systems configured with a PFC3 (Supervisor Engine 720 and Supervisor Engine 32) only.

If you do not enter the **mls ip cef rpf hw-enable-rpf-acl** command, when the uRPF with ACL is specified, packets that are permitted by the uRPF ACL are forwarded in hardware and the denied packets are sent to the Multilayer Switching Feature Card (MSFC) for the uRPF check. This command enables hardware forwarding with the uRPF check for the packets that are denied by the uRPF ACL. However, in this case packets permitted by the uRPF ACL are sent to the MSFC for forwarding.

**Examples** This example shows how to enable hardware uRPF when RPF and ACL are enabled:

```
mls ip cef rpf hw-enable-rpf-acl
```

This example shows how to disable hardware uRPF when RPF and ACL are enabled:

```
no mls ip cef rpf hw-enable-rpf-acl
```

Related Commands	Command	Description
	<b>ip verify unicast source reachable-via</b>	Enables and configures RPF checks with ACL.

# mls ip cef rpf interface-group

To define an interface group in the Reverse Path Forwarding (RPF)-VLAN table, use the **mls ip cef rpf interface-group** command in global configuration mode. To delete the interface group, use the **no** form of this command.

```
mls ip cef rpf interface-group group-number interface1 interface2 interface3 [...]
```

```
no mls ip cef rpf interface-group group-number interface1 interface2 interface3 [...]
```

## Syntax Description

<i>group-number</i>	Interface group number; valid values are from 1 to 4.
<i>interface</i>	Interface number; see the “Usage Guidelines” section for formatting guidelines.
...	(Optional) Additional interface numbers; see the “Usage Guidelines” section for additional information.

## Defaults

No groups are configured.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

A single interface group contains three to six interfaces. You can configure up to four interface groups. For each interface group, the first four entries are installed in the hardware RPF-VLAN table.

Enter the *interface* as *interface-typemod/port*.

Separate each interface entry with a space. You do not have to include a space between the *interface-type* and the *mod/port* arguments. See the “Examples” section for a sample entry.

## Examples

This example shows how to define an interface group:

```
Router(config)# mls ip cef rpf interface-group 0 F2/1 F2/2 F2/3 F2/4 F2/5 F2/6
```

# mls ip cef rpf multipath

To configure the Reverse Path Forwarding (RPF) modes, use the **mls ip cef rpf multipath** command in global configuration mode. To return to the default settings, use the **no** form of this command.

**mls ip cef rpf multipath {interface-group | punt | pass}**

**no mls ip cef rpf multipath {interface-group | punt | pass}**

## Syntax Description

<b>interface-group</b>	Disables the RPF check for packets coming from multiple path routes; see the “Usage Guidelines” section for additional information.
<b>punt</b>	Redirects the RPF-failed packets to the route processor for multiple path prefix support.
<b>pass</b>	Disables the RPF check for packets coming from multiple path routes.

## Defaults

**punt**

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The interface-group mode is similar to the pass mode but utilizes the RPF\_VLAN global table for the RPF check. Packets from other multiple path prefixes always pass the RPF check.

You enter the **mls ip cef rpf multipath interface-group** command to define an RPF\_VLAN table interface group. One interface group contains from three to six interfaces, and you can configure up to four interface groups. For each interface group, the first four entries are installed in the hardware RPF\_VLAN table. For the prefix that has more than three multiple paths, and all paths except two are part of that interface group, the FIB entry of that prefix uses this RPF\_VLAN entry.

## Examples

This example shows how to redirect the RPF-failed packets to the route processor for multiple path prefix support:

```
Router(config)# mls ip cef rpf multipath interface-group
```

## Related Commands

Command	Description
<b>show mls cef ip</b>	Displays the IP entries in the MLS-hardware Layer 3-switching table.

# monitor elog trigger position

To monitor system events using event-logging control and trigger control parameters, use the **monitor elog trigger position** command in privileged EXEC configuration mode.

**monitor elog trigger position** *position-percentage*

<b>Syntax Description</b>	<i>position-percentage</i>	The position of the trigger in the buffer expressed in percentage.
---------------------------	----------------------------	--

<b>Command Default</b>	System events are not monitored and logged.
------------------------	---

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

<b>Examples</b>	The following example shows how to monitor 50 percent of the system events using event-logging control and trigger control parameters:
-----------------	--

```
Router# monitor elog trigger position 50
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>monitor call leg event-log</b>	Displays the event log for an active call leg in real time.

# monitor event-trace (EXEC)

To monitor and control the event trace function for a specified Cisco IOS software subsystem component, use the **monitor event-trace** command in privileged EXEC mode.

**monitor event-trace** *component* { **clear** | **continuous** | **disable** | **dump** [**pretty**] | **enable** | **one-shot** }

## Cisco 10000 Series Routers

**monitor event-trace** *component* { **disable** | **dump** | **enable** | **size** | **stacktrace** }

## Catalyst 6500 Series Switches and Cisco 7600 Series Routers

**monitor event-trace all-traces** { **continuous** [**cancel**] | **dump** [**merged**] [**pretty**] }

**monitor event-trace l3** { **clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **interface** *type mod/port* | **one-shot** }

**monitor event-trace spa** { **clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot** }

**monitor event-trace subsys** { **clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot** }

### Syntax Description

<i>component</i>	Name of the Cisco IOS software subsystem component that is the subject of the event trace. To get a list of components that support event tracing, use the <b>monitor event-trace ?</b> command.
<b>clear</b>	Clears existing trace messages for the specified component from memory on the networking device.
<b>continuous</b>	Continuously displays the latest event trace entries.
<b>disable</b>	Turns off event tracing for the specified component.
<b>dump</b>	Writes the event trace results to the file configured using the <b>monitor event-trace</b> command in global configuration mode. The trace messages are saved in binary format.
<b>pretty</b>	(Optional) Saves the event trace message in ASCII format.
<b>enable</b>	Turns on event tracing for the specified component.
<b>one-shot</b>	Clears any existing trace information from memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the <b>monitor event-trace</b> command in global configuration mode.
<b>size</b>	Sets the number of messages that can be written to memory for a single instance of a trace.  <b>Note</b> Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the <b>show monitor event-trace component parameters</b> command.
	When the number of event trace messages in memory exceeds the size, new messages will begin to overwrite the older messages in the file.
<b>stacktrace</b>	Enables the stack trace at tracepoints.
<b>all-traces</b>	Displays the configured merged-event traces.

<b>merged</b>	(Optional) Dumps the entries in all event traces sorted by time.
<b>l3</b>	Displays information about the Layer 3 trace.
<b>spa</b>	Displays information about the Shared Port Adapter (SPA) trace.
<b>interface type mod/port</b>	Specifies the interface to be logged.
<b>cancel</b>	(Optional) Cancels the continuous display of latest trace entries.
<b>subsys</b>	Displays information about the subsystem's initial trace.

**Command Default**

The event trace function is disabled by default.

**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(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The <b>monitor event-trace cef ipv4 clear</b> command replaces the <b>clear ip cef event-log</b> command.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

**Usage Guidelines**

Use the **monitor event-trace** command to control what, when, and how event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the **monitor event-trace** command in global configuration mode.



**Note** The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace** command in global configuration mode for each instance of a trace.

The Cisco IOS software allows for the subsystem components to define whether support for event tracing is enabled or disabled at boot time. You can enable or disable event tracing in two ways: using the **monitor event-trace** command in privileged EXEC mode or using the **monitor event-trace** command in global configuration mode. To disable event tracing, you would enter either of these commands with the **disable** keyword. To enable event tracing again, you would enter either of these commands with the **enable** keyword.

To determine whether you can enable event tracing on a subsystem, use the **monitor event-trace ?** command to get a list of software components that support event tracing. To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace** command to display trace messages.



Use the **show monitor event-trace** command to display trace messages. Use the **monitor event-trace component dump** command to save trace message information for a single event. By default, trace information is saved in binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the **monitor event-trace component dump pretty** command.

To write the trace messages for all events currently enabled on a networking device to a file, enter the **monitor event-trace dump** command.

To configure the file where you want to save trace information, use the **monitor event-trace** command in global configuration mode. The trace messages are saved in a binary format.

## Examples

The following example shows the privileged EXEC commands to stop event tracing, clear the current contents of memory, and reenables the trace function for the interprocess communication (IPC) component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace ipc disable
Router# monitor event-trace ipc clear
Router# monitor event-trace ipc enable
```

The following example shows how the **monitor event-trace one-shot** command accomplishes the same function as the previous example except in one command. In this example, once the size of the trace message file has been exceeded, the trace is terminated.

```
Router# monitor event-trace ipc one-shot
```

The following example shows the command for writing trace messages for an event in binary format. In this example, the trace messages for the IPC component are written to a file.

```
Router# monitor event-trace ipc dump
```

The following example shows the command for writing trace messages for an event in ASCII format. In this example, the trace messages for the MBUS component are written to a file.

```
Router# monitor event-trace mbus dump pretty
```

### Catalyst 6500 Series Switches and Cisco 7600 Series Routers Examples Only

This example shows how to stop event tracing, clear the current contents of memory, and reenables the trace function for the SPA component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace spa disable
Router# monitor event-trace spa clear
Router# monitor event-trace spa enable
```

## Related Commands

Command	Description
<b>monitor event-trace (global)</b>	Configures event tracing for a specified Cisco IOS software subsystem component.
<b>monitor event-trace dump-traces</b>	Saves trace messages for all event traces currently enabled on the networking device.
<b>show monitor event-trace</b>	Displays event trace messages for Cisco IOS software subsystem components.

## monitor event-trace (global)

To configure event tracing for a specified Cisco IOS software subsystem component, use the **monitor event-trace** command in global configuration mode.

```
monitor event-trace component { disable | dump-file filename | enable | size number | stacktrace
number } timestamps [datetime [localtime] [msec] [show-timezone] | uptime]
```

### Cisco 10000 Series Routers

```
monitor event-trace component { disable | dump-file filename | enable | clear | continuous |
one-shot }
```

Syntax Description		
<i>component</i>	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, use the <b>monitor event-trace ?</b> command.	
<b>disable</b>	Turns off event tracing for the specified component.	
<b>dump-file</b> <i>filename</i>	Specifies the file where 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.	
<b>enable</b>	Turns on event tracing for the specified component provided that the component has been configured using the <b>monitor event-trace</b> command.	
<b>size</b> <i>number</i>	Sets the number of messages that can be written to memory for a single instance of a trace. Valid values are from 1 to 65536.	<p><b>Note</b> Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the <b>show monitor event-trace component parameters</b> command.</p> <p>When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.</p>
<b>stacktrace</b> <i>number</i>	Enables the stack trace at tracepoints and specifies the depth of the stack trace stored. Valid values are from 1 to 16.	
<b>timestamps</b>	(Optional) Includes time stamp information with the event trace messages for the specified component.	
<b>datetime</b>	(Optional) Specifies that the time stamp information included with event trace messages will consist of the date and time of the event trace.	
<b>localtime</b>	(Optional) Specifies that the time given in the time stamp will be local time.	
<b>msec</b>	(Optional) Includes milliseconds in the time stamp.	
<b>show-timezone</b>	(Optional) Includes time zone information in the time stamp.	
<b>uptime</b>	(Optional) Displays time stamped information about the system uptime.	
<b>clear</b>	Clears existing trace messages for the specified component from memory on the networking device.	

<b>continuous</b>	Continuously displays the latest event trace entries.
<b>one-shot</b>	Clears any existing trace information from memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the <b>monitor event-trace</b> command.

**Command Default** Event tracing is enabled or disabled depending on the software component.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and implemented on the Supervisor Engine 720.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

**Usage Guidelines** Use the **monitor event-trace** command to enable or disable event tracing and to configure event trace parameters for Cisco IOS software subsystem components.



**Note**

Event tracing is intended for use as a software diagnostic tool and should be configured only under the direction of a Technical Assistance Center (TAC) representative. In Cisco IOS software images that do not provide subsystem support for the event trace function, the **monitor event-trace** command is not available.

The Cisco IOS software allows the subsystem components 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 two ways: using the **monitor event-trace** command in privileged EXEC mode or using the **monitor event-trace** command in global configuration mode.

Additionally, default settings do not show up in the configuration file. If the subsystem software enables event tracing by default, the **monitor event-trace component enable** command will not show up in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem will create a command entry in the configuration file.



**Note**

The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace** command for each instance of a trace.

To determine whether you can enable event tracing on a subsystem, use the **monitor event-trace ?** command to get a list of software components that support event tracing.

To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace** command to display trace messages.

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

## Examples

The following example shows how to enable event tracing for the interprocess communication (IPC) subsystem component in Cisco IOS software and configure the size to 4096 messages. The trace messages file is set to ipc-dump in slot0 (flash memory).

```
configure terminal
!
monitor event-trace ipc enable
monitor event-trace ipc dump-file slot0:ipc-dump
monitor event-trace ipc size 4096
```

When you select Cisco Express Forwarding as the component for which to enable event tracing, you can use the following additional arguments and keywords: **monitor event-trace cef [events | interface | ipv6 | ipv4][all]**. The following example shows how to enable event tracing for IPv4 or IPv6 events of the Cisco Express Forwarding component in Cisco IOS software:

```
configure terminal
!
monitor event-trace cef ipv4 enable

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

The following example shows what happens when you try to enable event tracing for a component (in this case, adjacency events) when it is already enabled:

```
configure terminal
!
monitor event-trace adjacency enable

%EVENT_TRACE-6-ENABLE: Trace already enabled.
```

## Related Commands

Command	Description
<b>monitor event-trace (EXEC)</b>	Controls the event trace function for a specified Cisco IOS software subsystem component.
<b>monitor event-trace dump-traces</b>	Saves trace messages for all event traces currently enabled on the networking device.
<b>show monitor event-trace</b>	Displays event trace messages for Cisco IOS software subsystem components.

# monitor event-trace cef (EXEC)

To monitor and control the event trace function for Cisco Express Forwarding, use the **monitor event-trace cef** command in privileged EXEC mode.

```
monitor event-trace cef { dump [merged pretty | pretty] | { events | interface | ipv4 | ipv6 } { clear
| continuous [cancel] | disable | dump [pretty] | enable | one-shot } }
```

## Syntax Description

<b>dump</b>	Writes the event trace results to the file configured with the global configuration <b>monitor event-trace cef</b> command. The trace messages are saved in binary format.
<b>merged pretty</b>	(Optional) Sorts all event trace entries by time and writes the entries to a file in ASCII format.
<b>pretty</b>	(Optional) Saves the event trace message in ASCII format.
<b>events</b>	Monitors Cisco Express Forwarding events.
<b>interface</b>	Monitors Cisco Express Forwarding interface events.
<b>ipv4</b>	Monitors Cisco Express Forwarding IPv4 events.
<b>ipv6</b>	Monitors Cisco Express Forwarding IPv6 events.
<b>clear</b>	Clears existing trace messages for Cisco Express Forwarding from memory on the networking device.
<b>continuous</b>	Continuously displays the latest event trace entries.
<b>cancel</b>	(Optional) Cancels the continuous display of the latest trace entries.
<b>disable</b>	Turns off Cisco Express Forwarding event tracing.
<b>enable</b>	Turns on Cisco Express Forwarding event tracing.
<b>one-shot</b>	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 Default

Event tracing for Cisco Express Forwarding is enabled by default.

## 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(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(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.

Release	Modification
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

Use the **monitor event-trace cef** command to control what, when, and how Cisco Express Forwarding event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the **monitor event-trace cef** command in global configuration mode.



**Note** The amount of data collected from the 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.

You can enable or disable Cisco Express Forwarding event tracing 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 disable event tracing, you would enter either of these commands with the **disable** keyword. To enable event tracing again, you would enter either of these commands with the **enable** keyword.

Use the **show monitor event-trace cef** command to display trace messages. Use the **monitor event-trace cef dump** command to save trace message information for a single event. By default, trace information is saved in 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.

To configure the file in which you want to save trace information, use the **monitor event-trace cef** command in global configuration mode. The trace messages are saved in a binary format.

### Examples

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

```
Router# monitor event-trace cef events disable
Router# monitor event-trace cef events clear
Router# monitor event-trace cef events enable
```

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

```
Router# monitor event-trace cef ipv4 continuous
```

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

```
Router# monitor event-trace cef ipv4 continuous cancel
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>monitor event-trace cef (global)</b>	Configures event tracing for Cisco Express Forwarding.
<b>monitor event-trace cef ipv4 (global)</b>	Configures event tracing for Cisco Express Forwarding IPv4 events.
<b>monitor event-trace cef ipv6 (global)</b>	Configures event tracing for Cisco Express Forwarding IPv6 events.
<b>show monitor event-trace cef</b>	Displays event trace messages for Cisco Express Forwarding.
<b>show monitor event-trace cef events</b>	Displays event trace messages for Cisco Express Forwarding events.
<b>show monitor event-trace cef interface</b>	Displays event trace messages for Cisco Express Forwarding interface events.
<b>show monitor event-trace cef ipv4</b>	Displays event trace messages for Cisco Express Forwarding IPv4 events.
<b>show monitor event-trace cef ipv6</b>	Displays event trace messages for Cisco Express Forwarding IPv6 events.

## monitor event-trace cef (global)

To configure event tracing for Cisco Express Forwarding, use the **monitor event-trace cef** command in global configuration mode. To disable event tracing for Cisco Express Forwarding, use the **no** form of this command.

```
monitor event-trace cef { dump-file dump-file-name | { events | interface } } { disable | dump-file dump-file-name | enable | size number | stacktrace [depth] }
```

```
no monitor event-trace cef { dump-file dump-file-name | { events | interface } } { disable | dump-file dump-file-name | enable | size | stacktrace [depth] }
```

### Syntax Description

<b>dump-file</b> <i>dump-file-name</i>	Specifies 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.
<b>events</b>	Turns on event tracing for Cisco Express Forwarding events.
<b>interface</b>	Turns on event tracing for Cisco Express Forwarding interface events.
<b>disable</b>	Turns off event tracing for Cisco Express Forwarding events.
<b>enable</b>	Turns on event tracing for Cisco Express Forwarding events if it had been enabled with the <b>monitor event-trace cef</b> command.
<b>size</b> <i>number</i>	Sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536.  <b>Note</b> Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the <b>show monitor event-trace cef parameters</b> command.  When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
<b>stacktrace</b>	Enables the stack trace at tracepoints.
<i>depth</i>	(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.

### Command Default

Event tracing for Cisco Express Forwarding is enabled by default.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(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.



Release	Modification
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

### Usage Guidelines

Use the **monitor event-trace cef** command to enable or disable event tracing and to configure event trace parameters for Cisco Express Forwarding.

The Cisco IOS 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.

Additionally, default settings do not appear in the configuration file. If Cisco Express Forwarding enables event tracing by default, the **monitor event-trace cef enable** command does not appear in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem creates a command entry in the configuration file.



### Note

The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace cef** 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** command to display trace messages.

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

### Examples

The following example shows how to enable event tracing for Cisco Express Forwarding and configure the buffer size to 5000 messages. The trace messages file is set to cef-dump in slot0 (flash memory).

```
Router(config)# monitor event-trace cef events enable

Router(config)# monitor event-trace cef dump-file slot0:cef-dump

Router(config)# monitor event-trace cef events size 5000
```

The following example shows what happens when you try to enable event tracing for Cisco Express Forwarding events when it is already enabled:

```
Router(config)# monitor event-trace cef events enable

Router(config)#
00:04:33: %EVENT_TRACE-6-ENABLE: Trace already enabled.
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>monitor event-trace cef (EXEC)</b>	Monitors and controls the event trace function for Cisco Express Forwarding.
<b>monitor event-trace cef ipv4 (global)</b>	Configures event tracing for Cisco Express Forwarding IPv4 events.
<b>monitor event-trace cef ipv6 (global)</b>	Configures event tracing for Cisco Express Forwarding IPv6 events.
<b>show monitor event-trace cef</b>	Displays event trace messages for Cisco Express Forwarding.
<b>show monitor event-trace cef events</b>	Displays event trace messages for Cisco Express Forwarding events.
<b>show monitor event-trace cef interface</b>	Displays event trace messages for Cisco Express Forwarding interface events.
<b>show monitor event-trace cef ipv4</b>	Displays event trace messages for Cisco Express Forwarding IPv4 events.
<b>show monitor event-trace cef ipv6</b>	Displays event trace messages for Cisco Express Forwarding IPv6 events.

## monitor event-trace cef ipv4 (global)

To configure event tracing for Cisco Express Forwarding IPv4 events, use the **monitor event-trace cef ipv4** command in global configuration mode. To disable event tracing for Cisco Express Forwarding IPv4 events, use the **no** form of this command.

```
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 } ] }
```

```
no monitor event-trace cef { ipv4 { disable | distribution | dump-file dump-file-name | enable |
  match | size | stacktrace [depth] } | vrf }
```

Syntax Description	
<b>disable</b>	Turns off event tracing for Cisco Express Forwarding IPv4 events.
<b>distribution</b>	Logs events related to the distribution of Cisco Express Forwarding Forwarding Information Base (FIB) tables to the line cards.
<b>dump-file</b> <i>dump-file-name</i>	Specifies 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.
<b>enable</b>	Turns on event tracing for Cisco Express Forwarding IPv4 events if it had been enabled with the <b>monitor event-trace cef</b> command.
<b>match</b>	Turns on event tracing for Cisco Express Forwarding IPv4 that matches global events or events that match a specific network address.
<b>global</b>	Specifies global events.
<i>ip-address mask</i>	Specifies an IP address in A.B.C.D format and a subnet mask in A.B.C.D format.
<b>size number</b>	Sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536.  <b>Note</b> Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the <b>show monitor event-trace cef parameters</b> command.  When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
<b>stacktrace</b>	Enables the stack trace at tracepoints.
<i>depth</i>	(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.
<b>vrf vrf-name</b>	Turns on event tracing for a Cisco Express Forwarding IPv4 Virtual Private Network (VPN) routing and forwarding (VRF) table. The <i>vrf-name</i> argument specifies the name of the VRF.

**Command Default** Event tracing for Cisco Express Forwarding IPv4 events is enabled by default.

**Command Modes** Global configuration (config)

**Command History**

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines**

Use the **monitor event-trace cef ipv4** command to enable or disable event tracing for Cisco Express Forwarding IPv4 events.

The Cisco IOS 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.

**Note**

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.

**Examples**

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

```
Router(config)# monitor event-trace cef ipv4 enable
```

```
Router(config)# monitor event-trace cef ipv4 size 5000
```

The following example shows how to enable event tracing for events that match Cisco Express Forwarding IPv4 VRF vpn1:

```
Router(config)# monitor event-trace cef ipv4 enable
```

```
Router(config)# monitor event-trace cef ipv4 vrf vpn1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>monitor event-trace cef (EXEC)</b>	Monitors and controls the event trace function for Cisco Express Forwarding.
<b>monitor event-trace cef (global)</b>	Configures event tracing for Cisco Express Forwarding.
<b>monitor trace-event cef ipv6 (global)</b>	Configures event tracing for Cisco Express Forwarding IPv6 events.
<b>show monitor event-trace cef</b>	Displays event trace messages for Cisco Express Forwarding.
<b>show monitor event-trace cef events</b>	Displays event trace messages for Cisco Express Forwarding events.
<b>show monitor event-trace cef interface</b>	Displays event trace messages for Cisco Express Forwarding interface events.
<b>show monitor event-trace cef ipv4</b>	Displays event trace messages for Cisco Express Forwarding IPv4 events.
<b>show monitor event-trace cef ipv6</b>	Displays event trace messages for Cisco Express Forwarding IPv6 events.

## monitor event-trace cef ipv6 (global)

To configure event tracing for Cisco Express Forwarding IPv6 events, use the **monitor event-trace cef ipv6** command in global configuration mode. To disable event tracing for Cisco Express Forwarding, use the **no** form of this command.

```
monitor event-trace cef ipv6 { 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 } ] }
```

```
no monitor event-trace cef ipv6 { disable | distribution | dump-file dump-file-name | enable |
  match | size | stacktrace [depth] | vrf }
```

Syntax	Description
<b>disable</b>	Turns off event tracing for Cisco Express Forwarding IPv6 events.
<b>distribution</b>	Logs events related to the distribution of Cisco Express Forwarding Forwarding Information Base (FIB) tables to the line cards.
<b>dump-file</b> <i>dump-file-name</i>	Specifies 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.
<b>enable</b>	Turns on event tracing for Cisco Express Forwarding IPv6 events if it had been enabled with the <b>monitor event-trace cef ipv6</b> command.
<b>match</b>	Turns on event tracing for Cisco Express Forwarding IPv6 that matches global events or events that match a specific network address.
<b>global</b>	Specifies global events.
<i>ipv6-address/n</i>	Specifies an IPv6 address. This address must be in the form documented in RFC 2373: the address is specified in hexadecimal using 16-bit values between colons. The slash followed by a number ( <i>n</i> ) indicates the number of bits that do not change. Range: 0 to 128.
<b>size</b> <i>number</i>	Sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536.  <b>Note</b> Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the <b>show monitor event-trace cef parameters</b> command.  When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
<b>stacktrace</b>	Enables the stack trace at tracepoints.
<i>depth</i>	(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.
<b>vrf</b> <i>vrf-name</i>	Turns on event tracing for a Cisco Express Forwarding IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) table. The <i>vrf-name</i> argument specifies the name of the VRF.

**Command Default** Event tracing for Cisco Express Forwarding IPv6 events is enabled by default.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.2(25)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
	12.2(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.
	Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

**Usage Guidelines** Use the **monitor event-trace cef ipv6** command to enable or disable event tracing for Cisco Express Forwarding IPv6 events.

The Cisco IOS 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.



**Note** 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 IPv6 events, 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.

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

```
Router(config)# monitor event-trace cef ipv6 enable

Router(config)# monitor event-trace cef ipv6 size 10000
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>monitor event-trace cef (EXEC)</b>	Monitors and controls the event trace function for Cisco Express Forwarding.
<b>monitor event-trace cef (global)</b>	Configures event tracing for Cisco Express Forwarding.
<b>monitor event-trace cef ipv4 (global)</b>	Configures event tracing for Cisco Express Forwarding IPv4 events.
<b>show monitor event-trace cef</b>	Displays event trace messages for Cisco Express Forwarding.
<b>show monitor event-trace cef events</b>	Displays event trace messages for Cisco Express Forwarding events.
<b>show monitor event-trace cef interface</b>	Displays event trace messages for Cisco Express Forwarding interface events.
<b>show monitor event-trace cef ipv4</b>	Displays event trace messages for Cisco Express Forwarding IPv4 events.
<b>show monitor event-trace cef ipv6</b>	Displays event trace messages for Cisco Express Forwarding IPv6 events.