

enabled (aggregation cache)

To enable a NetFlow accounting aggregation cache, use the **enabled** command in NetFlow aggregation cache configuration mode. To disable a NetFlow accounting aggregation cache, use the **no** form of this command.

enabled

no enabled

Syntax Description

This command has no arguments or keywords.

Defaults

No aggregation cache is enabled.

Command Modes

NetFlow aggregation cache configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Examples

The following example shows how to enable a NetFlow protocol-port aggregation cache:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# enabled
```

The following example shows how to disable a NetFlow protocol-port aggregation cache:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# no enabled
```

Related Commands

Command	Description
cache	Defines operational parameters for NetFlow accounting aggregation caches.
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow accounting aggregation cache schemes.
mask (IPv4)	Specifies the source or destination prefix mask for a NetFlow accounting prefix aggregation cache.
show ip cache flow aggregation	Displays the NetFlow accounting aggregation cache statistics.

■ enabled (aggregation cache)

Command	Description
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration on interfaces.

encapsulation (Any Transport over MPLS)

To configure the ATM adaptation layer (AAL) for an Any Transport over MPLS (AToM) ATM permanent virtual circuit (PVC), use the **encapsulation** command in AToM VC configuration mode. To remove an encapsulation from an AToM PVC, use the **no** form of this command.

encapsulation *layer-type*

no encapsulation *layer-type*

Syntax Description

<i>layer-type</i>	The adaptation layer type. Possible values are: aal5 —ATM adaptation layer 5 aal0 —ATM adaptation layer 0
-------------------	---

Defaults

The default encapsulation is AAL5.

Command Modes

AToM VC configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The **pvc** command and the **encapsulation** command work together. How you use the commands for AToM is slightly different than for all other applications. The following table shows the differences in how the commands are used:

Other Applications	AToM
<code>pvc 1/100 encapsulation aal5snap</code>	<code>pvc 1/100 l2transport encapsulation aal5</code>

The following list highlights the differences:

- **pvc** command: For most applications, you create a PVC by using the **pvc vpi/vci** command. For AToM, you must add the **l2transport** keyword to the **pvc** command. The **l2transport** keyword enables the PVC to transport Layer 2 packets.
- **encapsulation** command: The **encapsulation** command for AToM has only two keyword values: **aal5** or **aal0**. You cannot specify an encapsulation type. In contrast, the **encapsulation aal5** command you use for most other applications requires you to specify the encapsulation type, such as **aal5snap**.
- **pvc** command and **encapsulation** command: The AToM **encapsulation** command works only with the **pvc** command. You cannot create switched virtual circuits or VC bundles to transport Layer 2 packets. You can only use PVCs to transport Layer 2 packets.

When you use the **aal5** keyword, incoming cells (except Operation, Administration, and Maintenance [OAM] cells) on that PVC are treated as AAL5 encapsulated packets. The router reassembles the packet from the incoming cells. The router does not check the contents of the packet, so it does not need to know the encapsulation type (such as aal5snap, aal5mux, and so on). After imposing the Multiprotocol Label Switching (MPLS) label stack, the router sends the reassembled packet over the MPLS core network.

When you use the **aal0** keyword, the router strips the header error control (HEC) byte from the cell header and adds the MPLS label stack. The router sends the cell over the MPLS core network.

Examples

The following example shows how to configure a PVC to transport ATM Cell Relay packets for AToM:

```
Router(config-if)# pvc 1/100 l2transport
Router(config-atm-vc)# encapsulation aal0
```

Related Commands

Command	Description
pvc	Creates or assigns a name to an ATM PVC.

encapsulation dot1q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN), use the **encapsulation dot1q** command in interface range mode.

encapsulation dot1q *vlan-id* [**native**]

Syntax Description

<i>vlan-id</i>	Virtual LAN identifier. The allowed range is from 1 to 4095.
native	(Optional) Sets the VLAN ID value of the port to the value specified by the <i>vlan-id</i> argument.

Defaults

IEEE 802.1Q encapsulation is disabled.

Command Modes

Interface range

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)T	The native keyword was added.
12.2(2)DD	Configuration of this command in interface range mode was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

IEEE 802.1Q encapsulation is configurable on Fast Ethernet interfaces. IEEE 802.1Q is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

Use the **encapsulation dot1q** command in interface range mode to apply a VLAN ID to each subinterface within the range specified by the **interface range** command. The VLAN ID specified by the *vlan-id* argument is applied to the first subinterface in the range. Each subsequent interface is assigned a VLAN ID, which is the specified *vlan-id* plus the subinterface number minus the first subinterface number (VLAN ID + subinterface number – first subinterface number).

Do not configure encapsulation on the native VLAN of an IEEE 802.1Q trunk without the **native** keyword. (Always use the **native** keyword when *vlan-id* is the ID of the IEEE 802.1Q native VLAN.)

Examples

The following example shows how to create the subinterfaces within the range 0.11 and 0.60 and apply VLAN ID 101 to the Fast Ethernet0/0.11 subinterface, VLAN ID 102 to Fast Ethernet0/0.12 (*vlan-id* = 101 + 12 – 11 = 102), and so on up to VLAN ID 150 to Fast Ethernet0/0.60 (*vlan-id* = 101 + 60 – 11 = 150):

```
Router(config)# interface range fastethernet0/0.11 - fastethernet0/0.60
Router(config-int-range)# encapsulation dot1q 101
```

Related Commands

Command	Description
encapsulation isl	Enables the Inter-Switch Link (ISL), which is a Cisco proprietary protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches.
encapsulation sde	Enables IEEE 802.10 encapsulation of traffic on a specified subinterface in VLANs.

encapsulation isl

To enable the Inter-Switch Link (ISL), use the **encapsulation isl** command in subinterface configuration mode.

encapsulation isl *vlan-identifier*

Syntax Description	<i>vlan-identifier</i>	Virtual LAN (VLAN) identifier. The allowed range is from 1 to 1000.
---------------------------	------------------------	---

Defaults	ISL is disabled.
-----------------	------------------

Command Modes	Subinterface configuration
----------------------	----------------------------

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines	<p>ISL is a Cisco protocol for interconnecting multiple switches and routers, and for defining VLAN topologies.</p> <p>ISL encapsulation is configurable on Fast Ethernet interfaces.</p> <p>ISL encapsulation adds a 26-byte header to the beginning of the Ethernet frame. The header contains a 10-bit VLAN identifier that conveys VLAN membership identities between switches.</p>
-------------------------	---

Examples	The following example shows how to enable ISL on Fast Ethernet subinterface 2/1.20:
-----------------	---

```
Router(config)# interface FastEthernet 2/1.20
```

```
Router(config-subif)# encapsulation isl 400
```

Related Commands	Command	Description
	bridge-group	Assigns each network interface to a bridge group.
	show interfaces	Displays statistics for all interfaces configured on the router or access server.
	show vlans	Displays VLAN subinterfaces.

encapsulation sde

To enable IEEE 802.10 encapsulation of traffic on a specified subinterface in virtual LANs (VLANs), use the **encapsulation sde** command in subinterface configuration mode.

encapsulation sde *sa-id*

Syntax Description

<i>sa-id</i>	Security association identifier. This value is used as the VLAN identifier. The valid range is from 0 to 0xFFFFFFFFE.
--------------	---

Defaults

IEEE 802.10 encapsulation is disabled.

Command Modes

Subinterface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

IEEE 802.10 is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

Secure Data Exchange (SDE) encapsulation is configurable only on the following interface types:

- IEEE 802.10 routing: FDDI
- IEEE 802.10 transparent bridging:
 - Ethernet
 - FDDI
 - HDLC serial
 - Transparent mode
 - Token Ring

Examples

The following example shows how to enable SDE on FDDI subinterface 2/0.1 and assigns a VLAN identifier of 9999:

```
Router(config)# interface fddi 2/0.1
Router(config-subif)# encapsulation sde 9999
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show vlans	Displays VLAN subinterfaces.

exit-address-family

To exit from the address family configuration submode, use the **exit-address-family** command in address family configuration submode.

exit-address-family

Syntax Description This command has no arguments or keywords.

Defaults This command has no default behavior or values.

Command Modes Address family configuration submode

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines This command can be abbreviated to **exit**.

Examples The following example shows how to exit the address family configuration mode:

```
(config-router-af)# exit-address-family
```

Related Commands	Command	Description
	address-family	Enters the address family submode for configuring routing protocols, such as BGP, RIP, and static routing.

export

To enable the exporting of NetFlow accounting information from NetFlow aggregation caches, use the **export** command in NetFlow aggregation cache configuration mode. To disable the export of NetFlow accounting information from NetFlow aggregation caches, use the **no** form of this command.

```
export {destination ip-address | hostname} udp-port | version [8 | 9] | template [refresh-rate
packets | timeout-rate minutes]
```

```
no export {destination ip-address | hostname} udp-port | version | template [refresh-rate |
timeout-rate]
```

Syntax Description

destination <i>ip-address</i> <i>hostname</i> <i>udp-port</i>	IP address or hostname of the workstation to which you want to send the NetFlow information and the number of the UDP port on which the workstation is listening for this input.
version [8 9]	(Optional) Version of the format for the export.
template	Enables the refresh-rate and timeout-rate keywords for configuring Version 9 export templates.
refresh-rate <i>packets</i>	(Optional) Specifies the number of export datagrams that are sent before the templates are resent. You can specify from 1 to 600 packets. The default is 20 packets.
timeout-rate <i>minutes</i>	(Optional) Specifies the interval (in minutes) between which the templates are resent. You can specify from 1 to 3600 minutes. The default is 30 minutes.

Defaults

A NetFlow aggregation cache export destination is not set.
 The default version format is Version 8.
 The default for **refresh-rate** is 20 packets.
 The default for **timeout-rate** is 30 minutes.

Command Modes

NetFlow aggregation cache configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(24)S	The version , template , refresh-rate , and timeout-rate keywords were added.
12.3(1)	This command was integrated into Cisco IOS Release 12.3(1).

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

export destination

You can configure a maximum of two concurrent destinations per-cache using the **destination** keyword with the **export** command.

Determine the Appropriate Export Version for Your Requirements

NetFlow aggregation caches export data in UDP datagrams using either the Version 9 or Version 8 export format. Table 2 describe how to determine the most appropriate export format for your requirements.

Table 2 When to Select a Particular NetFlow Export Format

Export Format	Select When...
Version 9	<p>You need a flexible and extensible format, which provides the versatility needed for support of new fields and record types.</p> <p>This format accommodates new NetFlow-supported technologies such as Multicast, IPv6 NetFlow, Egress NetFlow, NetFlow Layer 2 and security exports, Multiprotocol Label Switching (MPLS), and Border Gateway Protocol (BGP) next hop.</p> <p>Version 9 export format enables you to use the same version for main and aggregation caches, and the format is extendable, so you can use the same export format with future features</p>
Version 8	<p>You need to export data from aggregation caches or you need to export data from a Catalyst 6000 series switch with a Multilayer Switch Feature Card (MSFC). You do not plan to support new features.</p> <p>Version 8 export format is available only for export from aggregation caches.</p>

NetFlow Version 9 Data Export Format Overview

The NetFlow Version 9 Export Format feature was introduced in Cisco IOS Release 12.0(24)S and was integrated into Cisco IOS Release 12.3(1) and Cisco IOS Release 12.2(18)S.

NetFlow Version 9 is a flexible and extensible means for transferring NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

Third-party business partners who produce applications that provide NetFlow Collection Engine or display services for NetFlow do not need to recompile their applications each time a new NetFlow technology is added. Instead, with the NetFlow v9 Export Format feature, they can use an external data file that documents the known template formats and field types.

NetFlow Version 9 has the following characteristics:

- Record formats are defined by templates.
- Template descriptions are communicated from the router to the NetFlow Collection Engine.
- Flow records are sent from the router to the NetFlow Collection Engine with minimal template information so that the NetFlow Collection Engine can relate the records to the appropriate template.
- Version 9 is independent of the underlying transport (UDP, TCP, SCTP, and so on).

NetFlow Version 9 Template-Based Flow Record Format

The main feature of NetFlow Version 9 export format is that it is *template based*. A template describes a NetFlow record format and the attributes of the fields (such as type and length) within the record. The router assigns each template an ID, which is communicated to the NetFlow Collection Engine along with the template description. The template ID is used for all further communication from the router to the NetFlow Collection Engine.

NetFlow Version 9 Export Flow Records

The basic output of NetFlow is a *flow record*. In NetFlow Version 9 export format, a flow record follows the same sequence of fields that is found in the template definition. The template to which NetFlow flow records belong is determined by the prefixing of the template ID to the group of NetFlow flow records that belong to a template. For a complete discussion of existing NetFlow flow-record formats, see the [NetFlow Services Solutions Guide](#).

NetFlow Version 9 Export Packet

In NetFlow Version 9, an export packet consists of the packet header and flowsets. The packet header identifies the NetFlow Export version. Flowsets are of two types: template flowsets and data flowsets. The template flowset describes the fields that will be in the data flowsets (or flow records). Each data flowset contains the values or statistics of one or more flows that have the same template ID. When the NetFlow Collection Engine receives a template flowset, it stores the flowset and export source address so that subsequent data flowsets that match the flowset ID and source combination are parsed according to the field definitions in the template flowset. Version 9 is supported by NetFlow Collection Engine Version 4.0.

For a complete description of the Version 9 packet headers, template flowsets, and data flowsets, see the [Cisco IOS NetFlow Version 9 Flow-Record Format](#) white paper.

NetFlow Version 8 Data Export Format Overview

The Version 8 data export format is the NetFlow export format used when the router-based NetFlow aggregation feature is enabled on Cisco IOS router platforms. The Version 8 format allows for export datagrams to contain a subset of the Version 5 export data that is based on the configured aggregation cache scheme. For example, a certain subset of the Version 5 export data is exported for the destination prefix aggregation scheme, and a different subset is exported for the source-prefix aggregation scheme.

The Version 8 export format was introduced in Cisco IOS 12.0(3)T for the Cisco IOS NetFlow Aggregation feature. An additional six aggregation schemes that also use Version 8 format were defined for the NetFlow ToS-Based Router Aggregation feature introduced in Cisco IOS 12.0(15)S and integrated into Cisco IOS Releases 12.2(4)T and 12.2(14)S.

The Version 8 datagram consists of a header with the version number (which is 8) and time stamp information, followed by one or more records corresponding to individual entries in the NetFlow cache.

[Table 3](#) lists the NetFlow Version 8 export packet header field names and descriptions.

Table 3 NetFlow Version 8 Export Packet Header Field Names and Descriptions

Field Name	Description
Version	Flow export format version number. In this case 8.
Count	Number of export records in the datagram.
System Uptime	Number of milliseconds since the router last booted.
UNIX Seconds	Number of seconds since 0000 UTC 1970.
UNIX NanoSeconds	Number of residual nanoseconds since 0000 UTC 1970.
Flow Sequence Number	Sequence counter of total flows sent for this export stream.
Engine Type	The type of switching engine. RP = 0 and LC = 1.
Engine ID	Slot number of the NetFlow engine.
Aggregation	Type of aggregation scheme being used.
Agg Version	Aggregation subformat version number. The current value is 2.

Table 3 NetFlow Version 8 Export Packet Header Field Names and Descriptions (continued)

Field Name	Description
Sampling Interval	Interval value used if Sampled NetFlow is configured.
Reserved	Zero field.

For version 8 data exports, the maximum number of aggregated flow records and the maximum size in bytes of each UDP datagram are shown in [Table 4](#).

Table 4 NetFlow Version 8 Aggregation Scheme, Number of Flow Records and UDP Packet Size

Aggregation Scheme	Maximum Number of Flow Records	UDP Packet Size
BGP Autonomous System	51	1456 bytes
Destination Prefix	44	1436 bytes
Prefix	35	1428 bytes
Protocol Port	51	1456 bytes
Source Prefix	44	1436 bytes

Examples

The following example shows how to configure two export destinations for a NetFlow accounting protocol-port aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# export destination 10.41.41.1 9992
Router(config-flow-cache)# export destination 172.16.89.1 9992
Router(config-flow-cache)# enabled
```

The following example shows how to configure the Version 9 template refresh-rate and timeout-rate parameters for a NetFlow accounting protocol-port aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# version 9
Router(config-flow-cache)# export template refresh-rate 100
Router(config-flow-cache)# export template timeout-rate 120
Router(config-flow-cache)# enabled
```

Related Commands

Command	Description
cache	Defines operational parameters for NetFlow accounting aggregation caches.
enabled (aggregation cache)	Enables a NetFlow accounting aggregation cache.
ip flow-aggregation cache	Enables NetFlow accounting aggregation cache schemes.
mask (IPv4)	Specifies the source or destination prefix mask for a NetFlow accounting prefix aggregation cache.
show ip cache flow aggregation	Displays the NetFlow accounting aggregation cache statistics.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.

Command	Description
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

export map

To associate an export map with a VPN Routing and Forwarding (VRF) instance, use the **export map** command in VRF configuration mode.

export map *route-map*

Syntax Description	<i>route-map</i>	Specifies the route map to be used as an export map.
---------------------------	------------------	--

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	IP VPN Routing/Forwarding configuration mode
----------------------	--

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines The **export map** command is used to associate a route map with the specified VRF. The export map is used to filter routes that are eligible for export out of a VRF, based on the route target extended community attributes of the route. Only one export route map can be configured for a VRF.

An export route map can be used when an application requires finer control over the routes that are exported out of a VRF than the control that is provided by import and export extended communities configured for the importing and exporting VRFs.

Examples In the following example, an export is configured under the VRF and an access list and route map are configured to specify which prefixes are exported:

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 1:1
Router(config-vrf)# export map BLUE
Router(config-vrf)# route-target import 2:1
Router(config-vrf)# exit
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)# route-map BLUE permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set extcommunity rt 2:1
Router(config-route-map)# end
```

Related Commands	Command	Description
	import map	Configures an import route map for a VRF.
	ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
	ip vrf	Configures a VRF routing table.

Command	Description
route-target	Creates a route-target extended community for a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

extended-port

To associate the currently selected extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interface with a particular external interface on the remotely controlled ATM switch, use the **extended-port** command in interface configuration mode.

```
extended-port ctrl-if { bpx bpx-port-number | descriptor vsi-descriptor | vsi vsi-port-number }
```

Syntax Description

<i>ctrl-if</i>	Identifies the ATM interface used to control the remote ATM switch. You must configure Virtual Switch Interface (VSI) on this interface using the label-control-protocol interface configuration command.
bpx <i>bpx-port-number</i>	Specifies the associated Cisco BPX interface using the native BPX syntax. <i>slot.port</i> [<i>virtual port</i>] You can use this form of the command only when the controlled switch is a Cisco BPX switch.
descriptor <i>vsi-descriptor</i>	Specifies the associated port by its VSI physical descriptor. The <i>vsi-descriptor</i> string must match the corresponding VSI physical descriptor.
vsi <i>vsi-port-number</i>	Specifies the associated port by its VSI port number. The <i>vsi-port-number</i> string must match the corresponding VSI physical port number.

Defaults

Extended MPLS ATM interfaces are not associated.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

The **extended-port** interface configuration command associates an XTagATM interface with a particular external interface on the remotely controlled ATM switch. The three alternate forms of the command permit the external interface on the controlled ATM switch to be specified in three different ways.

Examples

The following example shows how to associate an extended MPLS ATM interface and bind it to BPX port 2.3:

```
ATM(config)# interface XTagATM23
ATM(config-if)# extended-port atm0/0 bpx 2.3
```

The following example shows how to associate an extended MPLS ATM interface and bind it to port 2.4:

```
ATM(config)# interface XTagATM24
ATM(config-if)# extended-port atm0/0 descriptor 0.2.4.0
```

The following example shows how to associate an extended MPLS ATM interface and binds it to port 1622:

```
ATM(config)# interface XTagATM1622
ATM(config-if)# extended-port atm0/0 vsi 0x00010614
```

Related Commands

Command	Description
interface XTagATM	Enters interface configuration mode for an extended MPLS ATM (XTagATM) interface.
show controller vsi status	Displays a summary of each VSI-controlled interface.

holding-time

To specify the holding time value for the MPS-p7 variable of a Multiprotocol over ATM server (MPS), use the **holding-time** command in MPS configuration mode. To revert to the default value, use the **no** form of this command.

holding-time *seconds*

no holding-time *seconds*

Syntax Description	<i>seconds</i>	Specifies the holding time value in seconds. The default is 1200 seconds.
---------------------------	----------------	---

Defaults	The default holding time is 1200 seconds (20 minutes).
-----------------	--

Command Modes	MPS configuration
----------------------	-------------------

Command History	Release	Modification
	11.3(3a)WA4(5)	This command was introduced.

Examples	The following example shows how to set the holding time to 600 seconds (10 minutes): <pre>holding-time 600</pre>
-----------------	---

import map

To configure an import route map for a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **import map** command in VRF configuration submode.

import map *route-map*

Syntax Description

<i>route-map</i>	Specifies the route map to be used as an import route map for the VRF.
------------------	--

Defaults

No import route map is configured for a VRF.

Command Modes

VRF configuration submode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use an import route map when an application requires finer control over the routes imported into a VRF than provided by the import and export extended communities configured for the importing and exporting VRF.

The **import map** command associates a route map with the specified VRF. You can use a route map to filter routes that are eligible for import into a VRF, based on the route target extended community attributes of the route. The route map might deny access to selected routes from a community that is on the import list.

The **import map** command does not replace the need for a route-target import in the VRF configuration. You use the **import map** command to further filter prefixes that match a route-target import statement in that VRF.

Examples

The following example shows how to configure an import route map for a VRF:

```
Router(config)# ip vrf vrf_blue
Router(config-vrf)# import map blue_import_map
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
route-target	Creates a route-target extended community for a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

index

To insert or modify a path entry at a specific index, use the **index** command in IP explicit path configuration mode. To remove the path entry at the specified index, use the **no** form of this command.

index *index command*

no index *index*

Syntax Description

<i>index</i>	Index number at which the path entry will be inserted or modified. Valid values are from 0 to 65534.
<i>command</i>	An IP explicit path configuration command that creates or modifies a path entry. (Currently you can use only the next-address command.)

Defaults

This command is disabled by default.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following example shows how to insert the next address at index 6:

```
Router(cfg-ip-expl-path)# index 6 next-address 3.3.29.3
```

```
Explicit Path identifier 6:
 6: next-address 3.3.29.3
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number. Commands might be renumbered as a result.
interface fastethernet	Enters the command mode for IP explicit paths and creates or modifies the specified path.
list	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

interface xtagatm

To create an extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interface, use the **interface xtagatm** command in global configuration mode.

interface xtagatm *interface-number*

Syntax Description	<i>interface-number</i>	The interface number.
--------------------	-------------------------	-----------------------

Defaults XTagATM interfaces are not created.No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.2(4)T	This command was updated to reflect the MPLS IETF terminology.

Usage Guidelines XTagATM interfaces are virtual interfaces that are created on reference-like tunnel interfaces. An XTagATM interface is created the first time the **interface xtagatm** command is issued for a particular interface number. These interfaces are similar to ATM interfaces, except that the former only supports LC-ATM encapsulation.

Examples The following example shows how to create an XTagATM interface with interface number 62:

```
Router(config)# interface xtagatm62
```

Related Commands	Command	Description
	extended-port	Associates the currently selected extended XTagATM interface with a remotely controlled switch.

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.
<i>threshold</i>	(Optional) Maximum number of invalidation requests considered to be quiet.

Defaults

minimum: 2 seconds

maximum: 5 seconds, and 3 seconds with no more than zero invalidation requests

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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
ip route-cache	Configures the high-speed switching caches for IP routing.

ip cef

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

```
ip cef [distributed] [accounting type | load-sharing algorithm algorithm | table type | traffic-statistics]
```

```
no ip cef [distributed] [accounting type | load-sharing algorithm algorithm | table type | traffic-statistics]
```

Syntax Description	
distributed	(Optional) Enables distributed CEF (dCEF) operation. Distributes CEF information to line cards. Line cards perform express forwarding.
accounting <i>type</i>	(Optional) Enables CEF accounting. The options for the <i>type</i> argument are as follows: <ul style="list-style-type: none"> • non-recursive—Enables accounting for traffic through non-recursive prefixes. • per-prefix—Enables per prefix accounting. • prefix-length—Enables prefix length accounting.
load-sharing algorithm <i>algorithm</i>	(Optional) Enables load sharing. The options for the <i>algorithm</i> argument are as follow: <ul style="list-style-type: none"> • original—Selects the original algorithm. • tunnel—Selects the algorithm for use in tunnel-only environments. • universal—Selects the algorithm for use in most environments.
table <i>type</i>	(Optional) Sets CEF forwarding table characteristics. The options for the <i>type</i> argument are as follows: <ul style="list-style-type: none"> • adjacency-prefix override—Sets adjacency prefixes to override other Forwarding Information Base (FIB) entries. • consistency-check—Sets consistency checking characteristics. • event-log—Sets table log characteristics. • resolution-timer—Sets background resolution timer. Valid entries are from 0 to 30 seconds. <p>Note Set timer to 0 for automatic exponential back-off scheme.</p>
traffic-statistics	(Optional) Enables the collection of traffic statistics.

Defaults

CEF is disabled by default, excluding these platforms:

- CEF is enabled on the Cisco 7100 series router.
- CEF is enabled on the Cisco 7200 series router.
- CEF is enabled on the Cisco 7500 series Internet router.

- Distributed CEF is enabled on the Cisco 6500 series router.
- Distributed CEF is enabled on the Cisco 12000 series Internet router.

Command Modes

Global configuration

Command History

Release	Modification
11.1 CC	This command was introduced.
12.2	The default for the ip cef command on 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.

Usage Guidelines

The **ip cef** command is not available on the Cisco 12000 series because that router series operates only in dCEF mode.

CEF is advanced Layer 3 IP switching technology. CEF 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 CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are fast switched. Logging disables CEF.

Use the **ip cef** command to control whether voice is switched on the router.

Examples

The following example shows how to enable standard CEF operation:

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

The following example shows how to enable dCEF operation:

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

The following example shows IP CEF configured for load sharing using the original algorithm:

```
Router(config)# ip cef load-sharing algorithm original
```

Related Commands

Command	Description
ip cache-route	Controls the use of high-speed switching caches for IP routing.

ip cef accounting

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

```
ip cef accounting {[non-recursive] [per-prefix] [prefix-length]}
```

```
no ip cef accounting {[non-recursive] [per-prefix] [prefix-length]}
```

Specific CEF Accounting Information Through Interface Configuration Mode

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

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

Syntax Description

non-recursive	Enables accounting through nonrecursive prefixes. This keyword is optional when used in global configuration mode.
per-prefix	(Optional) Enables the collection of the number of packets and bytes express forwarded to a destination (or prefix).
prefix-length	(Optional) Enables accounting through prefix length.
external	Counts input traffic in the nonrecursive external bin.
internal	Counts input traffic in the nonrecursive internal bin.

Defaults

Accounting is disabled by default.

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
11.2 GS	This command was introduced.
11.1 CC	Multiple platform support was added.
11.1 CC	The prefix-length keyword was added.
12.2(2)T	The ip cef accounting non-recursive command in interface configuration mode was added.

Usage Guidelines

You might want to collect statistics to better understand CEF patterns in your network.

When you enable network accounting for CEF from global configuration mode, accounting information is collected at the Route Processor (RP) when CEF mode is enabled and at the line cards when distributed CEF (dCEF) 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 the collection of packets and bytes to be express forwarded 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.

Examples

The following example shows how to enable the collection of CEF accounting information:

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

Related Commands

Command	Description
show ip cef	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 (CEF) 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*

Syntax Description	<i>kbps</i>	Kilobytes of line card memory allocated. Range is 0 to 12800.
---------------------------	-------------	---

Defaults	Default IPC memory allocation is 25 messages. However, this value is dependant on the switching platform.
-----------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(2)T	This command was introduced.

Usage Guidelines	<p>This command is available only on distributed switching platforms.</p> <p>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 CEF routing update messages. The memory pool reduces the transient memory requirements on the RP.</p> <p>To display and monitor the current size of the CEF message queues, use the show cef linecard command. Also, the peak size is recorded and displayed when you use the detail keyword.</p>
-------------------------	--

Examples	<p>The following example shows how to configure the CEF line card memory queue to 128000 kilobytes per second:</p> <pre>Router(config)# ip cef linecard ipc memory 128000</pre>
-----------------	---

Related Commands	Command	Description
	show cef linecard	Displays detailed CEF information for the specified line card.

ip cef load-sharing algorithm

To select a Cisco Express Forwarding (CEF) 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*]}

no ip cef load-sharing algorithm { **original** | **tunnel** [*id*] | **universal** [*id*]}

Syntax Description

original	Sets the load balancing algorithm to the original based on a source and destination hash.
tunnel	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.
universal	Sets the load balancing algorithm to the universal algorithm that uses a source and destination, and ID hash.
<i>id</i>	(Optional) Fixed identifier.

Defaults

The universal load sharing algorithm is selected.

Command Modes

Global configuration

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.

Usage Guidelines

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

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

Examples

The following example shows how to enable the CEF load sharing algorithm for universal environments:

```
Router(config)# ip cef load-sharing algorithm universal 1
```

Related Commands

Command	Description
debug ip cef hash	Records CEF load sharing hash algorithm events
ip load-sharing	Enables load balancing.

ip cef table adjacency-prefix

To modify how Cisco Express Forwarding (CEF) adjacency prefixes are managed, use the **ip cef table adjacency-prefix** command in global configuration mode. To disable CEF 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

override	Enables Cisco Express Forwarding (CEF) adjacency prefixes to override static host glean routes.
validate	Enables the periodic validation of Cisco Express Forwarding (CEF) adjacency prefixes.

Defaults

All CEF adjacency prefix management is disabled by default.

Command Modes

Global configuration

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 validate keyword was added.
12.1(19.02)E	The default behavior for ip cef table adjacency-prefix override was changed to disabled
12.3(04)XG	
12.3(04)XK	
12.3(06.01)PI03	

Usage Guidelines

When CEF 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 CEF, which in turn creates a corresponding host route entry in the FIB table. This entry is called an adjacency prefix.

override

If the CEF 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 CEF 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 CEF table adjacency prefix override:

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

validate

The following example shows how to enable CEF table adjacency prefix validation:

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

ip cef table adjacency-prefix override

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

To enable Cisco Express Forwarding (CEF) table consistency checker types and parameters, 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]
```

Specific to Suppress Errors During Route Updates

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

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

Syntax Description

type	(Optional) Type of consistency check to configure.
lc-detect	(Optional) Line card detects missing prefix. Confirmed by Route Processor (RP).
scan-lc	(Optional) Passive scan check of tables on line card.
scan-rib	(Optional) Passive scan check of tables on RP against Routing Information Base (RIB).
scan-rp	(Optional) Passive scan check of tables on RP.
count <i>count-number</i>	(Optional) Maximum number of prefixes to check per scan. Range is from 1 to 225.
period <i>seconds</i>	(Optional) Period between scans. Range is from 30 to 3600 seconds.
settle-time <i>seconds</i>	(Optional) Time elapsed during which updates for a candidate prefix are ignored as inconsistencies. Range is from 1 to 3600 seconds.

Defaults

All consistency checkers are disabled by default.

Command Modes

Global configuration

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.

Usage Guidelines

This command configures CEF consistency checkers and parameters for the following detection mechanism types:

Detection Mechanism	Operates On	Description
Lc-detect	Line Card	Operates on the line card by retrieving IP prefixes found missing from its forwarding information base (FIB) table. If IP prefixes are missing, the line card can not forward packets for these addresses. Lc-detect will then send IP prefixes to the RP for confirmation. If the RP detects that it has the relevant entry, an inconsistency is detected and an error message will be displayed. Also, the RP will send a signal back to the line card confirming that the IP prefix is an inconsistency.
Scan-lc	Line Card	Operates on the line card by looking through the FIB table for a configurable time period and sending the next <i>n</i> prefixes to the RP. The RP does an exact lookup. If it finds the prefix missing, the RP reports an inconsistency. Finally, the RP sends a signal back to the line card for confirmation.
Scan-rp	Route Processor	Operates on the RP (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. The line card does an exact lookup. If it finds the prefix missing, the line card reports an inconsistency and finally signals the RP for confirmation.
Scan-rib	Route Processor	Operates on all RPs (even nondistributed), and scans the RIB to ensure that prefix entries are present in the RP FIB table.

Examples

The following example shows how to enable the CEF consistency checkers:

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

Related Commands

Command	Description
clear ip cef inconsistency	Clears CEF inconsistency statistics and records found by the CEF consistency checkers.
debug ip cef	Displays various CEF table query and check events.
show ip cef inconsistency	Displays CEF IP prefix inconsistencies.

ip cef table event-log

To control Cisco Express Forwarding (CEF) 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	
<i>size event-number</i>	(Optional) Number of event entries. The range is from 1 to 4294967295.
match	(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.
vrf <i>vrf-name</i>	(Optional) Virtual Private Network (VPN) routing/forwarding instance (VRF) CEF table and VRF name.

Defaults Default size for event log is 10000 entries.

Command Modes Global configuration

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.

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

The CEF event log collects CEF 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 CEF feature.

When the CEF 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 CEF table event log size to 5000 entries:

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

■ ip cef table event-log

Related Commands	Command	Description
	clear ip cef event-log	Clears the CEF event-log buffer.
	ip cef table consistency-check	Enables CEF table consistency checker types and parameters.
	show ip cef events	Displays all recorded CEF FIB and adjacency events.

ip cef table resolution-timer

To change the Cisco Express Forwarding (CEF) 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

Command History	Release	Modification
	12.2(2)T	This command was introduced.

Usage Guidelines The CEF 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 CEF background resolution timer to 3 seconds:

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

ip explicit-path

To enter the command mode for IP explicit paths and create or modify the specified path, use the **ip explicit-path** command in router configuration mode. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path. To disable this feature, use the **no** form of this command.

ip explicit-path {name *word* | identifier *number*} [**enable** | **disable**]

no explicit-path {name *word* | identifier *number*}

Syntax Description

name <i>word</i>	Name of the explicit path.
identifier <i>number</i>	Number of the explicit path. Valid values are from 1 to 65535.
enable	(Optional) Enables the path.
disable	(Optional) Prevents the path from being used for routing while it is being configured.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following example shows how to enter the explicit path command mode for IP explicit paths and creates a path numbered 500:

```
Router(config-router)# ip explicit-path identifier 500
Router(config-ip-expl-path)#
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number. Commands might be renumbered as a result.
index	Inserts or modifies a path entry at a specific index.
ip route vrf	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

ip flow-aggregation cache

To enable NetFlow aggregation cache schemes, use the **ip flow-aggregation cache** command in global configuration mode. To disable NetFlow aggregation cache schemes, use the **no** form of this command.

```
ip flow-aggregation cache { as | as-tos | bgp-nexthop-tos | destination-prefix |
destination-prefix-tos | prefix | prefix-port | prefix-tos | protocol-port | protocol-port-tos |
source-prefix | source-prefix-tos }
```

```
no ip flow-aggregation cache { as | as-tos | bgp-nexthop-tos | destination-prefix |
destination-prefix-tos | prefix | prefix-port | prefix-tos | protocol-port | protocol-port-tos |
source-prefix | source-prefix-tos }
```

Syntax Description		
as		Configures the autonomous system aggregation cache scheme.
as-tos		Configures the autonomous system type of service (ToS) aggregation cache scheme.
bgp-nexthop-tos		Configures the BGP next hop ToS aggregation cache scheme.
destination-prefix		Configures the destination-prefix aggregation cache scheme.
destination-prefix-tos		Configures the destination prefix ToS aggregation cache scheme.
prefix		Configures the prefix aggregation cache scheme.
prefix-port		Configures the prefix port aggregation cache scheme.
prefix-tos		Configures the prefix ToS aggregation cache scheme.
protocol-port		Configures the protocol-port aggregation cache scheme.
protocol-port-tos		Configures the protocol port ToS aggregation cache scheme.
source-prefix		Configures the source-prefix aggregation cache scheme.
source-prefix-tos		Configures the source prefix ToS aggregation cache scheme.

Defaults This command is disabled by default.

Command Modes Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced.
	12.0(15)S	This command was modified to include the ToS aggregation scheme keywords.
	12.2(2)T	This command was modified to enable multiple NetFlow export destinations.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.3(1)	The bgp-nexthop-tos aggregation scheme keyword was added.

Usage Guidelines

The ToS (Type of Service) aggregation cache scheme keywords enable NetFlow aggregation cache schemes that include the ToS byte in their export records. The ToS byte is an 8-bit field in the IP header. The ToS byte specifies the quality of service for a datagram during its transmission through the Internet.

You can enable only one aggregation cache configuration scheme per command line. In source-prefix aggregation mode, only the source mask is configurable. In destination-prefix aggregation mode, only the destination mask is configurable.

To enable aggregation (whether or not an aggregation cache is fully configured), you must enter the **enabled** command in aggregation cache configuration mode. (You can use the **no** form of this command to disable aggregation. The cache configuration remains unchanged even if aggregation is disabled.)

Examples

The following example shows how to configure an autonomous system aggregation scheme:

```
Router(config)# ip flow-aggregation cache as
Router(config-flow-cache)# enabled
```

The following example shows how to configure multiple NetFlow export destinations on an aggregation cache:

```
Router(config)# ip flow-aggregation cache destination-prefix
Router(config-flow-cache)# export destination 10.0.101.254 9991
Router(config-flow-cache)# export destination 10.0.101.254 1999
Router(config-flow-cache)# enabled
```

The following example shows how to enable an autonomous system ToS aggregation scheme:

```
Router(config)# ip flow-aggregation cache as-tos
Router(config-flow-cache)# enabled
```

The following example shows how to enable a BGP next hop aggregation scheme:

```
Router(config)# ip flow-aggregation cache bgp-next-hop-tos
Router(config-flow-cache)# cache timeout active 20
Router(config-flow-cache)# export destination 2.2.2.2 3000
Router(config-flow-cache)# enabled
```

Related Commands

Command	Description
mask destination	Specifies the destination mask.
mask source	Specifies the source mask.
show ip cache flow aggregation	Displays the aggregation cache configuration.
show ip cache verbose flow aggregation	Displays the aggregation cache configuration in detailed format.

ip flow-cache entries

To change the number of entries maintained in the NetFlow cache, use the **ip flow-cache entries** command in global configuration mode. To return to the default number of entries, use the **no** form of this command.

ip flow-cache entries *number*

no ip flow-cache entries

Syntax Description	<i>number</i>	Number of entries to maintain in the NetFlow cache. The valid range is from 1024 to 524288 entries. The default is 65536 (64K).
---------------------------	---------------	---

Defaults	65536 entries (64K)
-----------------	---------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Usage Guidelines Normally the default size of the NetFlow cache will meet your needs. However, you can increase or decrease the number of entries maintained in the cache to meet the needs of your flow traffic rates. For environments with a high amount of flow traffic (such as an internet core router), a larger value such as 131072 (128K) is recommended. To obtain information on your flow traffic, use the **show ip cache flow EXEC** command.

The default is 64K flow cache entries. Each cache entry is approximately 64 bytes of storage. Assuming a cache with the default number of entries, approximately 4 MB of DRAM would be required. Each time a new flow is taken from the free flow queue, the number of free flows is checked. If only a few free flows remain, NetFlow attempts to age 30 flows using an accelerated timeout. If only one free flow remains, NetFlow automatically ages 30 flows regardless of their age. The intent is to ensure free flow entries are always available.



Caution

We recommend that you do not change the NetFlow cache entries. Improper use of this command could cause network problems. To return to the default NetFlow cache entries, use the **no ip flow-cache entries** global configuration command.

Examples

The following example shows how to increase the number of entries in the NetFlow cache to 131,072 (128K):

```
ip flow-cache entries 131072
```

Related Commands

Command	Description
show mpoa client	Displays the routing table cache used to fast switch IP traffic.

ip flow-export

To enable the export of information in NetFlow cache entries, use the **ip flow-export** command in global configuration mode. To disable the export of information, use the **no** form of this command.

```
ip flow-export { destination { ip-address | hostname } udp-port | source { interface-name } | version
{ 1 | [ { 5 | 9 } ] [ origin-as | peer-as ] [ bgp-nexthop ] ] | template { refresh-rate packets |
timeout-rate minutes } [ options { export-stats | refresh-rate packets | sampler | timeout-rate
minutes } ] }
```

```
no ip flow-export { destination ip-address | hostname } udp-port | source | version | template
{ refresh-rate | timeout-rate } [ options { export-stats | refresh-rate | sampler |
timeout-rate } ] }
```

Syntax Description

destination <i>ip-address</i> <i>hostname</i> <i>udp-port</i>	IP address or hostname of the workstation to which you want to send the NetFlow information and the number of the UDP port on which the workstation is listening on for this input.
source { <i>interface-name</i> }	IP address and interface type and number for the source address.
version 1	Specifies that the export datagram uses the Version 1 format. This is the default. The version field occupies the first two bytes of the export record. The number of records stored in the datagram is variable from 1 to 24 for Version 1.
version 5	Specifies that the export packet uses the Version 5 format. The number of records stored in the datagram is variable between 1 and 30 for version 5.
version 9	Specifies that the export packet uses the Version 9 format.
origin-as	(Optional) Specifies that export statistics include the originating autonomous system (AS) for the source and destination.
peer-as	(Optional) Specifies that export statistics include the peer AS for the source and destination.
bgp-nexthop	(Optional) Specifies that export statistics include Border Gateway Protocol (BGP) next-hop related information.
template	Enables the refresh-rate and timeout-rate keywords for configuring Version 9 export templates.
refresh-rate <i>packets</i>	(Optional) Specifies the number of export datagrams that are sent before the options and flow templates are resent. You can specify from 1 to 600 packets. The default is 20 packets. Note This applies to the ip flow-export template refresh-rate packets command.
timeout-rate <i>minutes</i>	(Optional) Specifies the interval (in minutes) that the router will wait after sending the templates (flow and options) before they are sent again. You can specify from 1 to 3600 minutes. The default is 30 minutes. Note This applies to the ip flow-export template timeout-rate minutes command.
options	Enables the export-stats , refresh-rate , sampler and timeout-rate keywords for configuring Version 9 export options.

export-stats	(Optional) Enables the export of statistics including the total number of flows exported and the total number of packets exported.
sampler	(Optional) When Version 9 export is configured, this enables the export of an option containing random-sampler configuration, including the sampler ID, sampling mode and sampling interval for each configured random sampler.
refresh-rate <i>packets</i>	(Optional) Specifies the number of datagrams that are sent before the configured options records are resent. You can specify from 1 to 600 packets. The default is 20 packets. Note This applies to the ip flow-export template options refresh-rate <i>packets</i> command.
timeout-rate <i>minutes</i>	(Optional) Specifies the interval (in minutes) that the router will wait after sending the options records before they are sent again. You can specify from 1 to 3600 minutes. The default is 30 minutes. Note This applies to the ip flow-export template options timeout-rate <i>minutes</i> command.

Defaults

Export of NetFlow information is disabled. When the Export of NetFlow information is enabled, the best source IP address for NetFlow datagrams will be picked automatically. The NetFlow Version 1 export format will be used. AS and BGP nexthop information will not be exported. No additional templates or options will be exported. When version 9 export is enabled, templates and options are resent every 20 export packets or 30 minutes, whichever is sooner.

Command Modes

Global configuration

Command History

Release	Modification
11.1 CA	This command was introduced.
11.1(15)CA	The ip flow-export <i>ip-address udp-port</i> syntax was changed to a hidden command in preparation for deprecating it. The new syntax ip flow-export destination <i>ip-address udp-port</i> was added.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S, and the 9 keyword was added.
12.3(1)	This command was integrated into Cisco IOS Release 12.3(1), and the bgp-nexthop keyword was added.
12.0(26)S	The bgp-nexthop and sampler keywords were added.
12.2(2)T	This command was modified to enable multiple NetFlow export destinations to be used.
12.3(13)	The ip flow-export <i>ip-address udp-port</i> syntax was removed from the Command-Line Interface (CLI).

Usage Guidelines

- [ip flow-export version](#)

- [ip flow-export destination](#)
- [ip flow-export source](#)
- [ip flow-export template options export-stats](#)
- [ip flow-export template options sampler](#)

ip flow-export version

The **ip flow-export version** command supports three export data formats: Version 1, Version 5, and Version 9. Version 1 should only be used when it is the only NetFlow data export format version that is supported by the application that you are using to analyze the exported NetFlow data. Version 5 exports more fields than Version 1. Version 9 is the flexible export format.

The NetFlow **bgp-nexthop** command can be configured when either the Version 5 export format (**ip flow-export version 5 bgp-nexthop**) or the Version 9 export format (**ip flow-export version 9 bgp-nexthop**) is configured.

The following caveats apply to the **bgp-nexthop** command:

- The values for the BGP nexthop IP address are exported to a NetFlow collector only when the Version 9 export format is configured.
- In order for the BGP information to be populated in the main cache you must either have a NetFlow export destination configured or NetFlow aggregation configured.



Note

The AS values for the **peer-as** and the **origin-as** keywords are only captured if you have configured an export destination with the **ip flow-export destination** command.

For more information on the available export data formats, see the “NetFlow Data Format” section in the “Configuring NetFlow Switching” chapter of the *Cisco IOS Switching Services Configuration Guide*. For more information on the Version 9 data format, see the *Cisco IOS NetFlow Version 9 Export Format Feature Guide*.



Caution

Entering the **ip flow-export** or **no ip flow-export** command on the Cisco 12000 Series Internet routers and specifying any format version other than version 1 (in other words, entering the **ip flow-export** or **no ip flow-export** command and specifying either the **version 5** or **version 9** keyword) causes packet forwarding to stop for a few seconds while NetFlow reloads the route processor and line card Cisco Express Forwarding (CEF) tables. To avoid interruption of service to a live network, either apply this command during a change window or include it in the startup-config file to be executed during a router reboot.

ip flow-export destination

If NetFlow is switching a high volume of traffic on your router, the NetFlow cache may contain a large quantity of information. This can make it difficult to interpret the NetFlow statistics when you view them on your router with NetFlow commands such as **show ip cache verbose flow**. It is easier to interpret the NetFlow data when you export it to a network management system that supports the NetFlow data export formats (such as a system running CNS NetFlow Collection Engine (NFC)). CNS NetFlow Collection Engine provides a web-based reporting tool that will help you analyze the statistics captured by NetFlow.

When NetFlow switching is enabled with the **ip route-cache flow** command you can use the **ip flow-export destination** command to configure the router to export the flow cache entries to a destination system (such as a system running CNS NetFlow Collection Engine (NFC)). NetFlow exports the flow cache entries to the destination system when the flows in the cache expire. You can use this command to supply data for applications such as statistical analysis, billing, and security.

The **ip flow-export destination** command can support a maximum of two destination ip-address and udp-port combinations. The most common usage of the multiple-destination feature is to send the NetFlow cache entries to two different destinations for redundancy. Therefore, in most cases the second destination IP address is not the same as the first IP address. The udp-port numbers can be the same when you are configuring two unique destination IP addresses. If you want to configure both instances of the command to use the same destination IP address, you must use unique udp-port numbers. You receive a warning message when you configure the two instances of the command with the same IP address. The warning message you will see is `%Warning: Second destination address is the same as previous address <ip-address>`.

ip flow-export source

After you configure NetFlow data export, use the `ip flow-export source` interface command to specify the interface that NetFlow will use to obtain the source IP address for the NetFlow datagrams that it sends to destination systems, such as a system running CNS NetFlow Collection Engine (NFC). This will over-ride the default behavior of using the IP address of the interface that the datagram is transmitted over as the source IP address for the NetFlow datagrams. Some of the benefits of using a consistent IP source address for the datagrams that NetFlow sends are:

- The source IP address of the datagrams exported by NetFlow is used by the destination system to determine which router the NetFlow data is arriving from. If your network has two or more paths that can be used to send NetFlow datagrams from the router to the destination system, and you do not specify the source interface to obtain the source IP address from, the router will use the IP address of the interface that the datagram is transmitted over as the source IP address of the datagram. In this situation it is possible that the destination system will receive NetFlow datagrams from the same router with different source IP addresses. This will cause the destination system to treat the NetFlow datagrams as if they are being sent from different routers unless you have configured the destination system to aggregate the NetFlow datagrams it receives from all of the possible source IP addresses in the router into a single NetFlow flow.
- It is easier to create and maintain access-lists for permitting NetFlow traffic from known sources and blocking it from unknown sources when you limit the source IP address for NetFlow datagrams to a single IP address for each router that is exporting NetFlow traffic.

ip flow-export template options export-stats

The **ip flow-export template options export-stats** command enables the export of statistics for the total number of exported flows and the total number of exported packets.

**Note**

The **ip flow-export template options export-stats** command requires that the NetFlow Version 9 export format be already configured on the router.

**Note**

The **ip flow-export template options sampler** option is not available for NetFlow aggregation caches. However, the options will be sent to destinations configured under the aggregation cache, if they are configured for the main cache.

ip flow-export template options sampler

When Version 9 export is configured, this enables the export of an option containing random-sampler configuration, including the sampler ID, sampling mode and sampling interval for each configured random sampler.

**Note**

The **ip flow-export template options sampler** command requires that the NetFlow Version 9 export format be already configured on the router.

**Note**

The **ip flow-export template options sampler** option is not available for NetFlow aggregation caches.

NetFlow Data Export of Template Options

The **ip flow-export template options refresh-rate** command enables you to configure how frequently the export-stats and/or sampler options records are sent

**Note**

The **ip flow-export template refresh-rate** command specifies how frequently the options templates will be sent.

Examples.

- [ip flow-export version](#)
- [ip flow-export destination](#)
- [ip flow-export source](#)
- [ip flow-export template options export-stats](#)
- [ip flow-export template](#)
- [ip flow-export template sampler](#)

ip flow-export version

The following example shows how to configure the networking device to use the NetFlow Version 9 format for the exported data and how to include the originating autonomous-system (origin-as) with its corresponding next BGP hop (bgp-nexthop):

```
Router(config)# ip flow-export version 9 origin-as bgp-nexthop
@@@
```

ip flow-export destination

The following example shows how to configure the networking device to export the NetFlow cache entry to a single export destination system:

```
Router(config)# ip flow-export destination 10.42.42.1 9991
```

The following example shows how to configure the networking device to export the NetFlow cache entry to multiple destination systems:

```
Router(config)# ip flow-export destination 10.42.42.1 9991
Router(config)# ip flow-export destination 10.0.101.254 9991
```

The following example shows how to configure the networking device to export the NetFlow cache entry to two different UDP ports on the same destination system:

```
Router(config)# ip flow-export destination 10.42.42.1 9991
Router(config)# ip flow-export destination 10.42.42.1 9992
%Warning: Second destination address is the same as previous address 10.42.42.1
```

ip flow-export source

The following example shows how to configure NetFlow to use a loopback interface as the source interface for NetFlow traffic:

**Caution**

The interface that you configure as the **ip flow-export source** interface must have an IP address configured and it must be up.

```
Router(config)# ip flow-export source loopback0
```

ip flow-export template options export-stats

The following example shows how to configure NetFlow so that the networking device sends the export statistics (total flows and packets exported) as options data:

```
Router(config)# ip flow-export template options export-stats
```

ip flow-export template

The following example shows how to configure NetFlow to send 100 export packets before the templates are resent to the destination host:

```
Router(config)# ip flow-export template refresh-rate 100
```

The following example shows how to configure NetFlow so that the export statistics include the total number of flows exported and the total number of packets exported:

```
Router(config)# ip flow-export template option export-stats
```

ip flow-export template sampler

The following example shows how to configure NetFlow to enable the export of information about NetFlow random samplers:

```
Router(config)# ip flow-export template option sampler
```

**Tip**

You must have a **flow-sampler** map configured before you can configure the sampler keyword for the **ip flow-export template options** command.

Related Commands

Command	Description
debug ip flow export	Enables debugging output for NetFlow data export.
ip route-cache flow	Enables NetFlow switching for IP routing.
show ip flow export	Displays the statistics for the NetFlow data export.

ip flow-export destination

The **ip flow-export destination** command is replaced by the **ip flow-export** command. See the **ip flow-export** command for more information.

ip flow-export source

The **ip flow-export source** command is replaced by the **ip flow-export** command. See the **ip flow-export** command for more information.

ip flow ingress

To configure NetFlow on an interface or subinterface, use the **ip flow ingress** command in interface or subinterface configuration mode. To disable NetFlow on an interface or subinterface, use the **no** form of this command.

ip flow ingress

no ip flow ingress

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Subinterface configuration

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

If you configure the **ip flow ingress** command on a few selected subinterfaces and then configure the **ip route-cache flow** command on the main interface, enabling the main interface will overwrite the **ip flow ingress** command and data collection will start from the main interface as well as all the subinterfaces. In a scenario where you configure the **ip flow ingress** command and then configure the **ip route-cache flow** command on the main interface, you can restore subinterface data collection by using the **no ip route-cache flow** command. This configuration will disable data collection from the main interface and restore data collection to the subinterfaces you originally configured with the **ip flow ingress** command.

Examples

The following example shows how to configure NetFlow on a Fast Ethernet subinterface 6/3.0:

```
Router(config)# interface FastEthernet6/3.0
Router(config-subif)# ip flow ingress
```

Related Commands

Command	Description
ip route-cache flow	Enables NetFlow switching for IP routing.
show ip cache flow	Displays a summary of NetFlow statistics.
show ip interface	Displays the usability status of interfaces configured for IP.