



Configuring Application Visibility and Control for Cisco Flexible Netflow

First published: July 22, 2011

This guide contains information about the Cisco Application Visibility and Control feature. It also provides instructions on how to configure the Cisco Application Visibility and Control feature.



Note

This guide contains basic information for configuring the feature. For information on advanced configurations, see the [“Additional References” section on page 40](#).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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

Contents

- [Prerequisites for Cisco Application Visibility and Control, page 2](#)
- [Restrictions for Cisco Application Visibility and Control, page 2](#)
- [Information About Cisco Application Visibility and Control, page 2](#)
- [How to Configure Cisco Application Visibility and Control, page 6](#)
- [Configuration Examples for Cisco Application Visibility and Control, page 30](#)
- [Information About Cisco NBAR Memory for Cisco Application Visibility and Control, page 33](#)
- [How to Configure Cisco NBAR Memory for Cisco Application Visibility and Control, page 33](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- [Displaying Cisco NBAR Information](#), page 34
- [Information About Cisco Modular QOS \(MQC\)](#), page 35
- [Configuration Examples for Cisco Modular QOS \(MQC\)](#), page 36
- [Additional References](#), page 40
- [Glossary](#), page 42

Prerequisites for Cisco Application Visibility and Control

- You are familiar with the information in *Cisco IOS NetFlow Overview* at http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/ios_netflow_ov.html
- You are familiar with the Modular QOS (MQC) information in the *Applying QoS Features Using the MQC* at http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_mqc.html.
- You are familiar with *Classifying Network Traffic Using NBAR in Cisco IOS XE Software* at http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/clsfy_traffic_nbar_xe.html.
- You are familiar with *Cisco IOS Quality of Service Solutions Command Reference* at http://www.cisco.com/en/US/products/ps11174/prod_command_reference_list.html
- You are familiar with the information in the *Cisco Application Visibility and Control Collection Manager User Guide* at http://www.cisco.com/en/US/products/ps6153/products_user_guide_list.html.
- The Cisco ASR 1000 Series Router is configured for IPv4 routing.



Note

More Cisco IOS Flexible NetFlow information resources are available at the [Additional References](#), page 40.

Restrictions for Cisco Application Visibility and Control

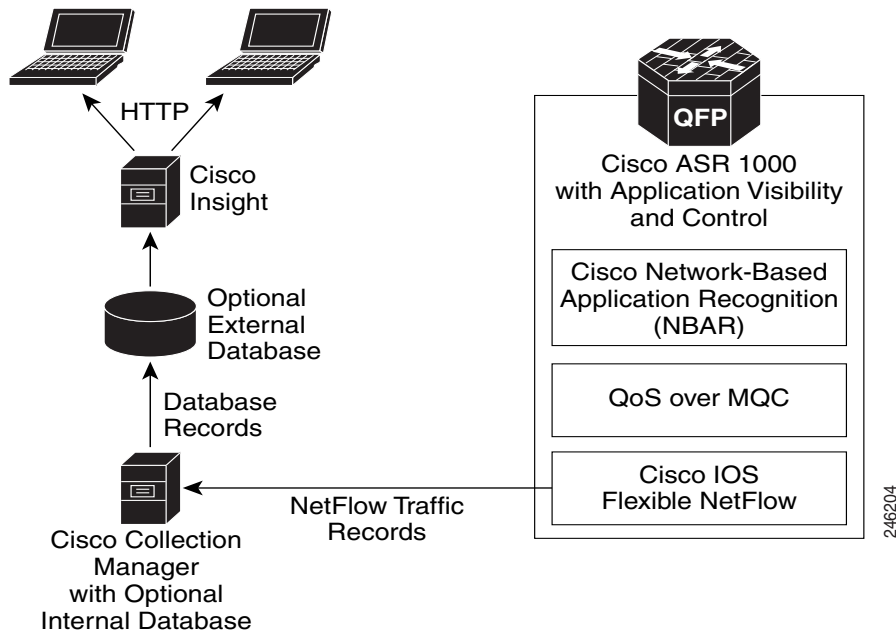
- The Cisco Application Visibility and Control feature supports export in Version 9 format only.

Information About Cisco Application Visibility and Control

- Internal components of the Cisco ASR 1000 Series Router:
 - [Cisco Network-Based Application Recognition](#), page 3
 - [Cisco Modular QOS](#), page 3
 - [Bandwidth Control](#), page 3
 - [Cisco NetFlow v9](#), page 4
 - [Cisco IOS Flexible NetFlow Traffic Records](#), page 4
- External components:
 - [Cisco Collection Manager](#), page 5
 - [Cisco Insight v3](#), page 5

Figure 1-1 illustrates the core components of the Cisco Application Visibility and Control solution.

Figure 1-1 Cisco ASR 1000 Application Visibility and Control Network Components



Cisco Network-Based Application Recognition

Cisco NBAR enables protocol detection for a network. Protocol detection is the process by which the system determines that a particular network flow is from a specific application. This process is performed using various techniques including payload signature matching, behavioral classification or classification based on Layer 7 parameters (sometimes called protocol sub-classification). Upon detection of a flow, a Protocol ID is assigned to it. The Protocol ID is then used by the solution to determine the appropriate actions on packets belonging to that flow.

Cisco Modular QoS

Standard Cisco Modular QoS (MQC) is used for the Cisco ASR 1000 Application Visibility and Control Modular QoS solution. It is used to create the application-aware policy of the solution.

Bandwidth Control

The Cisco Application Visibility and Control solution provides global bandwidth control by using pre-configured application categorization structure. This includes category (for example browsing), sub-category (for example streaming), or an application group (for example, flash-group) or application (for example, YouTube). This control allows service providers to set acceptable bandwidth consumption policies for different traffic classes. Bandwidth priority is provided by using platform policies.



Note

Examples of bandwidth control configuration are provided in [Configuration Examples for Cisco Modular QOS \(MQC\)](#), page 36.

Cisco NetFlow v9

Cisco NetFlow export format Version 9 is a flexible and extensible means for carrying 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.

Cisco IOS Flexible NetFlow Traffic Records

Cisco IOS Flexible NetFlow uses the Cisco ASR 1000 Series Router infrastructure to provide application visibility. It exports data in the form of Flexible NetFlow records. These records are in the NetFlow version 9 format. The two types of Flexible NetFlow records are Usage Records and Transaction Records.

[Figure 1-2](#) illustrates the packet fields used by the Transaction Records and Usage Records. The red fields are the key fields.

Figure 1-2 Packet Fields of Transaction Records and Usage Records

Source port	Last timestamp
Destination IP	Packets counter
Destination Port	Bytes counter
IP Protocol	New-Flows counter
Application ID	Total Seconds counter
Connection Initiator	IP Version
First timestamp	Input VRF ID
Last timestamp	
Packets counter	Global Usage Record
Bytes counter	Attached Interface (input/output)
Bundle/Flow ID	Direction
Flow close mode	Other interface (input/output)
Sampler ID	First timestamp
IPv6 Source Address	Last timestamp
IPv6 Destination Address	Packets counter
IP Version	Bytes counter
Input VRF ID	New-Flows counter
	Total Seconds counter
	IP Version
	Input VRF ID

246231

The following sections describe the two types of Flexible NetFlow records:

- [Usage Records, page 5](#)
- [Transaction Records, page 5](#)

Usage Records

Usage Records are records of the different type of applications that run on a specific interface. The operator can use Usage Records to monitor how much bandwidth the different applications use. The Usage Records can show this application usage over a specific time period, the peak and average usages, and usage for a specific application type. Usage Records perform periodic aggregation of the category information for the interface. (For example, export information for peer-to-peer traffic or email usage).

Transaction Records

A transaction is a set of logical exchanges between endpoints. There is normally one transaction within a flow. The Transaction Record monitors the traffic at transaction levels. These records provide a detailed analysis of the traffic flows. Transaction Records are bound to the input and output directions of the network side interfaces. These Transaction Records allow the system to capture each unidirectional flow once.

External Components

These solution components exist on platforms that are physically separate from the Cisco ASR 1000 Series Router.

Cisco Collection Manager

The Cisco Collection Manager is a set of software modules that runs on a server. It receives and processes Flexible NetFlow records. The processed records are stored in the Cisco Collection Manager database. The database can be either bundled or external.

The Cisco Collection Manager is covered in detail in the *Cisco Application Visibility and Control Collection Manager User Guide*.

Cisco Insight v3

Cisco Insight v3 is reporting platform software. It processes the formatted data from the Collection Manager database. It presents customized reports, charts, and statistics about the traffic. Cisco Insight v3 is a Web 2.0 application that is accessed with a browser.

Cisco Insight v3 is covered in detail in the *Cisco Insight v3 User Guide*.

How to Configure Cisco Application Visibility and Control

- [New Commands and Keywords, page 6](#)
- [Configuring the Flow Exporter, page 7](#) (required)
- [Creating Usage Records and Monitoring, page 10](#)
- [Creating Transaction Records and Monitoring, page 20](#)

New Commands and Keywords

The following commands and keywords are either new and introduced with the Cisco Application Visibility and Control feature or related to the feature.

Cisco NetFlow commands for Cisco Application Visibility and Control

These commands are Cisco NetFlow commands. Documentation for these commands can be found in the *Cisco IOS NetFlow Command Reference*
http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf_book.html.

- The **granularity connection** command
- The **collect connection** command
- The **match connection transaction-id** command
- The **collect connection initiator** command
- The **collect connection new-connections** command
- The **collect connection sum-duration** command
- The **collect flow end-reason** command
- The **account-on-resolution** keyword for the **match application name** command
- The **event transaction-end** keyword for the **cache timeout** command

Cisco NBAR and Cisco QoS Commands for Cisco Application Visibility and Control

These commands are Cisco NBAR and Cisco QoS commands. Documentation for these commands can be found in the *Cisco IOS Quality of Service Solutions Command Reference* at
http://www.cisco.com/en/US/products/ps11174/prod_command_reference_list.html.

- **match protocol attribute category**
- **match protocol attribute sub-category**
- **match protocol attribute application-group**
- **match protocol attribute encrypted**
- **match protocol attribute tunnel**
- **show ip nbar protocol-attribute**
- **show ip nbar attribute**
- **show ip nbar resources flow**
- **ip nbar resource flow max-sessions**

Configuring the Flow Exporter

Perform the following tasks to configure Flexible NetFlow and bind Flexible NetFlow to an interface:

- [Creating the Flow Exporter, page 7](#) (required)
- [Verifying the Flow Exporter Configuration, page 9](#) (optional)

Creating the Flow Exporter







To configure the flow exporter, perform the following required task.



SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **destination** *ip-address* [**vrf** *vrf-name*]
5. **template data timeout** *seconds*
6. **option interface-table timeout** *seconds*
7. **option sampler-table timeout** *seconds*
8. **option application-table timeout** *seconds*
9. **option application-attributes timeout** *seconds*
10. **option vrf-table timeout** *seconds*
11. **source** *interface-type interface-number*
12. **transport udp** *udp-port*
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	flow exporter <i>exporter-name</i> Example: Router(config)# flow exporter EXPORTER-1	Creates the flow exporter and enters Cisco Flexible NetFlow flow exporter configuration mode. <ul style="list-style-type: none">• This command also allows you to modify an existing flow exporter.

	Command or Action	Purpose
Step 4	<p>destination <i>ip-address</i> [vrf <i>vrf-name</i>]</p> <p>Example: Router(config-flow-exporter)# destination 172.16.10.2</p>	<p>Specifies the IP address or hostname of the destination system for the exporter. Use the optional vrf keyword if the export interface is inside an VRF.</p> <p> Note Exporting from a management interface inside VRF Mgmt-intf is not supported.</p>
Step 5	<p>template data timeout <i>seconds</i></p> <p>Example: Router(config-flow-exporter)# template data timeout 30</p>	<p>Configures the resending of templates based on a timeout.</p>
Step 6	<p>option interface-table timeout <i>seconds</i></p> <p>Example: Router(config-flow-exporter)# option inter- face-table timeout 30</p>	<p>Configures parameters for the exporter. The default timeout is 600s.</p> <p> Note You can configure all the option commands concurrently.</p>
Step 7	<p>option sampler-table timeout <i>seconds</i></p> <p>Example: Router(config-flow-exporter)# option sam- pler-table timeout 30</p>	<p>Configures parameters for the exporter.</p> <p> Note You can configure all the option commands concurrently.</p>
Step 8	<p>option application-table timeout <i>seconds</i></p> <p>Example: option application-table timeout 30</p>	<p>Configures parameters for the exporter.</p> <p> Note You can configure all the option commands concurrently.</p>
Step 9	<p>option application-attributes timeout <i>seconds</i></p> <p>Example: option application-attributes timeout 30</p>	<p>Configures parameters for the exporter.</p> <p> Note You can configure all the option commands concurrently.</p>
Step 10	<p>option vrf-table timeout <i>seconds</i></p> <p>Example: option application-attributes timeout 30</p>	<p>Configures parameters for the exporter.</p> <p> Note You can configure all the option commands concurrently.</p>

	Command or Action	Purpose
Step 11	<p>source <i>interface-type interface-number</i></p> <p>Example:</p> <pre>Router(config-flow-exporter)# source loopback 0</pre> <p>or</p> <pre>Router(config-flow-exporter)# source interface GigabitEthernet0/1/0</pre>	<p>(Optional) Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams.</p> <p> Note The source interface should be a management interface.</p> <p> Note The use of loopback as a source is a Cisco best practice but not required.</p>
Step 12	<p>transport udp 2055</p> <p>Example:</p> <pre>Router(config-flow-exporter)# transport udp 2055</pre>	Specifies UDP port 2055 for the Cisco Collection Manager to listen for exported datagrams.
Step 13	<p>end</p> <p>Example:</p> <pre>Router(config-flow-exporter)# end</pre>	Exits flow exporter configuration mode and returns to privileged EXEC mode.

Verifying the Flow Exporter Configuration

To verify the configuration commands that you entered, perform the following optional task.

SUMMARY STEPS

1. **enable**
2. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

Step 1 **enable**

The **enable** command enters privileged EXEC mode (enter the password if prompted).

```
Router> enable
Router#
```

Step 2 **show running-config flow exporter** *exporter-name*

The **show running-config flow exporter** command shows the configuration commands of the flow exporter that you specify.

```
Router# show running-config flow exporter EXPORTER-1
Building configuration...

Current configuration:
!
flow exporter EXPORTER-1
```

```

destination 10.24.88.60
source GigabitEthernet0/0/1
transport udp 2055
option interface-table timeout 300
option sampler-table timeout 300
option application-table timeout 300
!
end

```

Creating Usage Records and Monitoring

This section is made up of the following procedures

- [Configuring Usage Records, page 10](#) (required)
- [Verifying Usage Records, page 16](#) (optional)
- [Configuring Usage Monitoring, page 17](#) (required)
- [Verifying Usage Monitoring, page 19](#) (optional)

Configuring Usage Records

Both input and output usage records are required to capture in both directions. To configure usage records, perform the following tasks:

- [Configuring an Input Usage Record, page 10](#) (required)
- [Configuring an Output Usage Record, page 13](#) (required)

Configuring an Input Usage Record

To configure an input usage record, perform the following required task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *flow-record-name*
4. **match flow direction**
5. **match interface input**
6. **match ipv4 version**
7. **match ipv6 version**
8. **match application name account-on-resolution**
9. **collect interface output**
10. **collect flow direction**
11. **collect timestamp sys-uptime first**
12. **collect timestamp sys-uptime last**
13. **collect counter bytes long**
14. **collect counter packets**

15. collect connection new-connections
16. collect connection sum-duration
17. collect routing vrf input
18. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	flow record <i>flow-record-name</i> Example: Router(config)# flow record my-input-usage-monitor	Creates a flow record and enters flow record configuration mode.
Step 4	match interface input Example: Router(config-flow-record)# match interface input	Configures the input interface for the packet as a key field for the flow record. input —Traffic arrives on the Cisco router's input interface.
Step 5	match flow direction Example: Router(config-flow-record)# match flow direction	Configures the direction of the flow record as a key field. The direction is either input or output.
Step 6	match ipv4 version Example: Router(config-flow-record)# match ipv4 version	(Optional) For IPv4 networks, configures the IPv4 address version type as a key field. The direction is either input or output.
Step 7	match ipv6 version Example: Router(config-flow-record)# match ipv6 version	(Optional) For IPv6 networks, configures the IPv6 address version type as a key field. The direction is either input or output.
Step 8	match application name account-on-resolution Example: Router(config-flow-record)# match application name account-on-resolution	Configures the use of application name as a key field for a Cisco Flexible NetFlow flow record. <ul style="list-style-type: none"> • account-on-resolution—Provides an accurate accounting for the beginning of the flow. The system temporarily stores the record data until the application is resolved and combines the data with the created flow after resolution.

	Command or Action	Purpose
Step 9	<p>collect interface output</p> <p>Example: <pre>Router(config-flow-record)# collect interface output</pre></p>	Configures the output interface as a non-key field for a Cisco Flexible NetFlow flow record and enables collecting the output interface fields from the flows for the flow record.
Step 10	<p>collect flow direction</p> <p>Example: <pre>Router(config-flow-record)# collect flow direc- tion</pre></p>	Configures the flow direction as a non-key field for a Cisco Flexible NetFlow flow record.
Step 11	<p>collect timestamp sys-uptime first</p> <p>Example: <pre>Router(config-flow-record)# collect timestamp sys-uptime first</pre></p>	<p>Configures the system uptime of the first seen packet in a flow as a nonkey field for a Cisco Flexible NetFlow flow record.</p> <ul style="list-style-type: none"> first—Configures the system uptime for the time the first packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the first packet was seen from the flows.
Step 12	<p>collect timestamp sys-uptime last</p> <p>Example: <pre>Router(config-flow-record)# collect timestamp sys-uptime last</pre></p>	<p>Configures the system uptime of the last seen packet in a flow as a nonkey field for a Cisco Flexible NetFlow flow record.</p> <ul style="list-style-type: none"> last—Configures the system uptime for the time the last packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the most recent packet was seen from the flows.
Step 13	<p>collect counter bytes long</p> <p>Example: <pre>Router(config-flow-record)# collect counter bytes long</pre></p>	<p>Configures the number of bytes in a flow as a nonkey field for a Cisco Flexible NetFlow flow record.</p> <ul style="list-style-type: none"> bytes—Configures the number of bytes seen in a flow as a nonkey field and enables collecting the total number of bytes from the flow. long—Enables collecting the total number of bytes or packets from the flow by using a 64-bit counter rather than a 32-bit counter.
Step 14	<p>collect counter packets</p> <p>Example: <pre>Router(config-flow-record)# collect counter packets</pre></p>	<p>Configures the number of packets in a flow as a nonkey field for a Cisco Flexible NetFlow flow record.</p> <ul style="list-style-type: none"> packets—Configures the number of packets seen in a flow as a nonkey field and enables collecting the total number of packets from the flow.
Step 15	<p>collect connection new-connections</p> <p>Example: <pre>Router(config-flow-record)# collect connection new-connections</pre></p>	Counts the number of TCP or UDP connections which were opened during the observation period. The observation period may be specified by the flow start and end timestamps.

	Command or Action	Purpose
Step 16	collect connection sum-duration Example: Router(config-flow-record)# collect connection sum-duration	Aggregates the total time, in seconds, for all the TCP or UDP connections, which were in use during the observation period. For example, if there are five concurrent connections each for 10 seconds, the value would be 50 seconds.
Step 17	collect routing vrf input Example: Router(config-flow-record)# collect routing vrf input	Configures the routing VRF input as a nonkey field for a Cisco Flexible NetFlow flow record.
Step 18	end Example: Router(config-flow-record)# end	Exits flow record configuration mode and returns to privileged EXEC mode.

Configuring an Output Usage Record

To configure an output usage record, perform the following required task.



Note

The **account-on-resolution** keyword for the **match application name** command is introduced as part of the Cisco Application Visibility and Control feature. The **connection new-transactions** and **connection sum-duration** keywords for the **collect** command are introduced as part of the Cisco Application Visibility and Control feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *flow-record-name*
4. **match interface output**
5. **match flow direction**
6. **match application name account-on-resolution**
7. **collect interface input**
8. **collect routing vrf input**
9. **collect flow direction**
10. **collect timestamp sys-uptime first**
11. **collect timestamp sys-uptime last**
12. **collect counter bytes long**
13. **collect counter packets**
14. **collect connection new-connections**
15. **collect connection sum-duration**
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>flow record <i>flow-record-name</i></p> <p>Example: Router(config)# flow record my-output-us-age-monitor</p>	<p>Creates a flow record and enters flow record configuration mode.</p>
Step 4	<p>match interface output</p> <p>Example: Router(config-flow-record)# match interface output</p>	<p>Configures the output interface for the packet as a key field for the flow record.</p> <ul style="list-style-type: none"> output—Traffic arrives on the Cisco router's output interface.
Step 5	<p>match flow direction</p> <p>Example: Router(config-flow-record)# match flow direction</p>	<p>Configures the direction of the flow record as a key field. The direction is either input or output.</p>
Step 6	<p>match application name account-on-resolution</p> <p>Example: Router(config-flow-record)# match application name account-on-resolution</p>	<p>Configures the use of application name as a key field for a Cisco Flexible NetFlow flow record.</p> <ul style="list-style-type: none"> account-on-resolution—Provides an accurate accounting for the beginning of the flow. The system temporarily stores the record data until the application is resolved and combines the data with the created flow after resolution.
Step 7	<p>collect interface input</p> <p>Example: Router(config-flow-record)# collect interface input</p>	<p>Configures the input interface as a non-key field for a Cisco Flexible NetFlow flow record and enables collecting the input interface fields from the flows for the flow record.</p>
Step 8	<p>collect routing vrf input</p> <p>Example: Router(config-flow-record)# collect interface input</p>	<p>Configures the routing VRF input as a non-key field for a Cisco Flexible NetFlow flow record and enables collecting the routing VRF input fields from the flows for the flow record.</p>

	Command or Action	Purpose
Step 9	<p>collect flow direction</p> <p>Example: Router(config-flow-record)# collect flow direction</p>	Configures the flow direction as a non-key field for a Cisco Flexible NetFlow flow record.
Step 10	<p>collect timestamp sys-uptime first</p> <p>Example: Router(config-flow-record)# collect timestamp sys-uptime first</p>	<p>Configures the system uptime of the first seen packet in a flow as a nonkey field for a Cisco Flexible NetFlow flow record.</p> <ul style="list-style-type: none"> first—Configures the system uptime for the time the first packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the first packet was seen from the flows.
Step 11	<p>collect timestamp sys-uptime last</p> <p>Example: Router(config-flow-record)# collect timestamp sys-uptime last</p>	<p>Configures the system uptime of the last seen packet in a flow as a nonkey field for a Cisco Flexible NetFlow flow record.</p> <ul style="list-style-type: none"> last—Configures the system uptime for the time the last packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the most recent packet was seen from the flows.
Step 12	<p>collect counter bytes long</p> <p>Example: Router(config-flow-record)# collect counter bytes long</p>	<p>Configures the number of bytes in a flow as a nonkey field for a Cisco Flexible NetFlow flow record.</p> <ul style="list-style-type: none"> bytes—Configures the number of bytes seen in a flow as a nonkey field and enables collecting the total number of bytes from the flow. long—Enables collecting the total number of bytes or packets from the flow using a 64-bit counter rather than a 32-bit counter.
Step 13	<p>collect counter packets</p> <p>Example: Router(config-flow-record)# collect counter packets</p>	<p>Configures the number of packets in a flow as a nonkey field for a Cisco Flexible NetFlow flow record.</p> <ul style="list-style-type: none"> packets—Configures the number of packets seen in a flow as a nonkey field and enables collecting the total number of packets from the flow.
Step 14	<p>collect connection new-connections</p> <p>Example: Router(config-flow-record)# collect connection new-connections</p>	Counts the number of TCP or UDP connections which were opened during the observation period. The observation period may be specified by the flow start and end timestamps.

	Command or Action	Purpose
Step 15	collect connection sum-duration Example: Router(config-flow-record)# collect connection sum-duration	Aggregates the total time, in seconds, for all of the TCP or UDP connections, which were in use during the observation period. For example, if there are five concurrent connections each for 10 seconds, the value would be 50 seconds.
Step 16	end Example: Router(config-flow-record)# end	Exits flow record configuration mode and returns to privileged EXEC mode.

Verifying Usage Records

To verify usage records, perform the following optional task.

SUMMARY STEPS

1. **enable**
2. **show flow record** *[[name] record-name | netflow-original | netflow {ipv4 | ipv6} record [peer]]*

DETAILED STEPS

Step 1 **enable**

The **enable** command enters privileged EXEC mode (enter the password if prompted).

```
Router> enable
```

```
Router#
```

Step 2 **show flow record** *[[name] record-name | netflow-original | netflow {ipv4 | ipv6} record [peer]]*

Displays the status and statistics for a flow record.

```
Router# show flow record name my-usage-monitor-record
```

```
flow record my-input-usage-monitor
  match interface input
  match flow direction
  match application name account-on-resolution
  match ipv4 version
  collect interface output
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
  collect counter bytes long
  collect counter packets
  collect connection new-connections
  collect connection sum-duration
  collect routing vrf input
```

```
Router# show flow record name my-output-usage-monitor-record
```

```
flow record my-output-usage-monitor
  match application name account-on-resolution
  match flow direction
  match interface output
  collect interface input
  collect timestamp sys-uptime first
```



```

collect timestamp sys-uptime last
collect counter bytes long
collect counter packets
collect connection new-connections
collect connection sum-duration
collect routing vrf input
    
```

Configuring Usage Monitoring

To configure usage monitoring, perform the following required task.



Note



You must configure separate flow monitors for both input and output directions to capture traffic in each direction.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *flow-monitor-name*
4. **record** *flow-record-name*
5. **exporter** *exporter-name*
6. **cache type normal**
7. **cache entries** *cache-entries*
8. **cache timeout active 300**
9. **cache timeout inactive 300**
10. **exit**
11. **interface** *interface-type interface-number*
12. **ip flow monitor** *flow-monitor-name* **input**
13. **ip flow monitor** *flow-monitor-name* **output**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p>flow monitor <i>flow-monitor-name</i></p> <p>Example: Router(config)# flow monitor my-input-usage-monitor</p>	<p>Creates a a flow monitor/usage record and enters Cisco Flexible NetFlow flow monitor configuration mode.</p> <ul style="list-style-type: none"> This command also allows you to modify an existing flow monitor. <p> Note A usage record is a type of flow monitor. Either flow monitor or usage record may be used in the procedure to specify a usage record.</p>
Step 4	<p>record <i>flow-record-name</i></p> <p>Example: Router(config-flow-monitor)# record my-input-usage-record</p>	<p>Configures the record operation to operate on the usage record.</p>
Step 5	<p>exporter <i>exporter-name</i></p> <p>Example: Router(config-flow-monitor)# exporter EXPORT-ER-1</p>	<p>Specifies the name of an exporter that you created previously.</p> <ul style="list-style-type: none"> This is the exporter the usage record uses. <p> Note You configured the name of this exporter in Step 3 of “Creating the Flow Exporter” section on page 7.</p>
Step 6	<p>cache type normal</p> <p>Example: Router(config-flow-monitor)# cache type normal</p>	<p>(Optional) Configures parameters for the usage record.</p> <ul style="list-style-type: none"> cache entries is equal to the number of expected parallel applications multiplied by the number of interfaces with usage reports. The default is 500.
Step 7	<p>cache entries <i>cache-entries</i></p> <p>Example: cache entries 5000</p>	<p>(Optional) Configures parameters for the usage record</p>
Step 8	<p>cache timeout active 300</p> <p>Example: cache timeout active 300</p>	<p>(Optional) Configures parameters for the usage record</p>
Step 9	<p>cache timeout inactive 300</p> <p>Example: cache timeout inactive 300</p>	<p>(Optional) Configures parameters for the usage record</p>
Step 10	<p>exit</p> <p>Example: Router(config-flow-monitor)# exit</p>	<p>Exits Cisco Flexible NetFlow flow monitor configuration mode and returns to global configuration mode.</p>

	Command or Action	Purpose
Step 11	interface <i>interface-type interface-number</i> Example: Router(config)# interface et0/0	Enters interface configuration mode and configures the specific interface on which the usage record will record the different type of applications.
Step 12	ip flow monitor <i>flow-monitor-name input</i> Example: Router(config-if)# ip flow monitor my-input-us- age-monitor input	Attaches a specific flow monitor to monitor the input of the configured interface for the usage record. <ul style="list-style-type: none"> Use the usage record/flow monitor created for the input direction for the ip flow monitor <i>flow-monitor-name input</i> command.
Step 13	ip flow monitor <i>flow-monitor-name output</i> Example: Router(config-if)# ip flow monitor my-out- put-usage-monitor output	Attaches a specific flow monitor to monitor the output of the configured interface for the usage record. <ul style="list-style-type: none"> Use the usage record/flow monitor created for the output direction for the ip flow monitor <i>flow-monitor-name output</i> command.
Step 14	end Example: Router(config-flow-monitor)# end	Exits flow monitor configuration mode and returns to privileged EXEC mode.

Verifying Usage Monitoring

To verify usage monitoring, perform the following optional task.



Note

To display the current status of a flow exporter, refer to the [“Verifying the Flow Exporter Configuration” section on page 9](#).

Prerequisites

Before you can display the flows in the flow monitor cache, the interface to which you applied the input flow monitor must be receiving traffic.

SUMMARY STEPS

- enable**
- show flow monitor** *[[name] monitor-name [cache [format {csv | record | table}]] [statistics]]*
- show interface**

DETAILED STEPS

Step 1 enable

The **enable** command enters privileged EXEC mode (enter the password if prompted).

```
Router> enable
```

```
Router#
```

Step 2 **show flow monitor** *[[name] monitor-name* *[cache [format { csv | record | table }]] [statistics]]*

Displays the status and statistics for a flow monitor.

```
Router# show flow monitor name my-input-usage-monitor
```

```
flow monitor my-input-usage-monitor
  record my-input-usage-monitor-record
  exporter my-usage-monitor-exporter
  cache type normal
  cache entries 5000
  cache timeout active 300
  cache timeout inactive 300
```

or

```
Router# show flow monitor name my-output-usage-monitor
```

```
flow monitor my-output-usage-monitor
  record my-output-usage-monitor-record
  exporter my-usage-monitor-exporter
  cache type normal
  cache entries 5000
  cache timeout active 300
  cache timeout inactive 300
```

Step 3 **show interface**

Displays the specific flow monitors attached to the interface.

```
Router# show interface
```

```
interface et0/0
  ip flow monitor my-input-usage-monitor input
  ip flow monitor my-output-usage-monitor output
```

Creating Transaction Records and Monitoring

This section is made up of the following procedures:

- [Configuring Transaction Records, page 20](#) (required)
- [Verifying Transaction Records, page 29](#) (optional)
- [Configuring Transaction Records, page 20](#) (required)
- [Verifying Transaction Records, page 25](#) (optional)

Configuring Transaction Records

To configure transaction records, perform the following required task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *flow-record-name*
4. **match connection transaction-id**

5. collect interface input
6. collect interface output
7. collect flow direction
8. collect ipv4 protocol
9. collect ipv4 source address
10. collect ipv4 destination address
11. collect ipv4 version
12. collect ipv6 version
13. collect routing vrf input
14. collect transport source-port
15. collect transport destination-port
16. collect connection initiator
17. collect timestamp sys-uptime first
18. collect timestamp sys-uptime last
19. collect counter bytes long
20. collect counter packets
21. collect flow sampler
22. collect application name
23. collect flow end reason
24. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	flow record <i>flow-record-name</i> Example: Router(config)# flow record my-tr-monitor-record	Creates a flow record and enters flow record configuration mode.

	Command or Action	Purpose
Step 4	<p>match connection transaction-id</p> <p>Example: <pre>Router(config-flow-record)# match connection transaction-id</pre></p>	<p>Specifies match criteria.</p> <ul style="list-style-type: none"> transaction-id—This keyword identifies a transaction within a connection. A transaction is a meaningful exchange of application data between two network devices or a client and server. A transaction-id is assigned the first time a flow is reported, so that later reports for the same flow will have the same transaction. A different transaction Id is used for each transaction within a TCP or UDP connection. The identifiers are not required to be sequential.
Step 5	<p>collect interface input</p> <p>Example: <pre>Router(config-flow-record)# collect interface input</pre></p>	<p>Configures the input interface as a non-key field for a Cisco Flexible NetFlow flow record and enables collecting the input interface fields from the flows for the flow record.</p>
Step 6	<p>collect interface output</p> <p>Example: <pre>Router(config-flow-record)# collect interface output</pre></p>	<p>Configures the output interface as a non-key field for a Cisco Flexible NetFlow flow record and enables collecting the output interface fields from the flows for the flow record.</p>
Step 7	<p>collect flow direction</p> <p>Example: <pre>Router(config-flow-record)# collect flow direction</pre></p>	<p>Configures the flow direction as a non-key field for a Cisco Flexible NetFlow flow record.</p>
Step 8	<p>collect ipv4 protocol</p> <p>Example: <pre>Router(config-flow-record)# collect ipv4 protocol</pre></p>	<p>Configures one or more of the IPv4 fields as a nonkey field for a Cisco Flexible NetFlow flow record.</p> <p>protocol—Configures the IPv4 payload protocol field as a nonkey field and enables collecting the IPv4 value of the payload protocol field for the payload in the flows.</p>
Step 9	<p>collect ipv4 source address</p> <p>Example: <pre>Router(config-flow-record)# collect ipv4 source address</pre></p>	<p>Configures the IPv4 source address as a nonkey field for a Cisco Flexible NetFlow flow record.</p> <ul style="list-style-type: none"> address—Configures the IPv4 source address as a nonkey field and enables collecting the value of the IPv4 source address from the flows.
Step 10	<p>collect ipv4 destination address</p> <p>Example: <pre>Router(config-flow-record)# collect ipv4 destination address</pre></p>	<p>Configures the IPv4 destination address as a nonkey field for a Cisco Flexible NetFlow flow record.</p> <ul style="list-style-type: none"> address—Configures the IPv4 destination address as a nonkey field and enables collecting the value of the IPv4 destination address from the flows

	Command or Action	Purpose
Step 11	collect ipv4 version Example: Router(config-flow-record)# collect ipv4 version	(Optional) For IPv4 networks, configures the IPv4 version as a nonkey field for a Cisco Flexible NetFlow flow record.
Step 12	collect ipv6 version Example: Router(config-flow-record)# collect ipv6 version	(Optional) For IPv6 networks, configures the IPv6 version as a nonkey field for a Cisco Flexible NetFlow flow record.
Step 13	collect routing vrf input Example: Router(config-flow-record)# collect routing vrf input	Configures the routing VRF input as a nonkey field for a Cisco Flexible NetFlow flow record.
Step 14	collect transport source-port Example: Router(config-flow-record)# collect transport source-port	Configures one or more of the transport layer fields as a nonkey field for a Cisco Flexible NetFlow flow record. <ul style="list-style-type: none"> • source-port—Configures the source port as a nonkey field and enables collecting the value of the destination port from the flows.
Step 15	collect transport destination-port Example: Router(config-flow-record)# collect transport destination-port	Configures one or more of the transport layer fields as a nonkey field for a Cisco Flexible NetFlow flow record. <ul style="list-style-type: none"> • destination-port—Configures the destination port as a nonkey field and enables collecting the value of the destination port from the flows.
Step 16	collect connection initiator Example: Router(config-flow-record)# collect connection initiator	Configures the connection initiator as a nonkey field for a Cisco Flexible NetFlow flow record. <ul style="list-style-type: none"> • connection initiator—Provides information about the direction of the flow. <ul style="list-style-type: none"> – 0 x 00—undefined – 0 x 01—initiator (the flow source is initiator of the connection) – 0 x 02—reverse Initiator (the flow destination is the initiator of the connection)
Step 17	collect timestamp sys-uptime first Example: Router(config-flow-record)# collect timestamp sys-uptime first	Configures the system uptime of the first seen packet in a flow as a nonkey field for a Cisco Flexible NetFlow flow record. <ul style="list-style-type: none"> • first—Configures the system uptime for the time the first packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the first packet was seen from the flows.

	Command or Action	Purpose
Step 18	collect timestamp sys-uptime last Example: <pre>Router(config-flow-record)# collect timestamp sys-uptime last</pre>	Configures the system uptime of the last seen packet in a flow as a nonkey field for a Cisco Flexible NetFlow flow record. <ul style="list-style-type: none"> • last—Configures the system uptime for the time the last packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the most recent packet was seen from the flows.
Step 19	collect counter bytes long Example: <pre>Router(config-flow-record)# collect counter bytes long</pre>	Configures the number of bytes in a flow as a nonkey field for a Cisco Flexible NetFlow flow record. <ul style="list-style-type: none"> • bytes—Configures the number of bytes seen in a flow as a nonkey field and enables collecting the total number of bytes from the flow. • long—Enables collecting the total number of bytes or packets from the flow using a 64-bit counter rather than a 32-bit counter.
Step 20	collect counter packets Example: <pre>Router(config-flow-record)# collect counter packets</pre>	Configures the number of packets in a flow as a nonkey field for a Cisco Flexible NetFlow flow record. <ul style="list-style-type: none"> • packets—Configures the number of packets seen in a flow as a nonkey field and enables collecting the total number of packets from the flow.
Step 21	collect flow sampler Example: <pre>Router(config-flow-record)# collect flow sam- pler</pre>	Reports the sampler-id of the sampler configured for this record. Using the sampler option template, the sampler name can be retrieved based on the sampler-id .
Step 22	collect application name Example: <pre>Router(config-flow-record)# collect applica- tion name</pre>	Configures the use of the application name as a nonkey field for a Cisco Flexible NetFlow flow record.
Step 23	collect flow end reason Example: <pre>Router(config-flow-record)# collect flow end reason</pre>	Configures the use of the end of the flow as a nonkey field for a Cisco Flexible NetFlow flow record.
Step 24	end	Exits flow record configuration mode and returns to privileged EXEC mode.

Verifying Transaction Records

To verify transaction records, perform the following optional task.

SUMMARY STEPS

1. **enable**
2. **show flow record name** *record-name*

DETAILED STEPS

Step 1 enable

The **enable** command enters privileged EXEC mode (enter the password if prompted).

```
Router> enable
```

```
Router#
```

Step 2 show flow record name *record-name*]

Displays the status and statistics for a flow record.

```
Router# show flow record name my-tr-monitor-record
```

```
flow record my-tr-monitor-record
  match connection transaction-id
  collect interface input
  collect interface output
  collect flow direction
  collect ipv4 version
  collect ipv4 protocol
  collect ipv4 source address
  collect ipv4 destination address
  collect transport source-port
  collect transport destination-port
  collect connection initiator
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
  collect counter bytes long
  collect counter packets
  collect flow sampler
  collect application name
  collect flow end reason
  collect routing vrf input
```

Configuring Transaction Records

To configure transaction records, perform the following required task.

**Note**


You must configure separate flow monitors for both input and output directions to capture traffic in each direction.






SUMMARY STEPS





1. **enable**

2. **configure terminal**
3. **flow monitor** *flow-monitor-name*
4. **record** *flow-monitor-name*
5. **exporter** *exporter-name*
6. **cache timeout event transaction-end**
7. **cache entries** *cache-entries*
8. **exit**
9. **sampler** *sampler-name*
10. **mode {deterministic | random} 1 out-of window-size**
11. **granularity connection**
12. **interface** *interface-type interface-number*
13. **ip flow monitor** *flow-monitor-name* **input**
14. **ip flow monitor** *flow-monitor-name* **output**
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	flow monitor <i>flow-monitor-name</i> Example: Router(config)# flow monitor my-tr-monitor	Creates a a flow monitor/usage record and enters Cisco Flexible NetFlow flow monitor configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow monitor.
		 Note A usage record is a type of flow monitor. Either flow monitor or usage record may be used in the procedure to specify a usage record.
Step 4	record <i>flow-monitor-name</i> Example: Router(config-flow-monitor)# record my-tr-monitor-record	Configures the record operation to operate on the usage record.

	Command or Action	Purpose
Step 5	<p>exporter <i>exporter-name</i></p> <p>Example: <pre>Router(config-flow-monitor)# exporter my-tr-monitor-exporter</pre></p>	<p>Specifies the name of an exporter that you created previously. This is the exporter the usage record uses.</p> <p> Note You configured the name of this exporter in Step 3 of “Creating the Flow Exporter” procedure on page -7.</p>
Step 6	<p>cache timeout event transaction-end</p> <p>Example: <pre>Router(config-flow-monitor)# cache timeout event transaction-end</pre></p>	<p>Configures the timeout parameters for the usage record.</p> <ul style="list-style-type: none"> transaction-end—Generates the record in the NetFlow cache at the end of a transaction. <p> Note The Cisco Application Visibility and Control feature introduced the transaction-end as a keyword for the cache command.</p> <p> Note transaction-end must have the application name in the record.</p> <p> Note transaction-end must have the transaction-id as a matched field in the record.</p>
Step 7	<p>cache entries <i>cache-entries</i></p> <p>Example: <pre>Router(config-flow-monitor)# cache entries 30000</pre></p>	<p>Configures parameters for the usage record.</p> <ul style="list-style-type: none"> <i>cache-entries</i>—the maximum number of flows multiplied by two multiplied by the flow-sampling rate. <p> Note For further information about flows, see the “Information About Cisco NBAR Memory for Cisco Application Visibility and Control” section on page 33.</p>
Step 8	<p>exit</p> <p>Example: <pre>Router(config-flow-monitor)# exit</pre></p>	<p>Exits Cisco Flexible NetFlow flow monitor configuration mode and returns to global configuration mode.</p>
Step 9	<p>sampler <i>sampler-name</i></p> <p>Example: <pre>Router(config)# sampler my-tr-sampler</pre></p>	<p>Creates a Cisco Flexible NetFlow flow sampler and enters Cisco Flexible NetFlow sampler configuration mode.</p>

Command or Action	Purpose
<p>Step 10 mode {deterministic random} 1 out-of window-size</p> <p>Example: Router(config-sampler)# mode random 1 out-of 1000</p>	<p>Specifies the type of sampling and the packet interval for a Cisco Flexible NetFlow sampler.</p> <p> Note The sampling rate must conform to the Cisco Collection Manager supported rate for a given platform and a given network flow rate.</p>
<p>Step 11 granularity connection</p> <p>Example: Router(config-sampler)# granularity connection</p>	<p>Samples connections and sends all packets for this given connection. This is opposed to per packet sampling where all connections are exported but for each connection only sampled packets are accounted.</p> <p> Note The Cisco Application Visibility and Control feature introduced the granularity connection command.</p> <p> Note There is no deterministic sampler with the granularity connection.</p> <p> Note A granularity connection must have the application name in the record.</p>
<p>Step 12 interface interface-type interface-number</p> <p>Example: Router(config)# interface et0/0</p>	<p>Enters interface configuration mode and configures the specific interface on which the usage record will record the different type of applications on.</p>
<p>Step 13 ip flow monitor flow-monitor-name input</p> <p>Example: Router(config-if)# ip flow monitor my-tr-monitor sampler my-tr-sampler input</p>	<p>Attaches a specific flow monitor to monitor the input of the configured interface for the usage record.</p> <p>Use the usage record/flow monitor created for the input direction for the ip flow monitor flow-monitor-name input command.</p>
<p>Step 14 ip flow monitor flow-monitor-name output</p> <p>Example: Router(config-if)# ip flow monitor my-tr-monitor sampler my-tr-sampler output</p>	<p>Attaches a specific flow monitor to monitor the output of the configured interface for the usage record.</p> <p>Use the usage record/flow monitor created for the output direction for the ip flow monitor flow-monitor-name output command.</p>
<p>Step 15 end</p> <p>Example: Router(config-flow-monitor)# end</p>	<p>Leaves flow monitor configuration mode and returns to privileged EXEC mode.</p>

Verifying Transaction Records

To display the configuration of a flow monitor and a Cisco Flexible NetFlow sampler, perform the following optional procedure:

**Note**

To display the current status of a flow exporter, see the [“Verifying the Flow Exporter Configuration” section on page 9](#).

SUMMARY STEPS

1. **enable**
2. **show flow monitor** [**name** *flow-monitor-name*]
3. **show sampler** [[**name**] *sampler-name*]

DETAILED STEPS

Step 1 **enable**

The **enable** command enters privileged EXEC mode (enter the password if prompted).

```
Router> enable
```

```
Router#
```

Step 2 **show flow monitor** [**name** *flow-monitor-name*]

Displays the configuration of a flow monitor.

```
Router# show flow monitor name my-tr-monitor
```

```
flow monitor my-tr-monitor
  record my-tr-monitor-record
  exporter my-tr-monitor-exporter
  cache timeout event transaction-end
  cache entries 30000
```

Step 3 **show sampler** [[**name**] *sampler-name*]

Displays the configuration of a Cisco Flexible NetFlow sampler.

```
Router# show sampler name my-tr-sampler
```

```
sampler my-tr-sampler
  mode random 1 out-of 100
  granularity Connection
```

Configuration Examples for Cisco Application Visibility and Control

This section provides the following configuration example:

- [Example: Configuring Cisco Application Visibility and Control](#)

Example: Configuring Cisco Application Visibility and Control

The following example shows how to configure Cisco Application Visibility and Control. This sample starts in global configuration mode.

```

flow record my-total-input-usage-monitor-record
 match ipv4 version
 match interface input
 match flow direction
 collect routing vrf input
 collect ipv4 dscp
 collect interface output
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
 collect connection new-connections
 collect connection sum-duration
!
!
flow record my-total-output-usage-monitor-record
 match ipv4 version
 match interface output
 match flow direction
 collect routing vrf input
 collect ipv4 dscp
 collect interface input
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
 collect connection new-connections
 collect connection sum-duration
!
!
flow record my-ipv6-tr-monitor-record
 match connection transaction-id
 collect ipv6 version
 collect interface input
 collect interface output
 collect ipv6 protocol
 collect ipv6 source address
 collect ipv6 destination address
 collect transport source-port
 collect transport destination-port
 collect interface input
 collect interface output
 collect flow direction
 collect flow sampler
 collect flow end-reason

```

```
collect counter bytes long
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect application name
collect routing vrf input
collect connection initiator
!
!
flow exporter expl
destination 10.56.128.231
transport udp 2055
option interface-table timeout 300
option sampler-table timeout 300
option application-attributes timeout 300
option application-table timeout 300
option verf-table timeout 300
!
!
flow monitor input-usage-monitor
record input-usage-record
exporter expl
cache timeout inactive 300
cache timeout active 300
cache entries 5000
casche size entries 10000
!
!
flow monitor output-usage-monitor
record output-usage-record
exporter expl
cache timeout inactive 300
cache timeout active 300
cache entries 5000
cache size entries 10000
!
!
flow monitor my-total-input-usage-monitor
record my-total-input-output-usage-monitor-record
exporter expl
cache timeout inactive 300
cache timeout active 300
cache entries 100
!
!
flow monitor my-total-output-usage-monitor
record my-total-input-output-usage-monitor-record
exporter expl
cache timeout inactive 300
cache timeout active 300
cache entries 5000
!
!
flow monitor my-ipv6-tr-monitor
record my-ipv6-tr-monitor-record
exporter my-tr-monitor-exporter
cache timeout event transaction-end
cache entries 20000
!
!
flow monitor tr-monitor
record tr-record
exporter expl
cache timeout event transaction-end
```

```

cache entries 30000
!
!
sampler my-sampler
mode random 1 out-of 1000
granularity Connection
!

interface GigabitEthernet0/1/0
ip address 10.56.128.82 255.255.255.0
negotiation auto
!
! For IPv4:
!
interface GigabitEthernet0/1/1
description *** LAN*****
ip address 1.1.1.254 255.255.255.0
ip flow monitor my-input-usage-monitor input
ip flow monitor my-tr-monitor sampler my-sampler input
ip flow monitor my-output-usage-monitor output
ip flow monitor my-tr-monitor sampler my-sampler output
ip flow monitor my-total-input-usage-monitor input
ip flow monitor my-total-output-usage-monitor output

! For IPv6:
!
interface GigabitEthernet0/1/1
description *** LAN*****
ip address 1.1.1.254 255.255.255.0
ip flow monitor my-input-usage-monitor input
ip flow monitor my-output-usage-monitor output
ip flow monitor my-ipv6-tr-monitor sampler my-sampler input
ip flow monitor my-ipv6-tr-monitor sampler my-sampler output
ip flow monitor my-total-input-usage-monitor input
ip flow monitor my-total-output-usage-monitor output
!
ip flow monitor tr-monitor sampler my-sampler input
no negotiation auto
!
interface GigabitEthernet0/1/2
description *** WAN*****
ip address 2.2.2.254 255.255.255.0
ip flow monitor input-usage-monitor input
ip flow monitor output-usage-monitor output
ip flow monitor tr-monitor sampler my-sampler output
no negotiation auto

```


Information About Cisco NBAR Memory for Cisco Application Visibility and Control

Cisco NBAR is an essential part of Cisco Application Visibility and Control. In general, Cisco NBAR is can increase application performance through better QoS and policing, and visibility into what applications are using the network by determining that a particular network flow is from a specific application. This is done using various techniques. Upon detection of a flow, a protocol ID is assigned to it. The protocol ID is then used by the solution to determine the appropriate actions on packets belonging to that flow.

Cisco Application Visibility and Control uses the NBAR flow table to store per flow information. It can only act on flows which have an active session in the flow table. The number of flows in the flow table affects the performance and capacity of the Cisco ASR 1000 Series Router. You can configure the amount of memory depending on the memory available in your router.

There is also a fixed memory limit. This prevents strain on the Cisco ASR 1000 Series Router when features other than the Cisco Application Visibility and Control allocate flow table memory. When a fixed memory limit is reached, the Cisco Application Visibility and Control flows supported by the Cisco ASR 1000 Series Router may drop below the number you configured.

The maximum and default number of flows and the fixed memory limit supported is show in [Table 1](#). The amounts are based on the specific Embedded Service Processor (ESP) in your Cisco ASR 1000 Series Router. See your router specifications to determine the ESP type.

Table 1 Maximum and Default Number of Flows Based on ESP

Embedded Services Processors	Maximum Flows	Default Flows	Memory Upper Limit (MB) (Equals 70% of the Platform Memory)
ESP5	750,000	500,000	179
ESP10	1,650,000	1,000,000	358
ESP20	3,500,000	1,000,000	716
ESP40	3,500,000	1,000,000	716

How to Configure Cisco NBAR Memory for Cisco Application Visibility and Control

For general information on configuring Cisco NBAR, refer to *Classifying Network Traffic Using NBAR in Cisco IOS XE Software*

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/clsfy_traffic_nbar_xe.html

To configure NBAR flow table memory, perform the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nbar resources flow max-sessions *number-of-sessions***
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip nbar resources flow max-sessions <i>number-of-sessions</i> Example: Router(config)# ip nbar resources flow max-sessions <i>number-of-sessions</i>	Configures the maximum number of flows which can be allocated in the flow table. • <i>number-of-sessions</i> —The maximum and default number of flow sessions for a specific platform are shown in Table 1 .
Step 4	end Example: Router(config)# end	Leaves global configuration mode and returns to privileged EXEC mode.

Displaying Cisco NBAR Information

To display information about NBAR flow memory, complete the following procedure:

SUMMARY STEPS

1. **enable**
2. **show ip nbar resources flow**

DETAILED STEPS

Step 1 enable

The **enable** command enters privileged EXEC mode (enter the password if prompted).

```
Router> enable
```

```
Router#
```

Step 2 show ip nbar resources flow

Displays the NBAR flow statistics.

```
Router# show ip nbar resources flow
```

```

Maximum no of sessions allowed : 2000000
Maximum memory usage allowed   : 734003 KBytes
Active sessions                 : 1
Active memory usage            : 49338 KBytes
Peak session                    : 1

```

Peak memory usage : 49338 KBytes

Table 2 describes the significant fields shown in the display.

Table 2 *show ip nbar resources flow Field Descriptions*

Field	Description
Maximum number of sessions allowed	Currently configured max-sessions value.
Maximum memory usage allowed	Upper limit on memory usage.
Active sessions	Current active sessions.
Active memory usage	Current memory usage.
Peak sessions	Historical peak in terms of active sessions for the current boot cycle.
Peak memory usage	Historical peak in terms of memory usage for the current boot cycle.

Information About Cisco Modular QoS (MQC)

Standard Cisco Modular QoS (MQC) provides the control portion of Cisco Application Visibility and Control. Experience with Cisco QoS is required to implement a solution specific to your network.

- For specific information about configuring QoS with MQC, see *Applying QoS Features Using the MQC* at http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/qos_mqc.html.
- For information about configuring Cisco QoS, see the *Cisco IOS Quality of Service Solutions Configuration Guide* at http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/12_4/qos_12_4_book.html

Basic configuration of Cisco QoS for Cisco Application Visibility and Control includes:

- Configuring user defined sub-application IDs or access control lists (ACLs).
- Defining the classes required to apply policy by using application IDs or Categories/Attributes.
- Defining Monitoring action
 - Define the Usage and Transaction Records of Cisco Application Visibility and Control. (See the “[How to Configure Cisco Application Visibility and Control](#)” section on page 6).
 - Attach the record generation directly under the interface or under a class map.
- Defining a QoS policy
- Defining a monitoring policy
 - Use policy-map for reporting

Configuration Examples for Cisco Modular QoS (MQC)

This section provides the following examples:

- [Example: Protocol Classification, page 36](#)
- [Example: Attribute Classification, page 36](#)
- [Example: Combination Classification, page 36](#)
- [Example: Excluding an Application from a Category, page 36](#)
- [Example: Sub-application Classification, page 37](#)
- [Example: Destination-Based Policy, page 37](#)
- [Example: Applying a QoS Policy, page 38](#)
- [Example: Applying Different Policies to Different Interfaces, page 38](#)
- [Example: Default QoS Policy, page 39](#)
- [Example: Policy Hierarchy, page 39](#)
- [Example: Policy Hierarchy, page 39](#)

Example: Protocol Classification

The following example shows how a single protocol is classified:

```
class-map match-any bittorrent-class
  match protocol bittorrent
```

Example: Attribute Classification

The following example shows how to classify all mail traffic:

```
class-map match-any mail-class
  match protocol attribute category email
```

Example: Combination Classification

The following example shows how to classify FTP traffic, e-mail traffic, and a single application of BitTorrent. A class can contain the combination of application ID, attributes, or other classes:

```
class-map match-any ftp-mail-bittorrent-class
  match protocol attribute sub-category ftp
  match class-map mail-class
  match protocol bittorrent
```

Example: Excluding an Application from a Category

The following example shows how to exclude *edonkey* from *p2p*. You first define a class in the policy-map based on *edonkey*.

```
class-map match-any class-edonkey
  match protocol edonkey
class-map match-any class-p2p
```

```
match protocol attribute sub-category p2p
policy-map my-policy
class class-edonkey
  <actions only for edonkey>
class class-p2p
  <actions for p2p excluding edonkey>

interface eth0/0
  service-policy input my-policy
```

Example: Sub-application Classification

The following example shows a classification of a sub-application. Such a configuration does not impact the application ID definition. It adds a classification on the sub-application to be used in a match statement. This is different from an SCE “flavor” configuration which causes new applications (services in the SCE terms) to be created. The following example shows how to configure a 1 Gbps committed rate to myuploadserver.com, while a peak rate is applied to all other browsing traffic:

```
class-map match-any browsing-class
  match protocol attribute category browsing

class-map match-all my-upload-server-class
  match protocol http url "*myuploadserver.com*"

policy-map policy1
  class my-upload-server-class
    police cir 1000000000
  class browsing-class
    police pir 400000000
```

Example: Destination-Based Policy

The following example shows a destination-based policy. A destination-based policy doesn't impact the application ID definition as used in the SCE. It adds a group of Layer 4 classification filters for use in a match statement. The following example provides policing of HTTP traffic that goes to 30.3.0.0/16 or 20.2.0.0/16. The match on access-group could be applied to any class level.

```
access-list 101 permit ip 30.3.0.0 0.0.255.255 any
access-list 101 permit ip 20.2.2.0 0.0.255.255 any

class-map match-all 2030-http-class
  match protocol http
  match access-group 101

policy-map policy1
  class 2030-http-class
    police 4000
```

Example: Applying a QoS Policy

The following example shows how to apply maximum bandwidth on an application by using a policer. In this example, a peak information rate (PIR) of 1 Gbps is enforced on peer-to-peer traffic. The policer is defined on the input direction of the interface.

```
class-map match-any p2p-class
  match protocol attribute sub-category p2p

policy-map p2p-policy
  class p2p-class
    police pir 1000000000

interface eth0/0
  service-policy input p2p-policy
```

The following example shows how to apply maximum bandwidth on an application by using a queue instead of a policer. In this example, a PIR of 2 Gbps is enforced on the peer-to-peer traffic. The queue is defined on the output direction of the interface.

```
class-map match-any p2p-class
  match protocol attribute sub-category p2p

policy-map p2p-limit
  class p2p-class
    shape 2000000000

interface eth0/0
  service-policy output p2p-limit
```

The following example shows how to prioritize specific application over another application. In this example, all the traffic is directed to the same queue, but the peer-to-peer traffic gets a lower weight so it will be de-prioritized when the queue is full. The application prioritization can be enforced only on the output direction only because it is implemented with the queue.

```
class-map match-any p2p-class
  match protocol attribute sub-category p2p

policy-map p2p-prio
  class p2p-class
    bandwidth remaining ratio 10
  class class-default
    bandwidth remaining ratio 50

interface eth0/0
  service-policy output p2p-prio
```

Example: Applying Different Policies to Different Interfaces

The following example shows two policy maps, one for only FTP and one for FTP and peer-to-peer. The two policy maps apply to different interfaces:

```
class-map match-any ftp-class
  match protocol attribute sub-category ftp

class-map match-any p2p-ftp-policy-class
  match protocol attribute sub-category p2p
  match class-map ftp-class

policy-map p2p-ftp-policy
```

```
class p2p-ftp-policy-class
  police pir 400000000

policy-map ftp-policy
  class ftp-class
    police pir 100000000

interface eth0/0
  service-policy input p2p-ftp-policy
interface eth1/1
  service-policy input ftp-policy
```

Example: Default QoS Policy

The following example shows a default policy used to set a policy for all traffic that is not specifically classified. The reserved class-default class is used.

```
policy-map default-policy
  class class-default
    police pir 400000000

interface eth0/0
  service-policy input default-policy
```

Example: Policy Hierarchy

The following example shows a policy hierarchy. In many cases, you need to apply a policy for classified traffic when applying an additional policy for a subset of this traffic. In the standard way of class order, this cannot apply. To configure such a policy, a policy hierarchy is used.

The following example shows how to set a default limit for file-sharing traffic at 400 Mbps. The traffic limit for peer-to-peer and FTP, which are subsets of file-sharing, is set at 100 Mbps.

```
class-map match-any p2p-ftp-policy-class
  match protocol attribute sub-category p2p
  match protocol attribute sub-category ftp

class-map match-any file-sharing-class
  match protocol attribute category file-sharing

policy-map p2p-ftp-policy
  class p2p-ftp-policy-class
    police pir 100000000

policy-map file-sharing-policy
  class file-sharing-class
    police pir 400000000
    service-policy p2p-ftp-policy

interface eth0/0
  service-policy input file-sharing-policy
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
NetFlow commands	Cisco IOS NetFlow Command Reference
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
List of the features documented in the <i>Cisco IOS NetFlow Configuration Guide</i>	Cisco IOS NetFlow Features Roadmap
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for using Cisco MQC	Applying QoS Features Using the MQC
Tasks for configuring Cisco QoS	Cisco IOS Quality of Service Solutions Configuration Guide
Tasks for configuring Cisco NBAR	Classifying Network Traffic Using NBAR in Cisco IOS XE Software
NBAR commands.	Cisco IOS Quality of Service Solutions Command Reference

Standards

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

MIBs

MIBs	MIBs Link
None	<p>No new MIBs were created for this feature.</p> <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

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

Glossary

Application ID—The application identifier is the unique definition of a specific Layer 2 to Layer 7 application. Also referred to as protocol-ID.

Application Recognition— Classification of a flow that ends with an application ID. This can be stateless or stateful. Also called application detection.

Application Session—When a flow is associated with a particular protocol or application, this is referred to as a session. A session often implies a user login and logout, and may include the multiple flows of a particular subscriber.

BiFlow—A BiFlow is composed of packets associated with both the forward direction and the reverse direction between endpoints. Also referred to as a full flow or bi-directional flow. See RFC5101.

Cisco Collection Manager—The Cisco Collection Manager is a set of software modules that runs on a server. It receives and processes NetFlow Records. The processed records are stored in the Cisco Collection Manager database. The database can be either bundled or external.

Cisco Insight v3—Cisco Insight v3 is reporting platform software. It processes the formatted data from the Collection Manager database. It presents customized reports, charts, and statistics of the traffic. Cisco Insight v3 is a Web 2.0 application accessed by using a browser.

Flow—Unidirectional stream of packets between a given source and destination. Source and destination are each defined by a network-layer IP address and transport-layer source and destination port numbers.

MQC—Modular QoS CLI. A CLI structure that lets you create traffic polices and attach them to interfaces. A traffic policy contains a traffic class and one or more QoS features. The QoS features in the traffic policy determine how the classified traffic is treated.

NBAR 2—Network-Based Application Recognition 2. A classification engine in Cisco IOS software that recognizes a wide variety of applications, including web-based applications and client/server applications that dynamically assign TCP or UDP port numbers. After the application is recognized, the network can invoke specific services for that application. NBAR is a key part of the Cisco Content Networking architecture and works with QoS features to enable you to use network bandwidth efficiently.

NetFlow—Cisco IOS security and accounting feature that maintains per-flow information.

NetFlow sampler—A set of properties that are defined in a NetFlow sampler map that has been applied to at least one physical interface or subinterface.

NetFlow sampler map—The definition of a set of properties (such as the sampling rate) for NetFlow sampling.

NetFlow v9—NetFlow export format Version 9. A flexible and extensible means for carrying 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.

ToS—type of service. Second byte in the IP header that indicates the desired quality of service for a specific datagram.

Transaction—A set of logical exchanges between endpoints. A typical example of transactions are the series of multiple HTTP GET transactions (each with a different URL) within the same flow. Typically there is one transaction within a flow.

UniFlow—A UniFlow is composed of packets sent from a single endpoint to another single endpoint. Also referred to as a half flow or uni-directional flow. See RFC5101.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2010–2011 Cisco Systems, Inc. All rights reserved.

