Application Visibility and Control Configuration Guide, Cisco IOS XE Release 3S

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

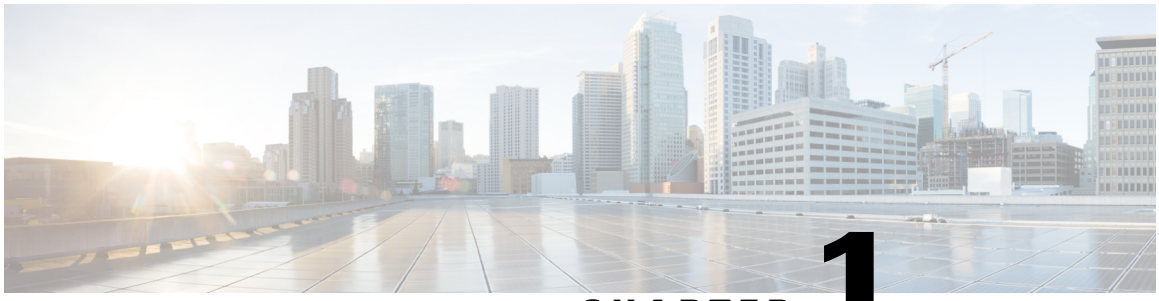
CHAPTER 1 **Configuring Application Visibility and Control for Cisco Flexible Netflow** 1

- New Location of Configuration Procedures 1
- Finding Feature Information 2
- Prerequisites for Cisco Application Visibility and Control 2
- Restrictions for Cisco Application Visibility and Control 2
- Information About Application Availibility and Control 2
  - Components of an Application Visibility and Control Network 2
    - Cisco Network-Based Application Recognition 3
    - Cisco Modular QOS 4
    - Bandwidth Control 4
    - Cisco NetFlow v9 4
    - Cisco IOS Flexible NetFlow Traffic Records 4
    - External Components 5
      - Cisco Collection Manager 6
      - Cisco Insight v3 6
  - Information About Cisco NBAR Memory for Cisco Application Visibility and Control 6
  - Information About Cisco Modular QOS (MQC) 7
- How to Configure Cisco Application Visibility and Control 7
  - New Location of Configuration Procedures 7
- Additional References 8
- Feature Information for Support for AVC on Wireless LAN 9
- Glossary 10

CHAPTER 2 **Easy Performance Monitor** 13

- Finding Feature Information 13
- Information About Easy Performance Monitor 13
  - Easy Performance Monitor 13
  - Profile 14

Traffic Monitor 14
Traffic Monitors for Application Experience Profile 14
Traffic Monitors for Application Statistics Profile 14
Context 15
How to Configure Easy Performance Monitor 15
Configuring Easy Performance Monitor 15
Configuration Examples for Configuring Easy Performance Monitor 17
Example: Configuring a Performance Monitor Context with Default ART, Media, and URL Traffic Monitors 17
Example: Configuring a Performance Monitor Context With Traffic Monitor Enabling the Media Metrics for Ipv6 Traffic in Ingress and Egress Directions 18
Example: Configuring a Performance Monitor Context on Multiple Interfaces 18
Example: Verifying the Complete Configuration for a Performance Monitor Context 18
Example: Verifying the Configuration of a Conversation Level Traffic Monitor Metrics for a Performance Monitor Context 27
Example: Configuring a Performance Monitor Context With Application Statistics Profile 29
Additional References 29
Feature Information for Easy Performance Monitor 30



CHAPTER 1

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, on page 8.

- New Location of Configuration Procedures, page 1
- Finding Feature Information, page 2
- Prerequisites for Cisco Application Visibility and Control, page 2
- Restrictions for Cisco Application Visibility and Control, page 2
- Information About Application Availibility and Control, page 2
- How to Configure Cisco Application Visibility and Control, page 7
- Additional References, page 8
- Feature Information for Support for AVC on Wireless LAN, page 9
- Glossary, page 10

New Location of Configuration Procedures

This guide has been superceded by the AVC Solutions Guide, located at Cisco AVC Solution Guide for IOS XE Release 3.9S.

Finding Feature Information

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

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

Prerequisites for 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 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 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, on page 8.

Restrictions for Cisco Application Visibility and Control

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

Information About Application Availibility and Control

Components of an Application Visibility and Control Network

The following internal and external components of an Application Visibility and Control network are descibed in detail in this section.

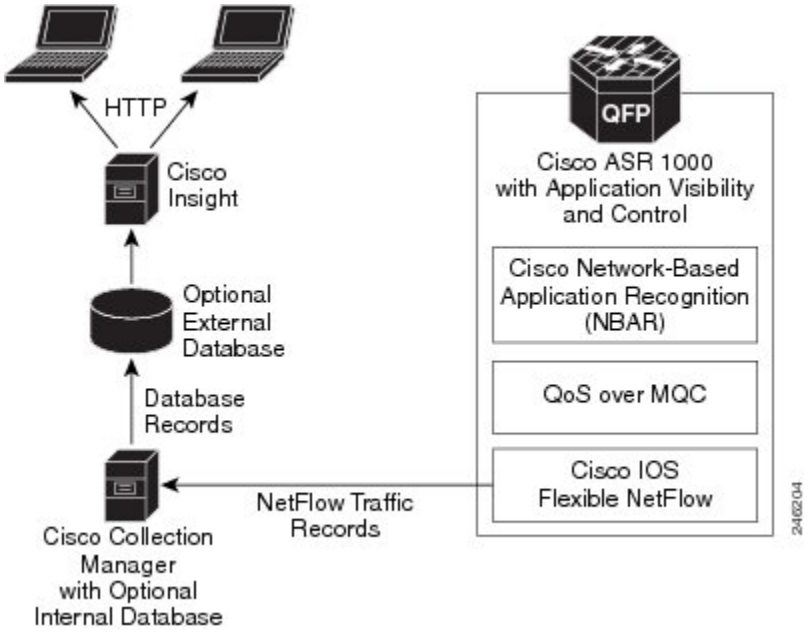
- Internal components (running on the Cisco ASR 1000 Series Router):

- Cisco Network-Based Application Recognition
- Cisco Modular QOS
- Bandwidth Control
- Cisco Netflow v9
- Cisco IOS Flexible Netflow Traffic Records

- External components (running on the separate platform from Cisco ASR 1000 Series Router):
  - Cisco Collection Manager
  - Cisco Insight v3

The core components of the Cisco Application Visibility and Control solution are shown below.

Figure 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).

Cisco NetFlow v9

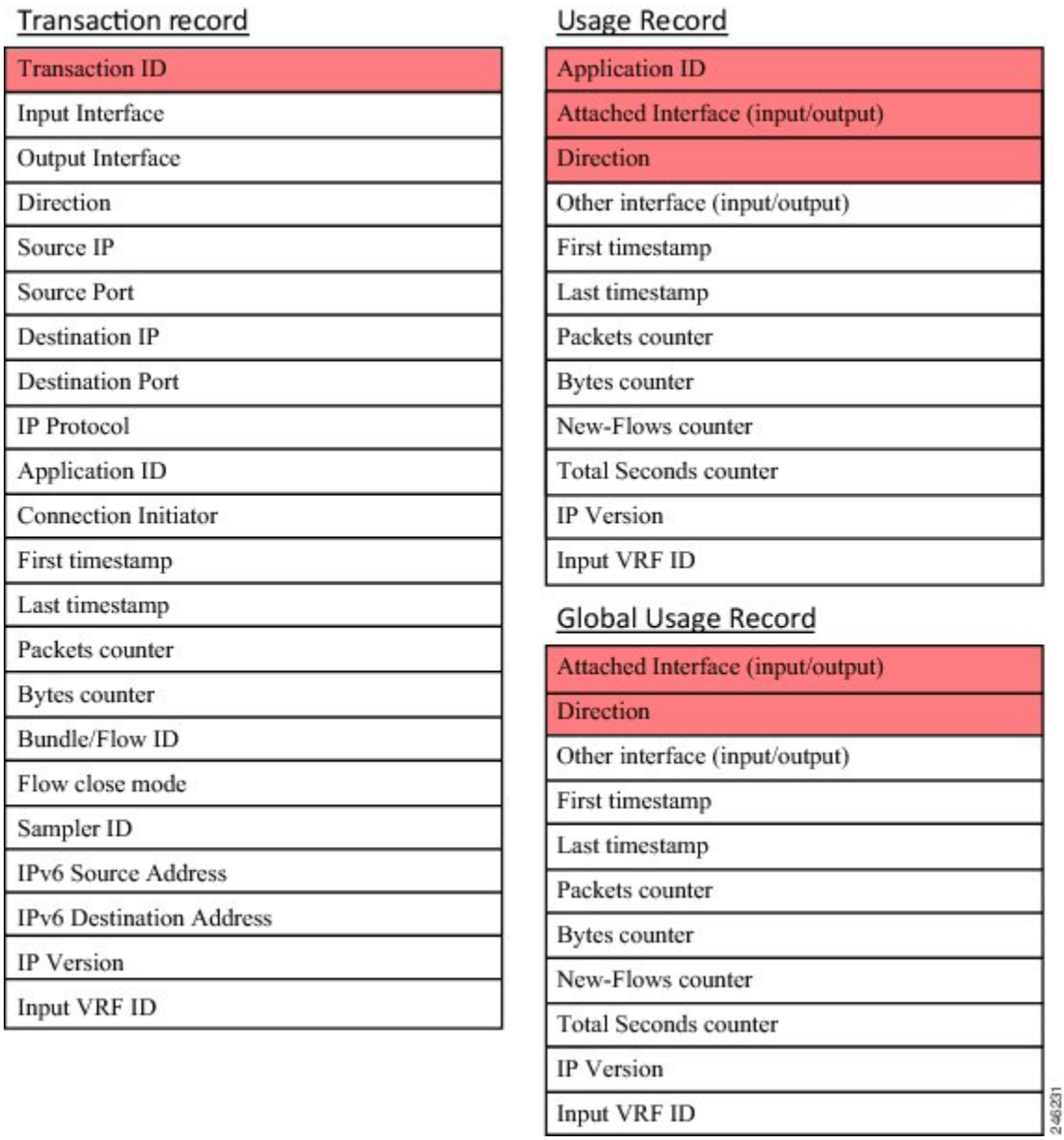
Cisco NetFlow export format Version 9 is a flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

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.

The figure below illustrates the packet fields used by the Transaction Records and Usage Records. The red fields are the key fields.

Figure 2: Packet Fields of Transaction Records and Usage Records



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

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.

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 policying, 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 the following table. 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

Embedded Services Processors	Maximum Flows	Default Flows	Memory Upper Limit (MB) (Equals 70% of the Platform Memory)
ESP40	3,500,000	1,000,000	716

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).
  - 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

How to Configure Cisco Application Visibility and Control

New Location of Configuration Procedures

This guide has been superceded by the AVC Solutions Guide, located at Cisco AVC Solution Guide for IOS XE Release 3.9S.

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 *Cisco IOS NetFlow Configuration Guide*	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	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	No new MIBs were created for this feature. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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

Feature Information for Support for AVC on Wireless LAN

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

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

Table 2: Feature Information for Support for AVC on Wireless LAN

Feature Name	Releases	Feature Information
Support for AVC on Wireless LAN	Cisco IOS XE Release 3.3SE	The Cisco Application Visibility and Control (AVC) solution for wireless networks identifies more than 1000 business– or consumer–class applications using deep packet inspection (DPI). The following commands are introduced or modified in the feature documented in this module: • **flow record** *record_name* • **flow exporter** *flow_exporter_name* • **flow monitor** *flow_monitor_name*

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.

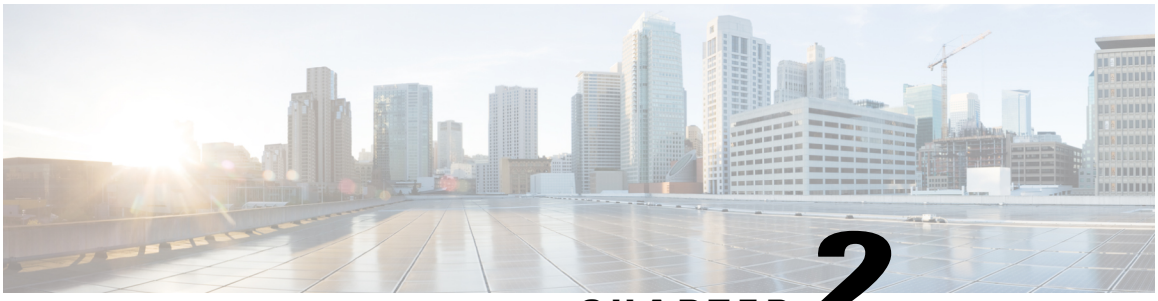
NetFlow sampler map —The definition of a set of properties (such as the sampling rate) for NetFlow sampling.

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.



CHAPTER 2

Easy Performance Monitor

The Easy Performance Monitor chapter describes how to configure Easy Performance Monitor (ezPM) for Application Visibility and Control (AVC).

- Finding Feature Information, page 13
- Information About Easy Performance Monitor, page 13
- How to Configure Easy Performance Monitor , page 15
- Configuration Examples for Configuring Easy Performance Monitor, page 17
- Additional References, page 29
- Feature Information for Easy Performance Monitor, page 30

Finding Feature Information

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

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

Information About Easy Performance Monitor

Easy Performance Monitor

The Easy Performance Monitor (Easy perf-mon or ezPM) feature provides an express method of provisioning monitors. This new mechanism adds functionality and does not affect the existing methods for provisioning monitors.

EzPM does not provide the full flexibility of the traditional perf-mon configuration model but provides 'profiles' that represent typical deployment scenarios. On selecting a profile and specifying a few parameters, ezPM provides the remaining provisioning information.

Profile

A profile is a pre-defined set of traffic monitors that contains default traffic monitor, and the traffic monitors can be enabled or disabled for a context. A profile also includes an exporter template. The following profiles are available for configuration:

- Application Experience
- Application Statistics

Traffic Monitor

A traffic monitor is a built-in definition of a perf-mon policy (that includes flow record, flow monitor, sampler, and monitor metrics) along with traffic classification on which it is activated.

Each traffic monitor defines the parameters that can be modified. While configuring the traffic monitor, the CLI displays the keywords based on the parameters that can be modified.

Traffic Monitors for Application Experience Profile

For an application experience profile, you can configure the following metrics:

- Application response time (ART) metrics and counters for TCP traffic
- Application level counters for DNS and DHT protocols
- Conversational level counters for IP traffic
- Media metrics and counters for rtp and telepresence media traffic
- URL information, ART metrics, and counters for sampled HTTP traffic.

For each of the metrics for a traffic monitor, you can configure the number of flow entries per cache, reduce the default traffic classification, and activate traffic monitor for IPv4 and IPv6 traffic. For media metrics, you can also activate the traffic monitor in ingress and egress directions.

Traffic Monitors for Application Statistics Profile

For an Application Statistics profile, the following traffic monitors are available for configuration:

- application-client-server-stats
- application-stats

The application statistics profile provides only application statistics and not performance statistics. The monitors operate on both IPv4 and IPv6 traffic. You can monitor either **application-client-server-stats** or

application-stats as the **application-client-server-stats** monitor provides the same information as that of **application-stats** along with additional information.

Context

A context represents a performance monitor policy map that is attached to an interface in ingress and egress directions. A context contains the information about the traffic-monitor that has to be enabled. When a context is attached to an interface, two policy-maps are created, one each in ingress and egress directions. Depending on the direction specified in the traffic monitor, the policy-maps are attached in that direction and the traffic is monitored. You can modify the context to override pre-defined directions.

You can create multiple contexts based on a single profile with different traffic monitors, different exporters, and different parameters for every selected traffic monitor.

An ezPM context can be attached to multiple interfaces.

A maximum of one (1) application experience profile context and three (3) application statistics profile contexts, for a total of four (4) contexts can be attached to a single interface.

You can modify the ezPM context only when the context is not attached to an interface. To detach the context from an interface, use the **no performance monitor context** *context-name* command.

How to Configure Easy Performance Monitor

Configuring Easy Performance Monitor

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **performance monitor context** *context-name* **profile** *profile-name*
4. **exporter destination** {*hostname* | *ipaddress*} **source interface** *interface-type number* [**port** *port-value* **transport udp vrf** *vrf-name*]
5. (Optional) Repeat Step 4 to configure additional exporters.
6. **traffic monitor** {**application-response-time** | **application-traffic-stats** | **conversation-traffic-stats** | **media** [**egress** | **ingress**] | **url**} [**cache-size** *max-entries*] [**cache-type** [**normal** | **synchronized**]] [[**class-and** | **class-replace**] *class-name*] [**ipv4** | **ipv6**] [**sampling-rate** *number*]
7. Repeat Step 6 to configure additional traffic monitor parameters.
8. **exit**
9. **interface** *interface-type number*
10. **performance monitor context** *context-name*
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**performance monitor context** *context-name* **profile** *profile-name* **Example:** `Device(config)# performance monitor context perf-mon-test profile application-experience`	Enters performance monitor configuration mode, creates a context with application-experience profile.
Step 4	**exporter destination** {*hostname* | *ipaddress*} **source interface** *interface-type number* [**port** *port-value* **transport udp vrf** *vrf-name*] **Example:** `Device(config-perf-mon)# exporter destination 10.1.1.1 source interface GigabitEthernet0/0/0 port 1 transport udp vrf vpn1`	Attaches the exporter to the context and configures exporter parameters.
Step 5	(Optional) Repeat Step 4 to configure additional exporters.	—
Step 6	**traffic monitor** {**application-response-time** | **application-traffic-stats** | **conversation-traffic-stats** | **media** [**egress** | **ingress**] | **url**} [**cache-size** *max-entries*] [**cache-type** [**normal** | **synchronized**]] [[**class-and** | **class-replace**] *class-name*] [**ipv4** | **ipv6**] [**sampling-rate** *number*] **Example:** `Device(config-perf-mon)# traffic monitor media egress cache-size 70 class-and cln ipv6`	Configures the traffic monitor to monitor the specified metrics. **Note** The **class-and** and **class-replace** keywords are not available for application-statistics profile.
Step 7	Repeat Step 6 to configure additional traffic monitor parameters.	—
Step 8	**exit** **Example:** `Device(config-perf-mon)# exit`	Exits performance monitor configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 9	**interface** *interface-type number* **Example:** `Device(config)# interface gigabitethernet 0/1/0`	Enters interface configuration mode.
Step 10	**performance monitor context** *context-name* **Example:** `Device(config-if)# performance monitor context perf-mon-test`	Configures the specified performance monitor context on the interface.
Step 11	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.

Configuration Examples for Configuring Easy Performance Monitor

Example: Configuring a Performance Monitor Context with Default ART, Media, and URL Traffic Monitors

The following example shows how to configure a performance monitor context to monitor the traffic metrics for ART, media, and URL:

```
Device# configure terminal
Device(config)# performance monitor context perf-mon-test profile application-experience
Device(config-perf-mon)# exporter destination 10.10.1.1 source interface GigabitEthernet0/0/0
 port 15 transport udp vrf in-vrf
Device(config-perf-mon)# traffic-monitor application-response-time
Device (config-perf-mon)# traffic-monitor media
Device(config-perf-mon)# traffic-monitor url
Device(config-perf-mon)# exit
```

Example: Configuring a Performance Monitor Context With Traffic Monitor Enabling the Media Metrics for Ipv6 Traffic in Ingress and Egress Directions

The following example shows how to configure a performance monitor context with traffic monitor enabling the media metrics for ipv6 traffic in ingress and egress directions:

```
Device# configure terminal
Device(config)# performance monitor context perf-mon-test profile application-experience
Device(config-perf-mon)# exporter destination 10.10.1.1 source interface GigabitEthernet0/0/0
 port 15 transport udp vrf in-vrf
Device(config-perf-mon)# traffic-monitor media ingress ipv6
Device(config-perf-mon)# traffic-monitor media egress ipv6
Device(config-perf-mon)# exit
```

Example: Configuring a Performance Monitor Context on Multiple Interfaces

The following example shows how to configure a performance monitor context on multiple interfaces:

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# performance monitor context perf-mon-test
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/2/0
Device(config-if)# performance monitor context perf-mon-test
Device(config-if)# exit
```

Example: Verifying the Complete Configuration for a Performance Monitor Context

The following example shows the complete underlying configuration of a performance monitor context that uses all traffic monitors. This configuration demonstrates how ezPM builds the configuration by applying the Application Experience profile definition to the context.

```
Device# show running-config performance monitor context reference

!
performance monitor context reference profile application-experience
exporter destination 5.4.3.2 source Ethernet0/0.1
traffic-monitor all
!
Device# show performance monitor context reference configuration

!================================================================================
! Equivalent Configuration of Context reference !
!================================================================================
!Exporters
!==========
!
flow exporter reference-1
description performance monitor context reference exporter
destination 5.4.3.2
source Ethernet0/0.1
transport udp 4739
export-protocol ipfix
template data timeout 300
option c3pl-class-table timeout 300
option c3pl-policy-table timeout 300
```

```
option interface-table timeout 300
option vrf-table timeout 300
option sampler-table timeout 300
option application-table timeout 300
option application-attributes timeout 300
option sub-application-table timeout 300
!
!Access Lists
!=============
ip access-list extended reference-conv_ipv4_tcp
permit tcp any any
!
ipv6 access-list reference-conv_ipv6_tcp
permit tcp any any
!
ip access-list extended reference-conv_ipv4_udp
permit udp any any
!
ipv6 access-list reference-conv_ipv6_udp
permit udp any any
!
ip access-list extended reference-art_ipv4_tcp
permit tcp any any
!
ipv6 access-list reference-art_ipv6_tcp
permit tcp any any
!
ip access-list extended reference-media_ipv4_udp
permit udp any any
!
ipv6 access-list reference-media_ipv6_udp
permit udp any any
!
ip access-list extended reference-url_ipv4_tcp
permit tcp any any
!
ipv6 access-list reference-url_ipv6_tcp
permit tcp any any
!
!Class-maps
!===========
class-map match-any reference-app_ts
match protocol dns
match protocol dht
!
class-map match-any reference-conv_ts_ipv4
match access-group name reference-conv_ipv4_tcp
match access-group name reference-conv_ipv4_udp
!
class-map match-any reference-conv_ts_ipv6
match access-group name reference-conv_ipv6_tcp
match access-group name reference-conv_ipv6_udp
!
class-map match-all reference-art_ipv4
match access-group name reference-art_ipv4_tcp
!
class-map match-all reference-art_ipv6
match access-group name reference-art_ipv6_tcp
!
class-map match-any reference-media_app
match protocol telepresence-media
match protocol rtp
!
class-map match-all reference-media_ipv4_in
match access-group name reference-media_ipv4_udp
match class-map reference-media_app
!
class-map match-all reference-media_ipv4_out
match access-group name reference-media_ipv4_udp
match class-map reference-media_app
!
class-map match-all reference-media_ipv6_in
match access-group name reference-media_ipv6_udp
```

```
match class-map reference-media_app
!
class-map match-all reference-media_ipv6_out
match access-group name reference-media_ipv6_udp
match class-map reference-media_app
!
class-map match-any reference-url_app
match protocol napster
match protocol gotomypc
match protocol yahoo-messenger
match protocol tunnel-http
match protocol baidu-movie
match protocol flashmyspace
match protocol directconnect
match protocol audio-over-http
match protocol skype
match protocol video-over-http
match protocol pando
match protocol flashyahoo
match protocol msn-messenger
match protocol flash-video
match protocol webthunder
match protocol vnc-http
match protocol activesync
match protocol irc
match protocol realmedia
match protocol gmail
match protocol google-earth
match protocol gnutella
match protocol rtmpt
match protocol http
match protocol ms-update
match protocol rtsp
match protocol http-alt
match protocol share-point
match protocol binary-over-http
match protocol ms-sms
match protocol megavideo
!
class-map match-all reference-url_ipv4
match access-group name reference-url_ipv4_tcp
match class-map reference-url_app
!
class-map match-all reference-url_ipv6
match access-group name reference-url_ipv6_tcp
match class-map reference-url_app
!
class-map match-all reference-art_url_ipv4
match class-map reference-art_ipv4
match class-map reference-url_ipv4
!
class-map match-all reference-art_url_ipv6
match class-map reference-art_ipv6
match class-map reference-url_ipv6
!
!Samplers
!=========
!Records and Monitors
!=====================
!
flow record type performance-monitor reference-app_ts_in
description ezPM record
match routing vrf input
match ipv4 version
match ipv4 protocol
match interface input
match flow direction
match application name account-on-resolution
collect ipv4 dscp
collect interface output
collect counter bytes long
collect counter packets
collect timestamp sys-uptime first
```

```
collect timestamp sys-uptime last
collect connection new-connections
collect connection sum-duration
!
!
flow monitor type performance-monitor reference-app_ts_in
record reference-app_ts_in
exporter reference-1
cache entries 1000
cache timeout synchronized 60
!
!
flow record type performance-monitor reference-app_ts_out
description ezPM record
match routing vrf input
match ipv4 version
match ipv4 protocol
match interface output
match flow direction
match application name account-on-resolution
collect ipv4 dscp
collect interface input
collect counter bytes long
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect connection new-connections
collect connection sum-duration
!
!
flow monitor type performance-monitor reference-app_ts_out
record reference-app_ts_out
exporter reference-1
cache entries 1000
cache timeout synchronized 60
!
!
flow record type performance-monitor reference-conv_ts_ipv4
description ezPM record
match routing vrf input
match ipv4 protocol
match application name account-on-resolution
match connection client ipv4 address
match connection server ipv4 address
match connection server transport port
collect ipv4 dscp
collect ipv4 ttl
collect interface input
collect interface output
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect connection new-connections
collect connection sum-duration
collect connection server counter bytes long
collect connection server counter packets long
collect connection client counter bytes long
collect connection client counter packets long
!
!
flow monitor type performance-monitor reference-conv_ts_ipv4
record reference-conv_ts_ipv4
exporter reference-1
cache entries 6250
cache timeout synchronized 60 export-spread 15
!
!
flow record type performance-monitor reference-conv_ts_ipv6
description ezPM record
match routing vrf input
match ipv6 protocol
match application name account-on-resolution
match connection client ipv6 address
match connection server transport port
```

```
match connection server ipv6 address
collect ipv6 dscp
collect ipv6 hop-limit
collect interface input
collect interface output
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect connection new-connections
collect connection sum-duration
collect connection server counter bytes long
collect connection server counter packets long
collect connection client counter bytes long
collect connection client counter packets long
!
!
flow monitor type performance-monitor reference-conv_ts_ipv6
record reference-conv_ts_ipv6
exporter reference-1
cache entries 6250
cache timeout synchronized 60 export-spread 15
!
!
flow record type performance-monitor reference-art_ipv4
description ezPM record
match routing vrf input
match ipv4 protocol
match application name account-on-resolution
match connection client ipv4 address
match connection server ipv4 address
match connection server transport port
collect ipv4 dscp
collect ipv4 ttl
collect interface input
collect interface output
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect connection new-connections
collect connection sum-duration
collect connection delay response to-server sum
collect connection server counter responses
collect connection delay response to-server histogram late
collect connection delay network to-server sum
collect connection delay network to-client sum
collect connection client counter packets retransmitted
collect connection delay network client-to-server sum
collect connection delay application sum
collect connection delay application max
collect connection delay response client-to-server sum
collect connection transaction duration sum
collect connection transaction counter complete
collect connection server counter bytes long
collect connection server counter packets long
collect connection client counter bytes long
collect connection client counter packets long
!
!
flow monitor type performance-monitor reference-art_ipv4
record reference-art_ipv4
exporter reference-1
cache entries 2250
cache timeout synchronized 60 export-spread 15
!
!
flow record type performance-monitor reference-art_ipv6
description ezPM record
match routing vrf input
match ipv6 protocol
match application name account-on-resolution
match connection client ipv6 address
match connection server transport port
match connection server ipv6 address
collect ipv6 dscp
collect ipv6 hop-limit
```

```
collect interface input
collect interface output
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect connection new-connections
collect connection sum-duration
collect connection delay response to-server sum
collect connection server counter responses
collect connection delay response to-server histogram late
collect connection delay network to-server sum
collect connection delay network to-client sum
collect connection client counter packets retransmitted
collect connection delay network client-to-server sum
collect connection delay application sum
collect connection delay application max
collect connection delay response client-to-server sum
collect connection transaction duration sum
collect connection transaction counter complete
collect connection server counter bytes long
collect connection server counter packets long
collect connection client counter bytes long
collect connection client counter packets long
!
!
flow monitor type performance-monitor reference-art_ipv6
record reference-art_ipv6
exporter reference-1
cache entries 2250
cache timeout synchronized 60 export-spread 15
!
!
flow record type performance-monitor reference-media_ipv4_in
description ezPM record
match routing vrf input
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport rtp ssrc
match interface input
collect ipv4 dscp
collect ipv4 ttl
collect transport packets lost counter
collect transport rtp jitter maximum
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 transport rtp payload-type
collect transport rtp jitter mean sum
!
!
flow monitor type performance-monitor reference-media_ipv4_in
record reference-media_ipv4_in
exporter reference-1
cache entries 4000
cache timeout synchronized 60 export-spread 15
!
!
flow record type performance-monitor reference-media_ipv6_in
description ezPM record
match routing vrf input
match ipv6 protocol
match ipv6 source address
match ipv6 destination address
match transport source-port
match transport destination-port
match transport rtp ssrc
match interface input
```

```
collect ipv6 dscp
collect ipv6 hop-limit
collect transport packets lost counter
collect transport rtp jitter maximum
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 transport rtp payload-type
collect transport rtp jitter mean sum
!
!
flow monitor type performance-monitor reference-media_ipv6_in
record reference-media_ipv6_in
exporter reference-1
cache entries 4000
cache timeout synchronized 60 export-spread 15
!
!
flow record type performance-monitor reference-media_ipv4_out
description ezPM record
match routing vrf input
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport rtp ssrc
match interface output
collect ipv4 dscp
collect ipv4 ttl
collect transport packets lost counter
collect transport rtp jitter maximum
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 transport rtp payload-type
collect transport rtp jitter mean sum
!
!
flow monitor type performance-monitor reference-media_ipv4_out
record reference-media_ipv4_out
exporter reference-1
cache entries 4000
cache timeout synchronized 60 export-spread 15
!
!
flow record type performance-monitor reference-media_ipv6_out
description ezPM record
match routing vrf input
match ipv6 protocol
match ipv6 source address
match ipv6 destination address
match transport source-port
match transport destination-port
match transport rtp ssrc
match interface output
collect ipv6 dscp
collect ipv6 hop-limit
collect transport packets lost counter
collect transport rtp jitter maximum
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 transport rtp payload-type
collect transport rtp jitter mean sum
!
!
flow monitor type performance-monitor reference-media_ipv6_out
record reference-media_ipv6_out
exporter reference-1
cache entries 4000
cache timeout synchronized 60 export-spread 15
!
!
flow record type performance-monitor reference-url_ipv4
description ezPM record
match routing vrf input
match ipv4 protocol
match application name account-on-resolution
match connection client ipv4 address
match connection server ipv4 address
match connection server transport port
collect ipv4 dscp
collect ipv4 ttl
collect interface input
collect interface output
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect connection new-connections
collect connection sum-duration
collect application http uri statistics
collect connection delay response to-server sum
collect connection server counter responses
collect connection delay response to-server histogram late
collect connection delay network to-server sum
collect connection delay network to-client sum
collect connection client counter packets retransmitted
collect connection delay network client-to-server sum
collect connection delay application sum
collect connection delay application max
collect connection delay response client-to-server sum
collect connection transaction duration sum
collect connection transaction counter complete
collect connection server counter bytes long
collect connection server counter packets long
collect connection client counter bytes long
collect connection client counter packets long
collect application http host
!
!
flow monitor type performance-monitor reference-url_ipv4
record reference-url_ipv4
exporter reference-1
cache entries 1000
cache timeout synchronized 60 export-spread 15
!
!
flow record type performance-monitor reference-url_ipv6
description ezPM record
match routing vrf input
match ipv6 protocol
match application name account-on-resolution
match connection client ipv6 address
match connection server transport port
match connection server ipv6 address
collect ipv6 dscp
collect ipv6 hop-limit
collect interface input
collect interface output
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect connection new-connections
collect connection sum-duration
collect application http uri statistics
```

```
collect connection delay response to-server sum
collect connection server counter responses
collect connection delay response to-server histogram late
collect connection delay network to-server sum
collect connection delay network to-client sum
collect connection client counter packets retransmitted
collect connection delay network client-to-server sum
collect connection delay application sum
collect connection delay application max
collect connection delay response client-to-server sum
collect connection transaction duration sum
collect connection transaction counter complete
collect connection server counter bytes long
collect connection server counter packets long
collect connection client counter bytes long
collect connection client counter packets long
collect application http host
!
!
flow monitor type performance-monitor reference-url_ipv6
record reference-url_ipv6
exporter reference-1
cache entries 1000
cache timeout synchronized 60 export-spread 15
!
!Policy-maps
!============
policy-map type performance-monitor reference-in
parameter default account-on-resolution
class reference-app_ts
flow monitor reference-app_ts_in
class reference-art_url_ipv4
flow monitor reference-url_ipv4
class reference-art_url_ipv6
flow monitor reference-url_ipv6
class reference-art_ipv4
flow monitor reference-art_ipv4
class reference-art_ipv6
flow monitor reference-art_ipv6
class reference-url_ipv4
flow monitor reference-url_ipv4
class reference-url_ipv6
flow monitor reference-url_ipv6
class reference-media_ipv4_in
flow monitor reference-media_ipv4_in
class reference-media_ipv6_in
flow monitor reference-media_ipv6_in
class reference-conv_ts_ipv4
flow monitor reference-conv_ts_ipv4
class reference-conv_ts_ipv6
flow monitor reference-conv_ts_ipv6
!
policy-map type performance-monitor reference-out
parameter default account-on-resolution
class reference-app_ts
flow monitor reference-app_ts_out
class reference-art_url_ipv4
flow monitor reference-url_ipv4
class reference-art_url_ipv6
flow monitor reference-url_ipv6
class reference-art_ipv4
flow monitor reference-art_ipv4
class reference-art_ipv6
flow monitor reference-art_ipv6
class reference-url_ipv4
flow monitor reference-url_ipv4
class reference-url_ipv6
flow monitor reference-url_ipv6
class reference-media_ipv4_out
flow monitor reference-media_ipv4_out
class reference-media_ipv6_out
flow monitor reference-media_ipv6_out
class reference-conv_ts_ipv4
```

```
flow monitor reference-conv_ts_ipv4
class reference-conv_ts_ipv6
flow monitor reference-conv_ts_ipv6
!
!Interface Attachments
!======================
interface Ethernet0/0
service-policy type performance-monitor input reference-in
service-policy type performance-monitor output reference-out
!
```

Example: Verifying the Configuration of a Conversation Level Traffic Monitor Metrics for a Performance Monitor Context

The following example from the **show running-configuration performance monitor context** command that displays the conversation level traffic monitor metrics configured on the performance monitor:

```
Device# show running-configuration performance monitor context conv

!================================================================================
! Equivalent Configuration of Context conv !
!================================================================================
!Exporters
!==========
!
flow exporter conv-1
description performance monitor context conv exporter
destination 5.4.3.2
source Ethernet0/0
transport udp 4739
export-protocol ipfix
template data timeout 300
option c3pl-class-table timeout 300
option c3pl-policy-table timeout 300
option interface-table timeout 300
option vrf-table timeout 300
option sampler-table timeout 300
option application-table timeout 300
option application-attributes timeout 300
option sub-application-table timeout 300
!
!Access Lists
!=============
ip access-list extended conv-conv_ipv4_tcp
permit tcp any any
!
ipv6 access-list conv-conv_ipv6_tcp
permit tcp any any
!
ip access-list extended conv-conv_ipv4_udp
permit udp any any
!
ipv6 access-list conv-conv_ipv6_udp
permit udp any any
!
!Class-maps
!===========
class-map match-any conv-conv_ts_ipv4
match access-group name conv-conv_ipv4_tcp
match access-group name conv-conv_ipv4_udp
!
class-map match-any conv-conv_ts_ipv6
match access-group name conv-conv_ipv6_tcp
match access-group name conv-conv_ipv6_udp
!
```

```
!Samplers
!=========
!Records and Monitors
!=====================
!
flow record type performance-monitor conv-conv_ts_ipv4
description ezPM record
match routing vrf input
match ipv4 protocol
match application name account-on-resolution
match connection client ipv4 address
match connection server ipv4 address
match connection server transport port
collect ipv4 dscp
collect ipv4 ttl
collect interface input
collect interface output
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect connection new-connections
collect connection sum-duration
collect connection server counter bytes long
collect connection server counter packets long
collect connection client counter bytes long
collect connection client counter packets long
!
!
flow monitor type performance-monitor conv-conv_ts_ipv4
record conv-conv_ts_ipv4
exporter conv-1
cache entries 6250
cache timeout synchronized 60 export-spread 15
!
!
flow record type performance-monitor conv-conv_ts_ipv6
description ezPM record
match routing vrf input
match ipv6 protocol
match application name account-on-resolution
match connection client ipv6 address
match connection server transport port
match connection server ipv6 address
collect ipv6 dscp
collect ipv6 hop-limit
collect interface input
collect interface output
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect connection new-connections
collect connection sum-duration
collect connection server counter bytes long
collect connection server counter packets long
collect connection client counter bytes long
collect connection client counter packets long
!
!
flow monitor type performance-monitor conv-conv_ts_ipv6
record conv-conv_ts_ipv6
exporter conv-1
cache entries 6250
cache timeout synchronized 60 export-spread 15
!
!Policy-maps
!============
policy-map type performance-monitor conv-in
parameter default account-on-resolution
class conv-conv_ts_ipv4
flow monitor conv-conv_ts_ipv4
class conv-conv_ts_ipv6
flow monitor conv-conv_ts_ipv6
!
policy-map type performance-monitor conv-out
parameter default account-on-resolution
```

```
class conv-conv_ts_ipv4
flow monitor conv-conv_ts_ipv4
class conv-conv_ts_ipv6
flow monitor conv-conv_ts_ipv6
!
!Interface Attachments
!=====================
interface Ethernet0/1
service-policy type performance-monitor input conv-in
service-policy type performance-monitor output conv-out
```

Example: Configuring a Performance Monitor Context With Application Statistics Profile

The following example shows how to configure a performance monitor context with traffic monitor enabling per interface, application, client, and server statistics:

```
Device# configure terminal
Device(config)# performance monitor context perf-mon-test profile application-statistics
Device(config-perf-mon)# traffic-monitor application-client-server-stats cache-size 755
cache-type synchronized ipv6
Device(config-perf-mon)# exit
Device(config)# interface gigabitethernet 0/1
Device(config-if)# performance monitor context perf-mon-test
Device(config-if)# exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco Application Visibility and Control User Guide	Cisco Application Visibility and Control User Guide for Cisco IOS XE Release 3.11S and Cisco IOS Release15.4(1)T. Cisco Application Visibility and Control User Guide for Cisco IOS XE Release 3.12S and Cisco IOS Release15.4(2)T. Cisco Application Visibility and Control User Guide for Cisco IOS XE Release 3.13S and Cisco IOS Release15.4(3)T.

Technical Assistance

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

Feature Information for Easy Performance Monitor

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

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

Table 3: Feature Information for Easy Performance Monitor

Feature Name	Releases	Feature Information
Easy Performance Monitor	Cisco IOS XE Release 3.10S	The Easy Performance Monitor chapter describes how to configure Easy Performance Monitor (ezPM) for Application Visibility and Control (AVC). This feature was introduced.
Easy Performance Monitor Phase II	Cisco IOS XE Release 3.12S	The following command was modified: **traffic monitor** The **sampler** keyword was added.
Adaptive AVC Reporting	Cisco IOS XE Release 3.13S	The support for Application Statistics profile was added. The following command was modified: **performance monitor** The **application-statistics** keyword was added.