



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 Availability 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This guide has been superseded by the AVC Solutions Guide, located at [Cisco AVC Solution Guide for IOS XE Release 3.9S](#).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](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 Availability and Control

Components of an Application Visibility and Control Network

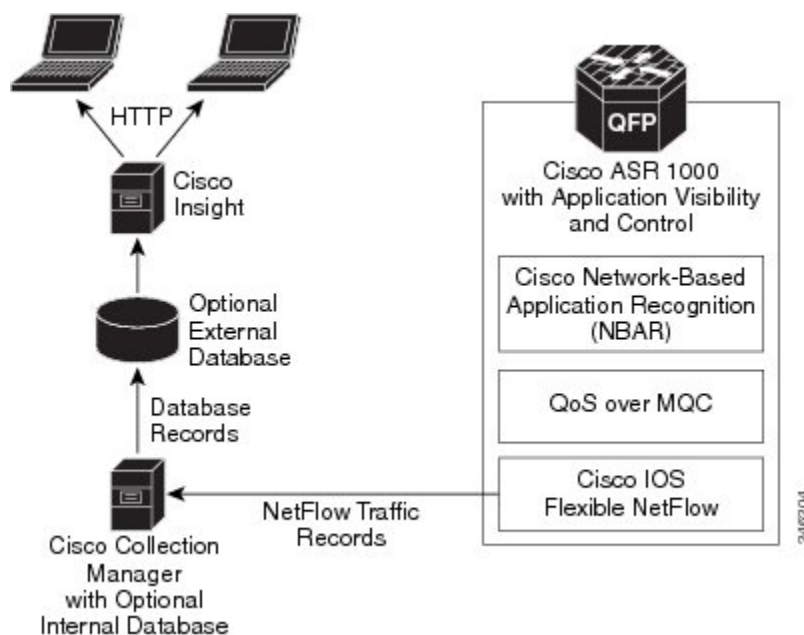
The following internal and external components of an Application Visibility and Control network are described in detail in this section.

- 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

<u>Transaction record</u>		<u>Usage Record</u>	
Transaction ID		Application ID	
Input Interface		Attached Interface (input/output)	
Output Interface		Direction	
Direction		Other interface (input/output)	
Source IP		First timestamp	
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		<u>Global Usage Record</u>	
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	

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 superseded 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 <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	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	<p>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).</p> <p>The following commands are introduced or modified in the feature documented in this module:</p> <ul style="list-style-type: none"> • flow record <i>record_name</i> • flow exporter <i>flow_exporter_name</i> • flow monitor <i>flow_monitor_name</i>

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.

