Technology Overview

This overview of AVC technology includes the following topics:

Overview

The Cisco Application Visibility and Control (AVC) solution leverages multiple technologies to recognize, analyze, and control over 1000 applications, including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. AVC combines several Cisco IOS/IOS XE components, as well as communicating with external tools, to integrate the following functions into a powerful solution.

- **Application Recognition**

  Operating on Cisco IOS and Cisco IOS XE, NBAR2 utilizes innovative deep packet inspection (DPI) technology to identify a wide variety of applications within the network traffic flow, using L3 to L7 data.

  NBAR2 can monitor over 1000 applications, and supports Protocol Pack updates for expanding application recognition, without requiring IOS upgrade or router reload.

- **Metrics Collection and Exporting**

  Metric providers, an embedded monitoring agent, and Flexible NetFlow combine to provide a wide variety of network metrics data. The monitoring agent collects:

  - TCP performance metrics such as bandwidth usage, response time, and latency.
  - RTP performance metrics such as packet loss and jitter.

  Performance metrics can be measured at multiple points within the router.

  Metrics are aggregated and exported in NetFlow v9 or IPFIX format to a management and reporting package. Metrics records are sent out directly from the data plane when possible, to maximize system performance. When more complex processing is required, such as when the router is maintaining a history of exported records, records may be exported by the route processor, which is slower than direct export from the data plane.

- **Management and Reporting Systems**

  Management and reporting systems, such as Cisco Prime Infrastructure or third-party tools, receive the network metrics data in Netflow v9 or IPFIX format, and provide a wide variety of system management and reporting functions. These functions include configuring metrics reporting, creating application and network performance reports, system provisioning, configuring alerts, and assisting in troubleshooting.

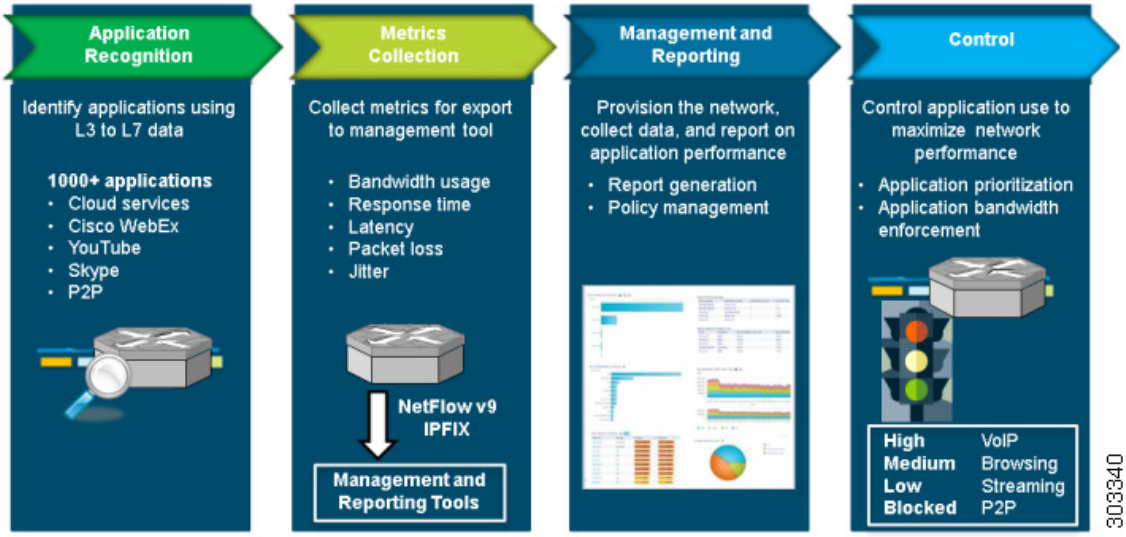
  Using the Cisco Prime Infrastructure management console, an administrator can configure each router in the network remotely using a GUI.

- **Control**

  Administrators can use industry-leading Quality of Service (QoS) capabilities to control application prioritization, manage application bandwidth, and so on. Cisco QoS employs the same deep packet inspection (DPI) technology used by NBAR2, to enable Cisco routers to reprioritize critical applications and enforce application bandwidth use.

Figure 2-1 provides a high level overview the functions of the Cisco AVC solution.

Figure 2-1 Functional Overview of the Cisco AVC Solution



AVC Features and Capabilities

Table 2-1 describes individual Cisco AVC solution features and their availability on Cisco IOS and Cisco IOS XE platforms. For a release-by-release history of AVC features and enhancements, see Appendix B, "AVC Feature History".

Table 2-1 AVC Features

Feature	Description	Available on IOS Platforms[1]	Available on IOS XE Platforms[2]
General			
Unified Solution	Cisco AVC combines application recognition, advanced metrics collection, sophisticated reporting, and network traffic control and optimization technologies into a unified solution.	Yes	Release 3.4S and later
Native IPv6 Support	Cisco AVC supports both IPv4 and IPv6.	Yes	Release 3.5S and later
Tunneled IPv6 Support	Support for tunneled IPv6 traffic.	Yes	Yes
Support on a wide range of Cisco routers operating with Cisco IOS and Cisco IOS XE	For details about supported platforms and feature activation, see: AVC Supported Platforms, page A-1 AVC Licensed Features (Legacy), page C-1	Yes	Yes
NBAR Interoperability with Cisco GET VPN	For information, see NBAR Interoperability with Cisco GET VPN, page 2-15.	—	Release 3.11S and later
AVC Interoperability with Cisco GET VPN	For information, see AVC Interoperability with Cisco GET VPN, page 2-16.	—	Release 3.12S and later
Adaptive AVC	Provides a mode with more limited application classification and reporting, for performance optimization. For information, see Adaptive AVC Reporting, page 2-17.	Release 15.4(3)T and later	Release 3.13S and later
Compatibility with L2 Transparent Mode (Local Switching)	A router operating in layer 2 transparent mode (local switching) bridges two interfaces, transparently forwarding packets directly from one interface to the other, without any other routing functionality. AVC can operate on a device configured in this mode, providing full AVC functionality on the bridged traffic. See AVC Compatibility with Layer 2 Transparent Mode, page A-3.	—	3.15S
Application Recognition			
Network Based Application Recognition 2 (NBAR2)	Provides application recognition. Uses an innovative deep packet inspection (DPI) technology to identify a wide variety of applications within the network traffic flow, using L3 to L7 data. NBAR2 can monitor over 1000 applications.	Yes	3.4S

Feature	Description	Available on IOS Platforms[1]	Available on IOS XE Platforms[2]
Protocol Pack updates	Expands NBAR2 application recognition without requiring IOS upgrade or router reload.	Yes	3.4S
Two levels of NBAR operation	NBAR2 can operate in fine-grain or coarse-grain modes. Fine-grain mode provides NBAR's full application recognition capabilities. Coarse-grain mode offers a performance advantage by minimizing deep packet inspection, and can be used in scenarios where the full power of fine-grain classification is not required. For information, see NBAR2 Fine-grain and Coarse-grain Modes, page 4-19.	Release 15.5(1)T and later	Release 3.14S and later
Metrics Collection			
Accounting	• Accounting of all metrics is performed by Flexible NetFlow (FNF) and the IPFIX exporter. • Multiple parallel monitors with overlapping data for the same traffic are permitted. • Flexible record keys provide different aggregation schemes for different traffic types.	Yes	3.4S
Account on Resolution (AOR)	Account-On-Resolution configures FNF to collect data in a temporary memory location until the record key fields are resolved. After resolution of the record key fields, FNF combines the temporary data collected with the standard FNF records. Account-on-resolution is useful when the field used as a key is not available at the time that FNF receives the first packet. When using Account-On-Resolution: • Flows ended before resolution are not reported. • On Cisco IOS XE platforms, FNF packet/octet counters, timestamp, and TCP performance metrics are collected until resolution. All other field values are taken from the packet that provides resolution or the following packets.	Yes	3.4S
Traffic Filtering	A policy-map defined in Cisco Common Classification Policy Language (C3PL) filters the traffic to be reported. Traffic filters operate separately from other types of policy-maps employed in the system.	Yes	3.4S
Interoperability with Cisco AppNav	Cisco AppNav is the Wide Area Application Services (WAAS) diversion mechanism. AVC provides statistics before and after the AppNav WAAS service controller (AppNav SC), as well as inspecting and reporting application information on optimized traffic. For more information about Cisco AppNav, see: http://www.cisco.com/en/US/prod/collateral/contnetw/ps5680/ps6474/white_paper_c11-705318.html	—	3.4S

Feature	Description	Available on IOS Platforms[1]	Available on IOS XE Platforms[2]
Packet Capture	Cisco Embedded Packet Capture (EPC) technology performs packet capture. For more information about Cisco EPC, see: http://www.cisco.com/en/US/products/ps9913/products_ios_protocol_group_home.html	—	3.4S
Reporting on Individual Transactions	Flexible NetFlow (FNF) monitors can report on individual transactions within a flow. This enables greater resolution for traffic metrics. For more information, see: Connection/Transaction Metrics, page 4-43	—	3.9S
QoS Metrics	Cisco AVC provides monitors to collect metrics related to Quality of Service (QoS) policy. Monitors can indicate: • Packets dropped on an interface, per QoS queue, due to a QoS policy that limits resources available to a specific type of traffic. • Class hierarchy (indicating traffic priority) of a reported flow, as determined by the QoS policy map. For more information, see: QoS Metrics: Cisco IOS XE Platforms, page 4-37	Yes	3.4S
Easy Performance Monitor Configuration	The Easy Performance Monitor ("Easy perf-mon" or "ezPM") feature provides an "express" method of provisioning monitors. Easy perf-mon provides "profiles" that represent typical deployment or use-case scenarios. After a user selects a profile and specifies a small number of parameters, Easy perf-mon provides the remaining provisioning details. For more information, see: Easy Performance Monitor (ezPM), page 4-4	15.4(1)T	3.10S
Customizing attribute values	See Customizing Attribute Values, page 4-30.	15.4(1)T	3.11S
Management and Reporting			
Cisco Prime Infrastructure 2.0 or later	The Cisco Prime Infrastructure management and reporting system is an integral part of the Cisco AVC solution and provides extensive management and reporting features, including provisioning the system, storing exported data, and generating reports. For more information about Cisco Prime Infrastructure, see: http://www.cisco.com/en/US/products/ps12239/index.html	Yes	3.4S

Feature	Description	Available on IOS Platforms[1]	Available on IOS XE Platforms[2]
Management and reporting products available from Cisco certified partners.	For information, see the Cisco Developer Network Solutions Catalog: http://marketplace.cisco.com/catalog 1. Select **Technology**. 2. In the **Technologies** list, select **Application Visibility and Control**. 3. Click **Find Solution**. A list of partner solutions appears. A **Cisco Compatible** logo indicates that the solution has passed compatibility tests with AVC. **Note** Operation of Solutions Catalog page is subject to change.	Yes	Yes

Feature	Description	Available on IOS Platforms[1]	Available on IOS XE Platforms[2]
Control			
Cisco Quality of Service (QoS)	See: • Cisco Quality of Service (QoS) • QoS Example 1: Control and Throttle Traffic, page 4-55 • QoS Example 2: Assigning Priority and Allocating Bandwidth, page 4-55	Yes	Yes

1. Applicable prior to Cisco IOS release 15.4(1)T where not specified.
2. Applicable prior to Cisco IOS XE release 3.11S where not specified.

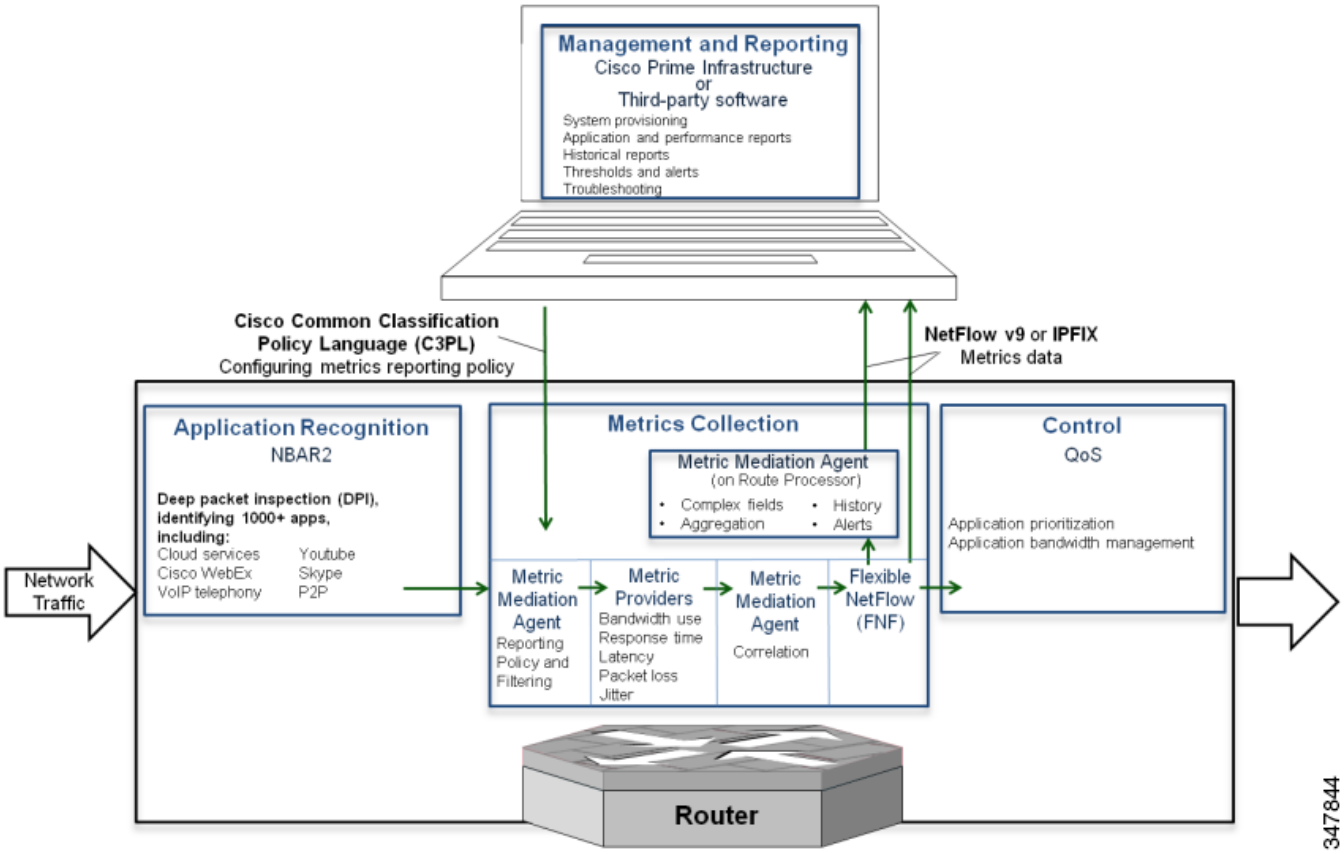
AVC Architecture

The following Cisco AVC components are described in this section:

- NBAR2, page 2-8
- Metric Mediation Agent, page 2-9
- Metric Providers, page 2-9
- Flexible NetFlow, page 2-10
- QoS, page 2-10
- Embedded Packet Capture, page 2-10
- Common Flow Table, page 2-10
- Management and Reporting Systems, page 2-11

Figure 2-2 describes the components in the Cisco AVC architecture.

Figure 2-2 AVC Architecture for Cisco IOS and Cisco IOS XE



NBAR2

Network Based Application Recognition 2 (NBAR2) provides native stateful deep packet inspection (DPI) capabilities. NBAR2 is the next generation of NBAR, enhancing the application recognition engine to support more than 1000 applications.

Note NBAR2 functionality requires an advanced license. See AVC Licensed Features (Legacy), page C-1.

NBAR2 provides powerful capabilities, including:

- Categorizing applications into meaningful terms, such as category, sub-category, application group, and so on. This categorization simplifies report aggregation and control configuration.
- Field extraction of data such as HTTP URL, SIP domain, mail server, and so on. The extracted application information can be used for classification or can be exported by IPFIX to the collector for creating reports.
- Customized definition of applications, based on ports, payload values, or URL/Host of HTTP traffic.
- The set of attributes for each protocol can be customized.

Additional Application Protocol Definitions

With NBAR2 Protocol Packs, new and updated application signatures can be loaded into a router without upgrading the software image. Major protocol packs providing new and updated signatures are released periodically. Minor protocol packs are released between major releases; they provide updates and bug fixes. For information about protocol pack support, see: http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

In addition to the predefined application protocols, you can create customized application definitions based on ports, payload values, or URL/Host of the HTTP traffic. Protocol attributes, such as application categorization, sub-categorization, application group, and so on, can also be customized.

For more information, see: http://www.cisco.com/go/nbar

Metric Mediation Agent

Cisco IOS Platforms	Cisco IOS XE Platforms
Added in release 15.4(1)T. Prior to this release, on Cisco IOS platforms, Cisco AVC made use of the Measurement, Aggregation, and Correlation Engine (MACE). Beginning with the current release, MMA replaces MACE functionality. AVC continues to support MACE, but users are encouraged to migrate to MMA. For links to information about MACE configuration, see Appendix D, “References”.	Added in release 3.8S.

The Metric Mediation Agent (MMA) manages, correlates, and aggregates metrics from different metric providers. It provides the following functions:

- Controls traffic monitoring and filtering policy.
- Correlates data from multiple metric providers (see Metric Providers, page 2-9) into the same record.
- Aggregates metrics.
- Supports history and alert functions. This requires sending the metrics records to the route processor (RP) before exporting them to the management and reporting tools.

Metric Providers

Metric providers collect and calculate metrics and provide them to the Metric Mediation Agent (MMA) for correlation. There are a variety of metric providers: some collect simple, stateless metrics per packet, while other more complex metric providers track states and collect metrics per flow, transforming the metrics at the time of export and making sophisticated calculations. These transformations may require punting of records to the route processor (RP) before the metrics are exported to the management and reporting system.

The MMA compiles multiple metric providers of different types into the same record (see Metric Mediation Agent, page 2-9).

Flexible NetFlow

Netflow/IPFIX is the industry standard for acquiring operational data from IP networks to enable network planning, monitoring traffic analysis, and IP accounting. Flexible NetFlow (FNF) enables customizing traffic analysis parameters according to specific requirements. The AVC solution is compatible with NetFlow v9 (RFC-3954) and IPFIX (RFC-5101).

For more information, see: http://www.cisco.com/go/fnf

QoS

Cisco Quality of Service (QoS) provides prioritization, shaping, and rate-limiting of traffic. QoS can place designated applications into specific QoS classes/queues. This enables:

- Placing high priority, latency-sensitive traffic into a priority queue.
- Guaranteeing a minimum bandwidth for an individual application or for a group of applications within a QoS traffic class.

Similarly, QoS can also be used for “policing” or managing non-enterprise, recreational applications such as YouTube and Facebook.

The Cisco AVC solution integrates QoS functionality with NBAR2. QoS can use application information provided by NBAR2 in managing network traffic. The QoS class-map statements enable matching to NBAR2-supported applications and L7 application fields (such as HTTP URL or Host), as well as to NBAR2 attributes. Class-map statements can coexist with all other traditional QoS match attributes, such as IP, subnet, and DSCP.

For more information, see: http://www.cisco.com/go/qos

Embedded Packet Capture

Cisco IOS Platforms	Cisco IOS XE Platforms
Not available	Added in release 3.8S

Embedded Packet Capture (EPC) enables capturing the entire traffic for a given traffic class. The capture is limited only by available memory. The management and reporting system can read packets captured as a packet capture (pcap) file.

For more information, see: http://www.cisco.com/go/epc

Common Flow Table

The Common Flow Table (CFT) manages L4 connections and enables storing and retrieving states for each flow. Using a common flow table optimizes use of system memory and improves performance by storing and running data for each flow only once. The CFT standardizes flow management across the entire system.

Management and Reporting Systems

Cisco AVC operates with a variety of management and reporting systems.

- **Cisco Prime Infrastructure Management and Reporting**—For additional information, see Cisco Prime Infrastructure, page 2-11.
- **Third-Party Management and Reporting Solutions**—Cisco certifies solutions for AVC through the Cisco Developer Network. For a list of certified third-party management solutions, see the Cisco Developer Network Solutions Catalog:

  1. Navigate to http://marketplace.cisco.com/catalog
  2. Select **Technology**.
  3. In the **Technologies** list, select **Application Visibility and Control**.
  4. Click **Find Solution**. A list of partner solutions appears. A **Cisco Compatible** logo indicates that the solution has passed compatibility tests with AVC.

Note Operation of the Solutions Catalog page is subject to change.

Cisco Prime Infrastructure

Cisco Prime Infrastructure provides infrastructure lifecycle management and end-to-end visibility of services and applications for improved troubleshooting. It combines the solution lifecycle from design phase to monitor and troubleshooting phase.

For configuration, Cisco Prime Infrastructure has a provisioning GUI and built-in templates for enabling AVC capabilities on network devices.

For monitoring, Cisco Prime Infrastructure leverages the rich information provided by the network infrastructure, such as routers, and provides network administrators with a single tool for monitoring both network and application performance.

Network administrators can use Cisco Prime Infrastructure to drill down from an enterprise-wide network view to an individual user at a site, to proactively monitor and troubleshoot network and application performance problems.

For more information, see: http://www.cisco.com/go/primeinfrastructure

Interoperability of AVC with other Services

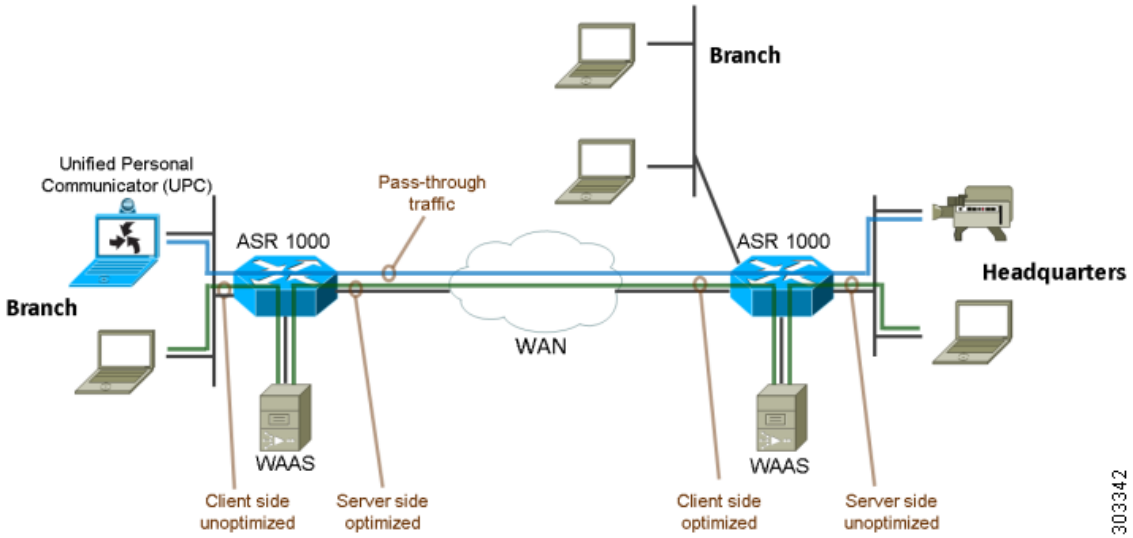
Cisco AVC is interoperable with many router features and services. This section provides additional information about AVC integration with AppNav WAAS, NAT, and VRF.

Interoperability with AppNav WAAS

Cisco IOS Platforms	Cisco IOS XE Platforms
Not available	Added in release 3.8S

Figure 2-3 shows a typical deployment scenario for Cisco AVC, demonstrating the integration with WAAS and the combination of optimized and pass-through traffic.

Figure 2-3 Typical AVC Deployment

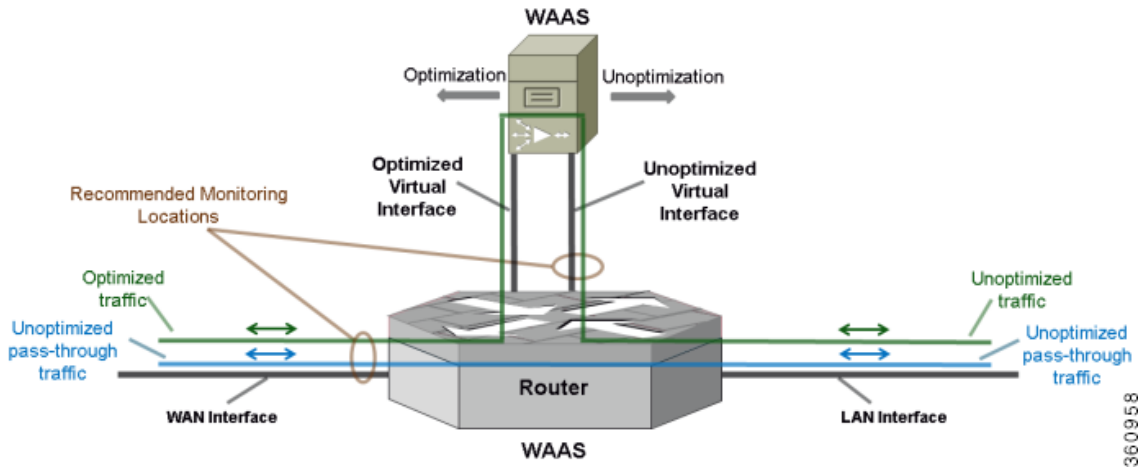


Attachment to a WAAS-Enabled Interface

Cisco Wide Area Application Services (WAAS) provides WAN optimization and application acceleration. The Cisco AVC solution operates closely with Cisco WAAS, reporting performance on both optimized and unoptimized traffic.

Figure 2-4 shows two recommended locations for metric collection. The monitoring location on the WAN interface collects metrics for optimized and unoptimized traffic. The monitoring location on the unoptimized virtual interface collects metrics for unoptimized traffic.

Figure 2-4 Recommended WAAS Monitoring Points



Because optimized traffic may be exported twice (pre/post WAAS), a new segment field, servicesWaasSegment, is exported within the record in order to describe the type of traffic at the monitoring location. Table 2-2 describes the segment definitions.

Table 2-2 AppNav "servicesWaasSegment" Field Values

Value	Description
0	Unknown
1	Client unoptimized
2	Server optimized
4	Client optimized
8	Server unoptimized
16	Pass-through

For pass-through traffic (bypassing WAAS), the servicesWaasPassThroughReason field indicates the reason for pass-through. See the *Cisco Application Visibility and Control Field Definition Guide for Third-Party Customers* for a description of this field.

Application Recognition on Optimized Traffic

The interoperability of Cisco AVC and WAAS enables executing traffic policies and monitoring on optimized traffic, utilizing NBAR2 application recognition.

Note When using WAAS, application L7 fields are only supported on unoptimized traffic. URL records must be attached on the unoptimized AppNav virtual interface.

Reported Input/Output Interfaces

Table 2-3 describes the input/output interface field values used by AppNav when a monitor is attached to the WAN, LAN, or an AppNav virtual interface.

Table 2-3 AppNav Exported Interfaces

Interface	Direction	Input interface value	Output interface value
WAN	Ingress	WAN	LAN
WAN	Egress	LAN	WAN
Optimized VI	Ingress	Optimized VI	LAN
Optimized VI	Egress	WAN	Optimized VI
UnOptimized VI	Ingress	UnOptimized VI	LAN
UnOptimized VI	Egress	LAN	UnOptimized VI
LAN	Ingress	LAN	WAN
LAN	Egress	WAN	LAN

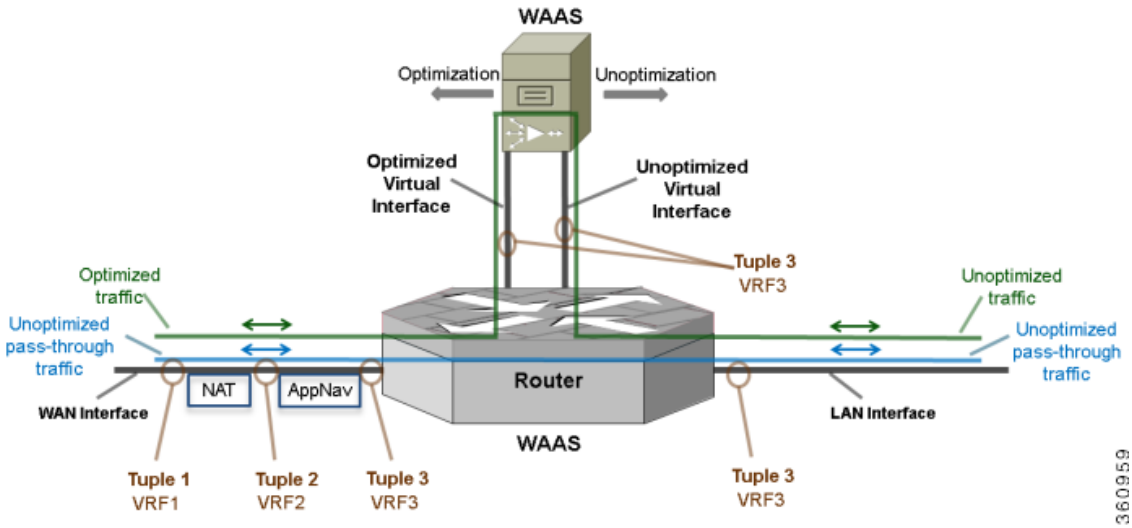
AppNav Interoperability with NAT and VRF

Cisco IOS Platforms	Cisco IOS XE Platforms
Not available	Added in release 3.8S

When AppNav is enabled, it uses the virtual routing and forwarding (VRF) configuration of the LAN interface although it is installed on the WAN interface. AppNav uses the LAN VRF to divert traffic to WAAS, based on local addresses.

Up to three tuples can be used per flow. Figure 2-5 shows an example. Using more than one tuple can be necessary because of different VRF configurations and/or NAT translation. The NBAR/FNF/AppNav features in the path interact together using the same flow.

Figure 2-5 AppNav Interaction in VRF/NAT Cases



NBAR Interoperability with Cisco GET VPN

Cisco IOS Platforms	Cisco IOS XE Platforms
Not available	Added in release 3.11S

Background

Cisco Group Encrypted Transport VPN (GET VPN) is a tunnel-less VPN technology designed to provide the security of encrypted communication, with high media performance, such as lower audio/video latency, and advanced provisioning and management abilities. When using GET VPN, the router performs the encryption and decryption of the VPN traffic.

Encrypted Traffic and NBAR Functionality

Prior to IOS XE release 3.11S, for encrypted traffic, the NBAR component operated on the traffic in its encrypted form. As a result, NBAR was not able to provide deep packet inspection of GET VPN traffic.

Beginning with release 3.11S, NBAR operates on clear traffic (after decryption for ingress, before encryption for egress). This enables running output QoS on inspected applications. In this release, input QoS and reporting in this release continue to operate on encrypted traffic.

To revert to the NBAR functionality that existed prior to release 3.11S, use the following command:

```
ip nbar disable classification encrypted-app
```

Note Enabling NBAR to operate on encrypted traffic requires additional processing, which may impact overall performance.

Limitations

The following limitations apply to NBAR interoperability with GET VPN:

- As in previous releases, QoS continues to operate on ingress traffic in its encrypted form, utilizing application identification information provided by the NBAR legacy component.
- In this release, only the operation of NBAR and QoS output have changed. AVC visibility functionality is not supported for GET VPN encrypted traffic.

Related Topics

- For more information about Cisco GET VPN, see Group Encrypted Transport VPN.
- AVC Interoperability with Cisco GET VPN, page 2-16

AVC Interoperability with Cisco GET VPN

Cisco IOS Platforms	Cisco IOS XE Platforms
Not available	Added in release 3.12S

Background

Cisco Group Encrypted Transport VPN (GET VPN) is a tunnel-less VPN technology designed to provide the security of encrypted communication, with high media performance, such as lower audio/video latency, and advanced provisioning and management abilities. When using GET VPN, the router performs the encryption and decryption of the VPN traffic.

Encrypted Traffic and AVC Functionality

Beginning with Cisco IOS XE 3.12S, when GET VPN is configured, AVC operates on clear text traffic (after decryption for ingress to the interface, before encryption for egress from the interface).

This clear text functionality applies to the following traffic types:

- IPv4 unicast
- IPv4 multicast
- IPv6 unicast
- IPv6 multicast

The feature does not apply to the following:

- Virtual (tunnel) interfaces
- Native FNF monitors attached to the same interface

FNF Native Monitors

FNF native monitors continue to operate in the same way as prior to release 3.12S, operating on traffic on the encrypted side.

Overriding AVC Operation on Clear Text

The default behavior when using GET VPN is for AVC to operate on clear text.

In special circumstances, it may be useful to disable the feature enabling AVC to operate on clear text. To revert to the AVC functionality that existed prior to release 3.12S, use the following command (in general configuration mode):

```
performance monitor observation-point encrypted-text
```

Example

To disable the feature on all policies attached to interfaces configured with GET VPN:

```
Device# configure t
Device(conf)# performance monitor observation-point encrypted-text
```

Limitations

The following limitations apply to AVC interoperability with GET VPN:

- For performance monitors, FNF on the egress side operates on traffic before encryption. Consequently, the accounting includes egress traffic that might be dropped later by other features, such as QoS and ACL.
- For performance monitors, FNF on the egress side operates before QoS. Consequently, QoS class hierarchy and QoS queue ID cannot be collected.
- The following L2 fields cannot be matched or collected:
  - datalink destination-vlan-id
  - datalink mac source address output
- When Perf-mon and native FNF are configured on an interface and operating in full GET VPN interoperability mode, native FNF monitors do not support account on resolution (AOR). Do not configure AOR on these monitors.
- AVC cannot operate on both clear and encrypted traffic.
- AVC interoperability with GET VPN is not supported on tunnel interfaces.

Related Topics

- For more information about Cisco GET VPN, see Group Encrypted Transport VPN.
- NBAR Interoperability with Cisco GET VPN, page 2-15

Adaptive AVC Reporting

Cisco IOS Platforms	Cisco IOS XE Platforms
Coarse-grain reporting added in release 15.4(3)T	Coarse-grain reporting added in release 3.13S

The Cisco AVC solution can operate in different modes—“working points”—to adapt to various deployments and use cases. This feature, known as Adaptive AVC Reporting, provides options to operate in a more powerful “fine grain” mode, with more extensive, granular application reporting, or in a “coarse grain” mode with application-level statistics reporting in place of detailed flow-level metrics.

Note Prior to Cisco IOS 15.4(3)T and IOS XE 3.13S, AVC operated only in the fine grain mode.

Selecting a Mode

Selecting the AVC mode to use depends on use case objectives. Easy Performance Monitor (ezPM) provides an "express" method for configuring AVC in one of these modes. (See Easy Performance Monitor (ezPM), page 4-4.)

- Fine-grain mode: The ezPM "Application Experience" profile provides extensive, fine-grain reporting, including flow-level performance monitoring metrics. (See Application Experience Profile, page 4-5.)
- Coarse-grain mode: The ezPM "Application Statistics" profile provides a simpler level of AVC functionality, especially suitable to the common use cases of capacity planning and troubleshooting network congestion. This mode reports top application usage and the bandwidth utilized by each application. (See Application Statistics Profile, page 4-10.)

Comparison of Fine-Grain and Coarse-Grain AVC Functionality

Table 2-4 compares fine-grain and coarse-grain AVC functionality.

Table 2-4 Comparison: Fine-Grain and Coarse-Grain Functionality

	Fine-Grain AVC Functionality "Application Experience" ezPM Profile	Coarse-Grain AVC Functionality "Application Statistics" ezPM Profile
Use Cases		
	All AVC use cases, including detailed reporting of all flows. Includes: • Performance metrics per application • Field extraction (Host/URL)	Optimized for common use cases, such as capacity planning or troubleshooting network congestion. Provides information on top applications in the network and the bandwidth utilized by those applications. Detailed flow-level metrics or performance metrics are not in the scope of coarse-grain reporting. Includes: • Network/Site/Device/Link planning • Top applications • Clients/servers

	Fine-Grain AVC Functionality "Application Experience" ezPM Profile	Coarse-Grain AVC Functionality "Application Statistics" ezPM Profile
Reporting		
Functionality	Reporting includes: • ART and media performance metrics • URL and other field extraction • Ability to filter a subset of interface traffic and use different reports for different traffic types • Account-On-Resolution (AOR)	Reporting includes: • Bytes, packets, flows reported per application, interface, direction, protocol, and IP version • Top clients/servers per application (optional) • All interface traffic—no option to filter the monitored traffic

Combining Fine and Coarse-Grain Working Points

Some use cases may require a combination of fine and coarse-grain working points. For example, it may be necessary to configure coarse-grain monitoring for all interface traffic, with fine-grain monitoring for a small subset of the traffic.

To achieve this, it is possible to define multiple contexts operating in parallel: one for a coarse-grain working point and another for fine-grain.

Note It is not possible to combine two fine-grain contexts on the same interface.

Example Use Case

As an example use case, it may be necessary to define a configuration that:

- Provides coarse-grain monitoring for all traffic on an interface.
- Reports performance metrics for specific critical applications. This would require defining fine-grain monitoring for that application traffic.

Configuration Example

For an examples of configuring two contexts on a single interface, one for fine-grain reporting and another for coarse-grain, see ezPM Configuration Example 5: Fine-grain and Coarse-grain Contexts Configured on a Single Interface, page 4-53.

Notes and Limitations

Cisco IOS Platforms

- Defining multiple contexts to combine fine and coarse-grain monitoring is not available in this release.

Cisco IOS XE Platforms

- It is possible to combine one fine-grain and one coarse-grain context on a single interface, but not two fine-grain contexts.