

AVC Solution Guide with Cisco Prime Infrastructure

<u>Scope</u>	4
<u>AVC Solution Overview</u>	4
Getting Visibility	4
Today's Challenges	4
What Is Application Visibility and Control?	5
How Does Application Visibility and Control Work?	6
<u>AVC Technology Overview</u>	7
Presentation	7
NBAR2	7
Flexible NetFlow	7
Performance Collection	8
Reporting Tools	9
Control	9
<u>Use Cases Overview</u>	9
Discover Application Usage in the Network	10
Top Applications	12
Top Talkers (Client or Server)	14
Busiest Site/Location	15
Application Throughput over Time over an Interface	16
Identify an Enterprise's Own Applications and Create Custom Apps to Monitor	16
Monitor and Troubleshoot Voice and Video Performance	19
Why Is My Video Quality Poor?	19
Where in My Network Is Dropping Packets?	20
Monitor and Troubleshoot TCP Performance	21
Which Applications May Be Having Performance Issues?	21
What Might Cause the Problem - Is Application Slowness Caused by the Network or Application?	22
<u>Deployment Scenarios</u>	23
Enterprise Reference Topology	23
AVC at the WAN Edge	24
AVC at the Internet Edge	26
AVC for Managed Service Providers (MSPs)	26
AVC for Traditional Wireless Deployments (Cisco Unified Wireless Network)	28
AVC for Converged Access	29
AVC for Perimeter Security/Firewall	32
AVC Deployment Caveats	33
<u>AVC Enablement with Cisco Prime Infrastructure</u>	33
Cisco Prime Infrastructure Download	33
Installation	33
AVC Configuration	34
AVC-Supported Platforms	34
Prerequisites	34
Interface Roles Configuration	34
Protocol Pack Update	35
AVC Configuration and Activation	36
Custom Application Creation	42
Advanced System Settings	43
Monitoring/Visualizing AVC	43
Monitoring Dashboards	43
Use Cases Workflow	43
Troubleshooting	59
AVC Configuration Through DWC	59
Is Cisco Prime Infrastructure Receiving NetFlow Data?	59
Troubleshooting Flowchart	60

<u>Appendix</u>	61
<u>Preparing the Network</u>	61
<u>Configuring SNMP</u>	61
<u>Enabling Telnet/SSH</u>	61
<u>Device Discovery</u>	61
<u>Configuring Medianet</u>	62
<u>Detailed CLI Configuration for AVC</u>	63

Scope

This document aims at providing an overview of the Cisco® Application and Visibility Control (AVC) 2.0 Solution and how customers can enable this solution using the product Cisco Prime™ Infrastructure version 2.0.

AVC Solution Overview

Getting Visibility

Network operators would like to understand how their network is being used and by which applications. Traditionally, this knowledge has been available by exporting information about the flows traversing the network using Traditional and Flexible NetFlow (FNF), and then analyzing them using a network management system (NMS). Exported fields can then be used to classify the flows' range from IP addresses, port numbers, differentiated services code point (DSCP) markings (assuming that the operator has classified applications based on DSCP markings), and application names using Network Based Application Recognition (NBAR), among other techniques.

Today's Challenges



Cloud services and cloud applications such as WebEx®, SalesForce.com, and Office 365 are delivered over HTTP and HTTPS, which are the same ports used by typical recreational web traffic such as Netflix, Hulu, Pandora, and iTunes.

To improve availability and ensure business continuity, organizations need efficient ways to maintain production systems while minimizing downtime. Virtualization technology simplifies IT so that organizations can more effectively use their storage, network, and computing resources to control costs and respond faster to the ever-changing landscape. Virtual desktop infrastructure (VDI) solution provides a delivery of a rich user desktop experience in virtual desktop and remote workstation environments. VDI clients can be in the same building as the server, on the same network, or across the WAN. This creates additional requirements on the network to help ensure a proper delivery of the information to the end user.

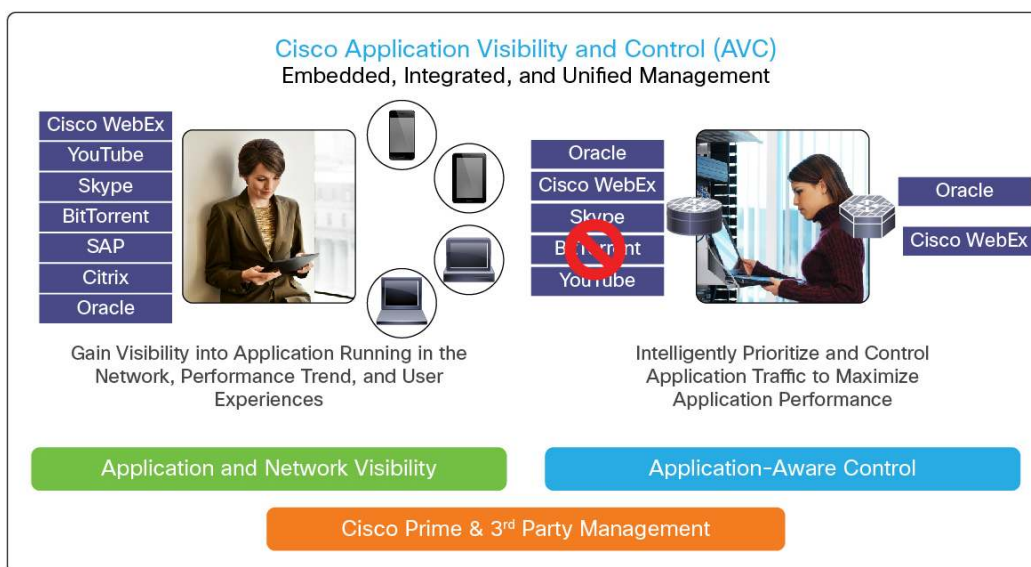
In addition, consolidation of the data center in order to reduce overhead and operating expenses requires the network to carry a much greater volume of both business and recreational traffic. Network admins need to gain visibility into different types of traffic and their performance in greater detail to be able to quickly isolate and troubleshoot application performance issues. They need the ability to granularly define policies to control and tune the performance of these different applications.

What Is Application Visibility and Control?

Cisco Application Visibility and Control (AVC) is a solution that uses multiple core technologies found in the Cisco Aggregation Services Routers (ASR) 1000 Series, the Cisco Integrated Service Routers Generation 2 (ISR G2), the Cisco Integrated Service Routers Generation 3 (ISR G3), the Cisco Cloud Services Router (CSR) and the Cisco Wireless Controllers.

The Cisco AVC solution offers a truly innovative approach to facilitate application awareness in the network. AVC incorporates application recognition and performance monitoring capabilities that were traditionally only available as dedicated appliances in the WAN router platform. This integrated approach greatly reduces the network footprint, simplifies network operations, and reduces total cost of ownership (TCO). The information collected by Cisco AVC is exported in an open standard format such as NetFlow Version 9 and IP Flow Information Export (IPFIX), which allows both Cisco and third-party network management to support the Cisco AVC solution.

Coupled with network management tools, Cisco AVC provides a powerful and pervasive integrated solution for discovering and controlling applications within the network. Empowered with these tools, network administrators can gain a much deeper insight into applications running in their networks and their performance characteristics, while applying policies to further improve performance and control of network resource usage.



In addition to providing visibility into applications running on the network and their performance, Cisco AVC enables per application policy for granular control of application bandwidth utilization which results in better end-user experiences. Cisco AVC is enabled in Cisco IOS® Software and Cisco IOS XE Software.

How Does Application Visibility and Control Work?

AVC uses a number of technologies and consists of four functional components:



The Cisco AVC solution uses multiple technologies to recognize, analyze, and control more than 1000 applications including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications.

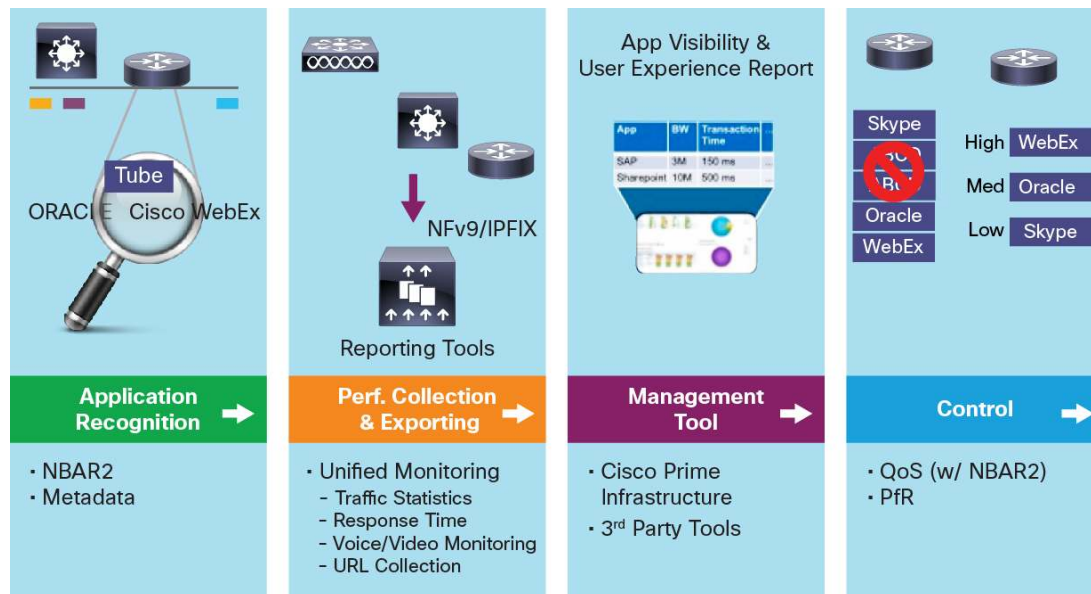
Cisco AVC has the following functional components:

- **Application Recognition:** With Cisco AVC, Cisco ASR 1000, ISR G2, and Cisco Wireless Controllers can identify more than 1000 applications within the traffic flow using NBAR2, Cisco's innovative deep packet inspection (DPI) technology. In order to address the evolving nature of applications, NBAR2's application signature can be updated through Protocol Pack while the router is in service.
- **Performance Collection and Exporting:** Cisco AVC uses an embedded monitoring agent to collect application response time (ART) metrics such as transaction time and latency for TCP applications, and packet loss and jitter for voice and video applications. These metrics are aggregated and exported using standard flow export formats such as NetFlow Version 9 and IPFIX.
- **Management Tool:** With open flow export formats such as NetFlow Version 9 and IPFIX, Cisco Prime Infrastructure and other third-party network management tools can consume data exported by AVC. This gives customers flexibility to use the Cisco management tool or to use the management tool of their choice.
- **Control:** By utilizing common DPI technology, NBAR2, these routers can reprioritize critical applications or enforce application bandwidth use using Cisco's industry-leading quality of service (QoS) capabilities. In addition, intelligent application path selection based on real-time performance is provided through Cisco Performance Routing (PfR).

AVC Technology Overview

Presentation

The following picture shows technologies and features that support each of Cisco AVC components:



NBAR2

NBAR2 provides stateful deep packet inspection capability natively. This next-generation NBAR, or NBAR2, enhances the application recognition engine to support more than 1000 applications.

NBAR2 also provides additional capabilities such as application attributes, which provide grouping of applications with similar properties into category, subcategory, application group, and so on. NBAR2's categorization of protocols into meaningful terms simplifies report aggregation and control configuration. NBAR2 also provides field extraction capability, such as HTTP URL, Session Initiation Protocol (SIP) domain, mail server, and so on, which allow extraction of information from the application for classification or exporting.

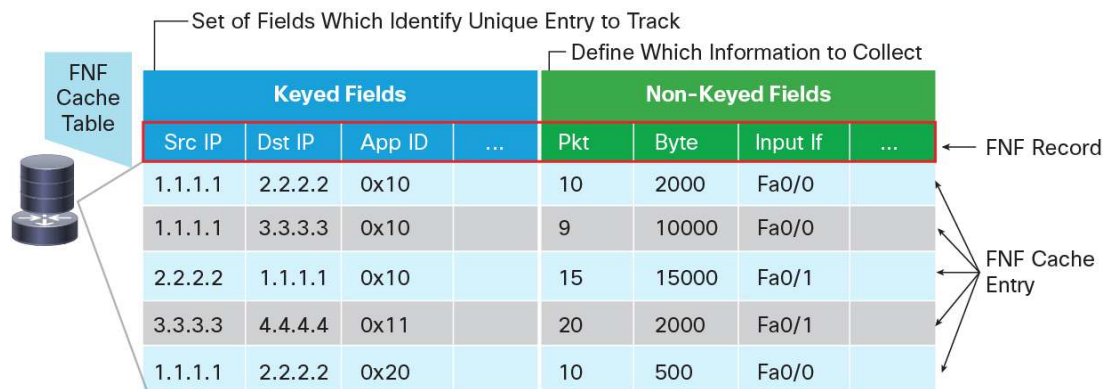
With NBAR2 Protocol Pack, new and updated application signatures can be loaded into the routers without the need to upgrade the software image.

NBAR2 is capable of defining customized applications based on ports, payload values, or URL. The set of attributes for each protocol could be customized as well.

Flexible NetFlow

All the information collected and exported by AVC is done through Flexible NetFlow infrastructure that can collect application information provided by NBAR2, traffic flow information, and application statistics such as byte and packet count.

In addition, there are specific engines that analyze performance metrics for voice, video, and TCP applications.



All information is aggregated and then exported through open export formats such as NetFlow Version 9 and IPFIX. Classic NetFlow (also called Traditional NetFlow) and NetFlow Version 5 are not suitable for AVC because they can only report Layer 3 and Layer 4 information.

NetFlow Version 9 and IPFIX are industry standards for acquiring operational data from IP networks to allow network planning, monitoring traffic analysis, and IP accounting. Flexible NetFlow has the capability to customize the traffic analysis parameters for customer's specific requirements.

Performance Collection

By utilizing the Flexible NetFlow infrastructure, users have complete control of what information needs to be collected and how it is aggregated, by defining what is called an FNF record. An FNF record consists of FNF keyed fields and nonkeyed fields.

Keyed fields are all fields that need to be unique in order for a new FNF cache entry to be created. How keyed fields are chosen depends on what information is of interest to users:

- Collect application usage: Keyed field is the NBAR2 application
- Collect traffic between two endpoints: Keyed fields are source and destination IP addresses
- Collect application usage between two endpoints: Keyed fields are source, destination IP addresses, and NBAR2 application

Nonkeyed fields provide other information of interest into the FNF record. Nonkeyed fields typically are information such as byte count, packet count, input and output interfaces, and performance metrics such as latency or jitter.

Metric providers are responsible to collect and calculate metrics. Some metric providers are simple and collect stateless metrics per packet. Some other metric providers could be more complex and require keeping states and collecting metrics per flow, making some transformation at export time or even doing more sophisticated calculation in the route processor.

Performance collection includes traffic statistics, URL collection, application response time, and also media monitoring such as voice or video.

Reporting Tools

The volume of information collected by AVC necessitates the need for a management platform to show the information in an easy-to-understand manner. Different types of reports are possible for different use-cases. Today, there are several vendors with reporting tools compatible with AVC. The recommended management platform from Cisco is Cisco Prime Infrastructure, which will be referenced throughout this document.

Control

QoS provides prioritization, shaping, or rate limiting of traffic. High-priority, latency-sensitive traffic can be put into the priority queue. QoS can also guarantee minimal bandwidth available to an application or group of applications with QoS traffic class. For AVC, QoS class-map statements allow matching on all the new NBAR2-supported applications and Layer 7 application fields (such as URL, host, and so on) or protocols, as well as on the NBAR2 attributes, which can coexist with all other traditional QoS match attributes such as IP, subnet, and DSCP.

Performance Routing allows network administrators to minimize bandwidth costs, enable intelligent load distribution, improve application performance, and improve application availability. Whereas other routing mechanisms can provide both load sharing and failure mitigation, Cisco IOS PfR makes real-time routing adjustments based on application criteria such as response time, packet loss, jitter, path availability, interface load, and circuit cost minimization.

Use Cases Overview

With the growing applications, mobility, and number of devices, network administrators are looking to:

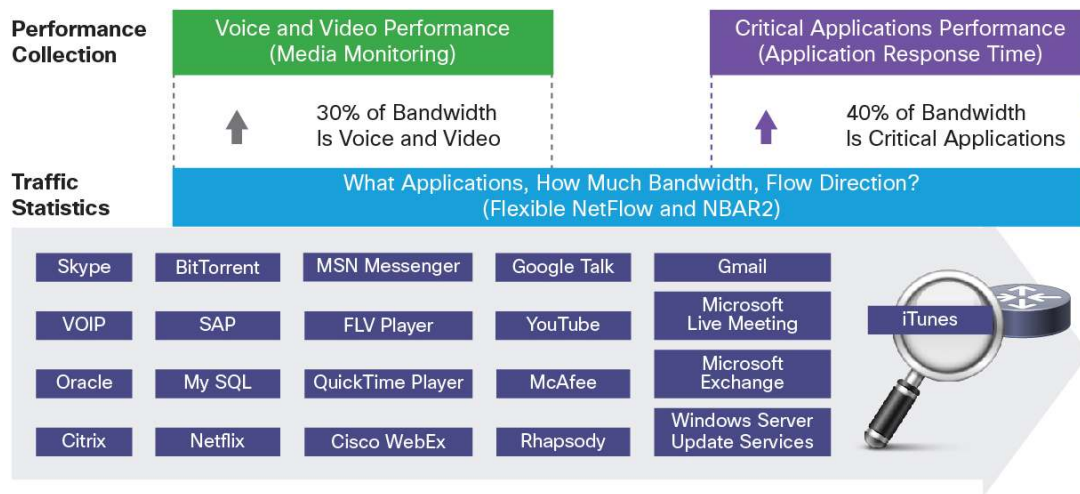
- Gain visibility into applications in the network
- Monitor the performance of each application
- Maximize the user experience by controlling the application usage in the network

By using the Cisco AVC solution, operators could intelligently manage applications and monitor their performance to optimize the available bandwidth on the links.

The AVC solution tracks each user transaction, classifies the application, and exports the transaction information using NetFlow or IPFIX. The NetFlow/IPFIX records are consumed and reported to the operator. Using the rich records and reports, the network administrator is able to:

- Analyze application usage and improve performance
- Improve the user experience
- Improve operational efficiencies
- Increase overall profit

Implementing application visibility is simply defining various NetFlow records to collect the following information:

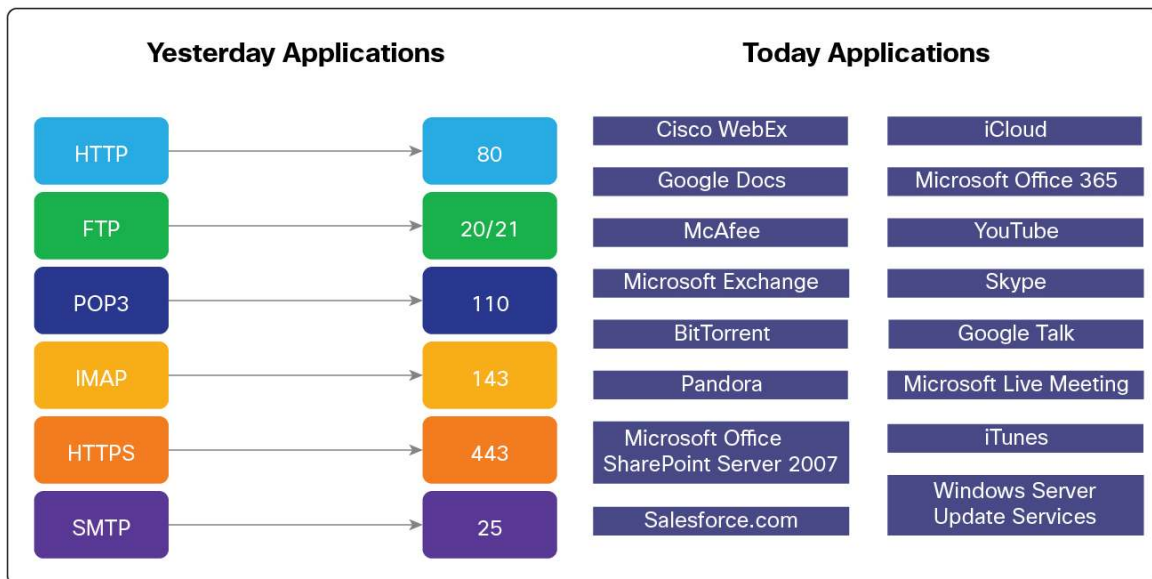


Based on all NetFlow records and performance metrics that are embedded in Cisco's platforms, the following monitoring profiles have been defined. This is based on customer and service provider feedback and can be extended moving forward:

Traffic Statistics	URL Visibility	Application Response Time	Media Performance
<ul style="list-style-type: none"> Application Usage Per Client IP/Subnet/Site Top Clients Per Application 	<ul style="list-style-type: none"> Most Visited Web-Site Per-URL Application Response Time 	<ul style="list-style-type: none"> Per-Application End-to-End Latency Application Response Time & Transaction Time Application Processing Time Top Conversation Per Application 	<ul style="list-style-type: none"> Per-Stream Jitter and Packet Loss RTP Conversations

Discover Application Usage in the Network

In the past, typical network traffic could easily be identified using well-known port numbers. HTTP, HTTPS, POP3, or IMAP were among common traffic seen in enterprises. Today, an increasing number of applications are delivered over HTTP - both business and recreational applications. Many applications use dynamic ports such as Exchange and voice and video that are delivered over Real-time Protocol (RTP). This makes them impossible to be identified by looking at port numbers. In addition, some applications disguise themselves as HTTP because they do not want to be detected. As a result, identifying applications by checking for well-known ports is no longer sufficient.



NBAR2 is the deep packet inspection engine used in AVC and it detects more than 1000 applications. Its heuristic analysis engine allows NBAR2 to identify applications regardless of the ports on which the applications may be running.

The support of NBAR2 Protocol Pack (PP) allows updating application signatures while the routers are running. A new Protocol Pack is released every month.

In addition to providing the application name, NBAR2 also brings attributes to simplify application management for both classification and reporting. Application categorization, for example, allows the grouping of similar applications.

NBAR2 can also extract information from applications such as HTTP URL, HTTP User Agent, and SIP URL, for export or classification.

Global Application ID: A unique ID per application reported from all DPI engines in Cisco:

- Cisco IOS ISR, Cisco IOS-XE ASR 1000
- Network Analysis Module, Cisco IOS Firewall
- Future: Wide Area Application Services (WAAS) Express, and so on

This application ID format is 4 bytes with a 1-byte engine ID and a 3-byte selector ID:



- For applications such as Open Shortest Path First (OSPF) and Internet Control Message Protocol (ICMP), which are protocol types, IANA has allocated protocol numbers and the engine ID used will be "protocol" - (IANA_L3_STANDARD, ID: 1)
- For applications based on well-known IANA ports, the engine ID used will be "port" - (IANA_L4_STANDARD, ID: 3)

- For custom applications defined by an enterprise, the engine ID used will be “NBAR” - (NBAR_CUSTOM, ID: 6)
- For real applications like Skype and Bittorrent, there is no standard way to define what an application is. From a router prospective, there is no standard way to classify these applications because they use some features such as dynamic port allocation and so on. In such cases, the engine ID will be cisco - (CISCO_L7_GLOBAL, ID: 13)

Field Extraction - Subapplication ID Format:

If you look at YouTube or WebEx, both of which run on top of HTTP, these applications also require the router to look into the header or into the payload.

In that case the application ID will be HTTP, and an additional field will be exported, that is, the subapplication ID. Subapplication IDs could be the HTTP URL, referrer, user-agent, host, and so on.

By having these application-related fields along with other information from the traffic flow such as IP address, port, byte count, packet count, and DSCP in the FNF records, reporting tools can produce various application statistics reports that include, but are not limited to, top talkers, top applications, visited websites, or top clients.

Top Applications

Traditionally, this knowledge has been available by exporting information about the flows traversing the network using Traditional and Flexible NetFlow (FNF) and then analyzing the flows using a network management system (NMS). Exported fields that can be used to classify flows range from IP addresses to port numbers and DSCP marking.

AVC provides the ability to report application statistics. Application information, such as Sharepoint, Netflix, or Google Docs, which is provided by NBAR2, is exported in an FNF field called Application ID (described previously). Extracted information such as URI or hostname is exported in another FNF field called Extracted Field (also called subapplication field, described previously).

Configuring “ip nbar protocol-discovery” on an interface enables NBAR. The show command, **show ip nbar protocol-discovery**, produces the following output:

```
ASR1#sh ip nbar protocol-discovery

GigabitEthernet0/0/0

Last clearing of "show ip nbar protocol-discovery" counters 01:27:11
```

Protocol	Input	Output
	-----	-----
	Packet Count	Packet Count
	Byte Count	Byte Count
	5min Bit Rate (bps)	5min Bit Rate (bps)
	5min Max Bit Rate (bps)	5min Max Bit Rate (bps)
bittorrent	696992	442556
	804629283	26345408

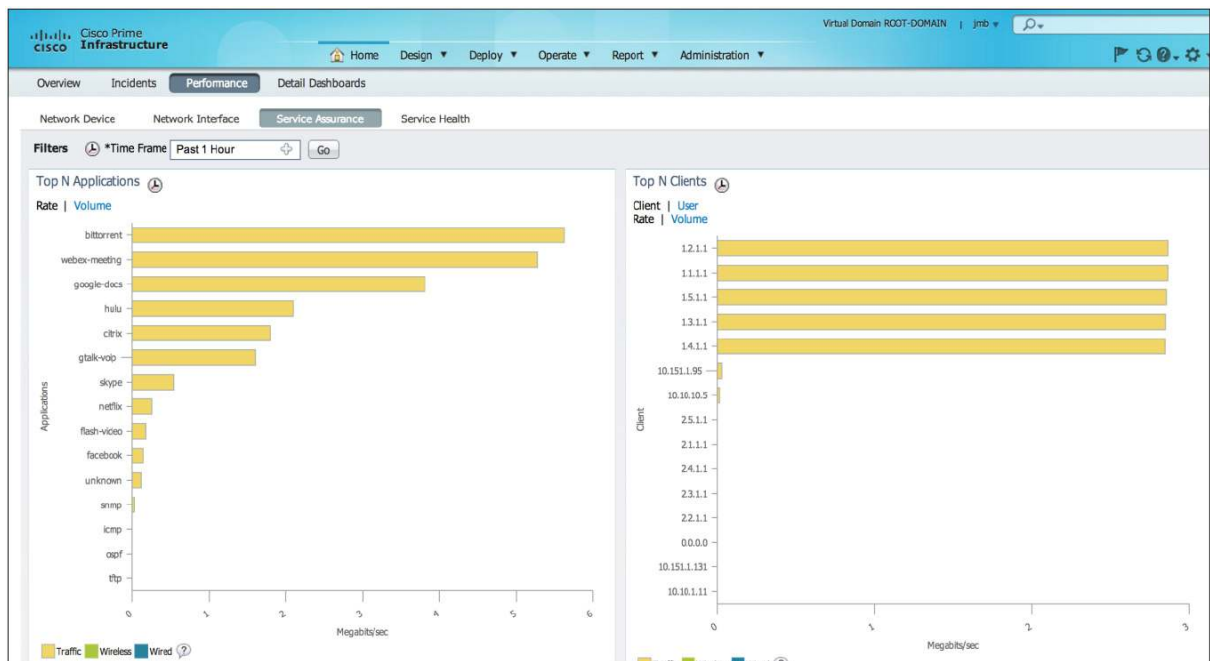
	576000	4000
	2737000	79000
webex-meeting	490553	767015
	404958293	406156304
	255000	273000
google-docs	994000	1005000
	663653	531562
	845095007	73970024
	402000	11000
netflix	1824000	171000
	255409	145098
	317677726	10576284
	235000	2000
	1575000	46000

But this only provides a local view on a specific platform and therefore is mostly used for troubleshooting purposes.

To obtain a global view and be able to have the top applications running over a network, a network administrator has to use Flexible NetFlow or Unified Monitoring. Using Flexible NetFlow with the application name and by collecting bytes/packets allows a network operator to get the list of top applications on a global basis, or a per site basis, or even on a specific interface.

Global View

The recommended way is to use Cisco Prime Infrastructure and look at the detail dashboards. To have a global view of all applications running across your network, go to **Operate → Performance** or **Home → Performance** and select **Service Assurance**:



One of the main dashlets is the **Top N Applications**, which will give you the top 15 applications running over your network.

In order to obtain a deeper understanding of how Cisco Prime Infrastructure could achieve this, please refer to the later “Top Applications” section.

Top Talkers (Client or Server)

One of the common requirements is to track the top talkers, both in terms of clients and servers. A network operator can check as to who is using a specific application or who is consuming a lot of bandwidth and check whether this is a normal mode of operation.

This is something that you can get directly on a router with a feature called Flexible NetFlow Top Talkers. It is a generic instrumentation to display flow monitor content and it works with any type of flows/fields (IPv4, IPv6, Layer 2, and so on).

Flexible NetFlow Top Talkers introduces advanced search capabilities.

Flow Filtering: Enables users to select flows based on specific values for any fields that are defined for that cache.

Flow Aggregation: Enables users to aggregate on a subset of the key and nonkey fields present in the flows of an FNF cache.

Flow Sorting: Enables users to control how the displayed cache entries are sorted on any field present in the flows of an FNF cache and display them in order or reverse order.

Flow Filtering, Flow Aggregation, and Flow Sorting can be combined to select what and how information will be displayed.

Example: Top Ten IP Addresses with the Most Traffic (Packets):

```
ISR7#sh flow monitor MONITOR-STATS cache aggregate ipv4 source address sort  
highest counter bytes long top 10
```

```
Processed 185 flows
```

```
Aggregated to 60 flows
```

```
Showing the top 10 flows
```

IPV4 SRC ADDR	flows	bytes long	pkts
=====	=====	=====	=====
4.2.1.1	1	2352476	2065
4.4.1.1	1	2346674	2058
4.5.1.1	1	2338162	2051
4.1.1.1	1	2334010	2049
4.3.1.1	1	2332679	2048
1.3.1.1	18	2033969	14603
1.2.1.1	18	2016353	14460
1.4.1.1	18	1989883	14307
1.5.1.1	18	1989865	14295
1.1.1.1	18	1967106	14062

```
ISR7#
```

Example: Top Ten Applications with the Most Traffic (Packets):

```
ISR7#sh flow monitor MONITOR-STATS cache aggregate application name sort highest
counter bytes long top 10
Processed 173 flows
Aggregated to 9 flows
Showing the top 9 flows
```

APP NAME	flows	bytes long	pkts
=====	=====	=====	=====
cisco bittorrent	10	5699636	8084
cisco google-docs	30	4198058	7102
cisco webex-meeting	20	3577396	5724
port http	10	2700052	2376
cisco gtalk-voip	10	1798206	15246
cisco citrix	10	1271757	13276
cisco skype	20	291070	5666
cisco unclassified	58	211073	3232
prot icmp	5	5760	10

```
ISR7#
```

The Flexible NetFlow Top Talkers feature is interesting primarily for troubleshooting, but this option is not available on all platforms. (Typically it is available on the ISR G2 but not available on the ASR 1000 platform yet).

So, the best option to get the top talkers on a global basis is to use Flexible NetFlow or Unified Monitoring on a global basis - at least on the WAN edge - and then use Cisco Prime Infrastructure (or any NetFlow tool that can enable traffic statistics using Flexible NetFlow or Unified Monitoring).

There are two options here:

- Global View: Browse to the dashboards at **Home → Performance → Service Assurance** or **Operate → Performance → Service Assurance**.
- Global view with filter options: **Home → Detail Dashboards** or **Operate → Detail Dashboards**

In order to obtain a deeper understanding of how Cisco Prime Infrastructure could achieve this, please refer to the later “Top Applications” section.

Busiest Site/Location

If Flexible NetFlow or Unified Monitoring has been deployed on all sites, at least on the WAN edge, then a NetFlow application can be used to sort the top sites based on the site prefixes.

The mapping between site names and prefixes should have been defined using Cisco Prime Infrastructure. Please refer to the “Device Discovery” section in the Appendix for more information.

A traffic statistics profile gives information like bytes and packets as well as IP source and destination addresses and application names. From that, one can extract and sort the top sites based on throughput.

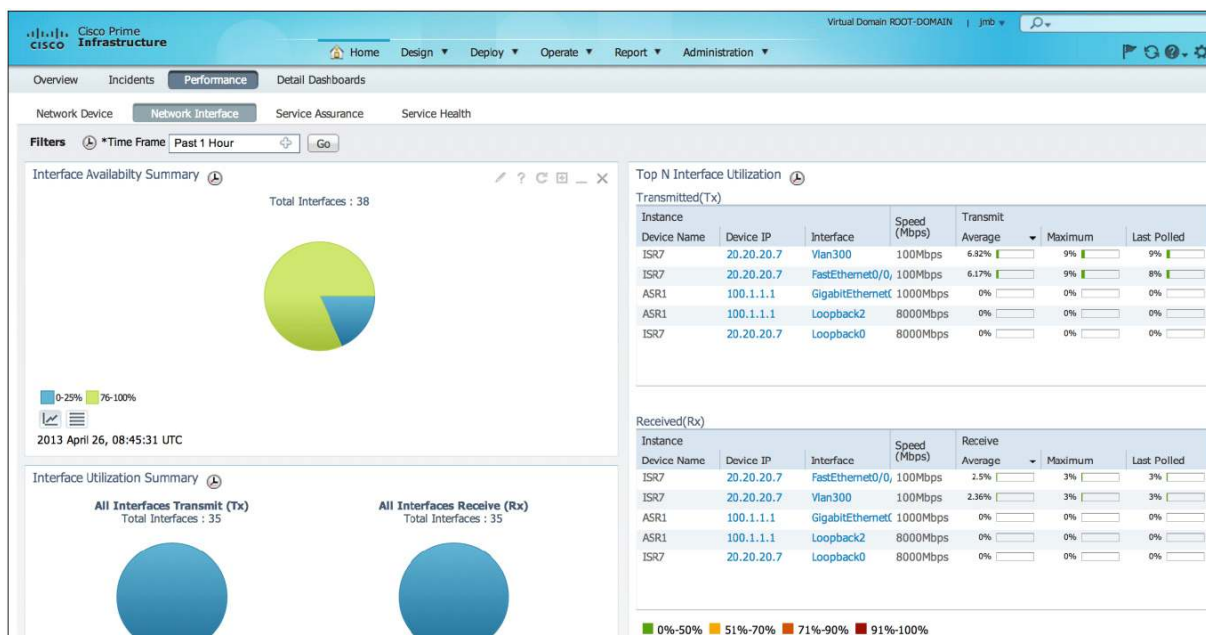
In order to obtain a deeper understanding of how Cisco Prime Infrastructure could achieve this, please refer to the later “Busiest Site/Location” section.

Application Throughput over Time over an Interface

So far we have seen how we could check the application usage on a global basis or per site. There could also be a need to troubleshoot the application usage on a specific interface.

A first step would be to check the top interface utilization.

Browse to **Home → Performance → Network Interface**.



The interesting dashlet here is Top N Interface Utilization.

In order to obtain a deeper understanding of how Cisco Prime Infrastructure could achieve this, please refer to the later "Application Throughput over Time over an Interface" section.

Identify an Enterprise's Own Applications and Create Custom Apps to Monitor

Routers have a list of applications supported based on a Protocol Pack, but most enterprise customers also have homegrown applications that they want to monitor.

When NBAR2 is enabled and lists a large number of unknown applications, the network operator will have to check whether the Protocol Pack needs to be updated to accommodate the new applications or if a specific application is used in the enterprise that is not directly supported by NBAR2.

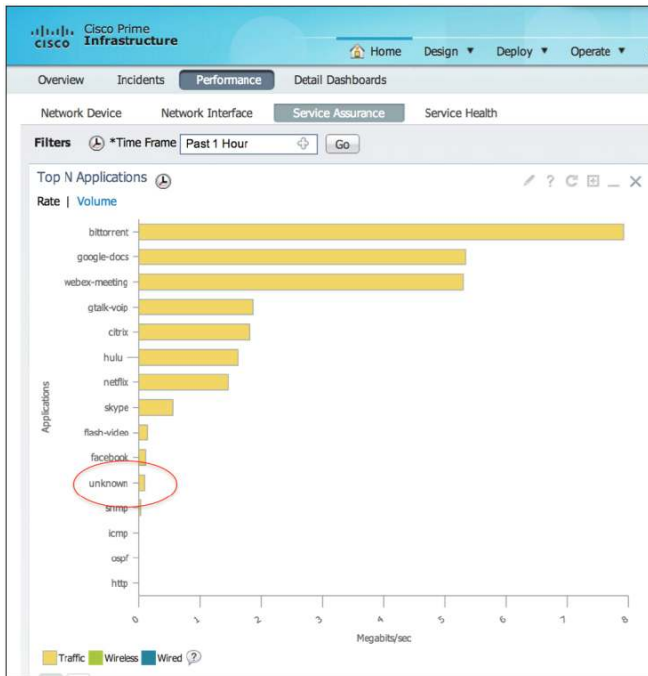
A custom-based application can then be defined, based on a range of ports, or based on the payload, or even based on a specific URL.

If you are going to define custom applications in AVC, the recommendation is to do it from Cisco Prime Infrastructure and **not** through the command-line interface (CLI).

- If you use Cisco Prime Infrastructure to create custom applications, your custom applications will show up in the selection list for configuring monitoring policies. This option is not available with CLI.

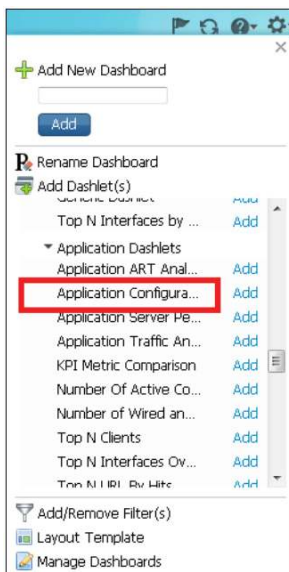
- For pushing the custom application definitions to multiple interfaces and devices across an enterprise, it is easier to use Cisco Prime Infrastructure than having to include the CLIs to define the application signature in the script or template for each distinct group of interfaces or devices. Once an application is defined in Cisco Prime Infrastructure, it is globally available, and you can select the devices that you would like to configure these custom applications.

You can have unknown applications when you check the top applications at **Performance → Service Assurance**:



Click **unknown** and you are redirected to **Detail Dashboard → Application** where you can check the top clients, top servers, and the traffic analysis.

You can also add a very useful dashlet that is not enabled by default. Click at the top-right, select **Add Dashlet**, and choose **Application Configuration** under the application dashlets.



Now you can check as to what ports are used by the unknown applications running across your network:

Application Configuration			
Application	Protocol	Port	bytes
unknown	tcp	54297	12425752
unknown	tcp	4218	7582524
unknown	tcp	443	3468133
unknown	tcp	80	3324536
unknown	udp	9991	1203326
unknown	tcp	62521	1139436
unknown	udp	5353	67

2013 April 26, 09:12:15 UTC

NBAR2 allows defining custom-based applications in addition to applications defined in the active Protocol Pack:

Add Port
Port(s):
Protocol: tcp
Cancel OK

Port

- TCP or UDP
- 16 Static Ports Per Application
- Range of Ports (1000 Maximum)

Payload

- Search the First 255 Bytes of TCP or UDP Payload
- ASCII (16 Characters)
- Hex (4 Bytes)
- Decimal (1-4294967295)
- Variable (4 Bytes Hex)

HTTP URL NEW

- URI Regex
- Host Regex

Custom applications can be based on ports, payload pattern, or URL (new).

You can define a custom-based application directly on the router, so that you can check this application when you use NBAR discovery:

```
ip nbar custom 001myapp tcp 4085 id 60002
```

You can check with the following command:

```
1941-7#sh ip nbar protocol-id
```

Protocol Name	id	type
001myapp	60002	Custom

© 2013-2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Page 18 of 63

TIP: NBAR2 Custom Protocol Naming Best Practice

- Only alphanumeric and _ (underscore) allowed
- First three characters cannot match existing NBAR2 application names
- Best practice - Start with a three-digit number, the same number as the selector ID

```
ip nbar custom 001_cisco_cec http host wwwin.cisco.com id 001
ip nbar custom 002_cisco_eng http host wwwin-eng.cisco.com id 002
```

You can also define custom apps in Cisco Prime Infrastructure. In order to obtain a deeper understanding of how Cisco Prime Infrastructure could achieve this, please refer to the later section “Identify the Enterprise’s Own Applications and Create Custom Apps to Monitor.”

Monitor and Troubleshoot Voice and Video Performance

Delivering a real-time collaboration experience is a major challenge. When enterprises deploy IP-based video applications they must often overprovision their WAN and campus networks in order to meet the scalability requirements and assure the service levels required to achieve the expected quality standards. Video quality standards are very high, as the threshold for poor quality video is much lower than voice or data.

Enterprises invest in collaboration tools to improve communications and increase employee productivity. Yet many of these rich-media systems have the opposite effect and often do not provide the expected level of end-user experience.

Often the problem is a combination of application and network issues. The challenge now is the ability to track, monitor, and assess the end-to-end quality of experience provided to the end users. IT organizations need to be able to constantly monitor and improve those services as the demand for higher quality and new usages is growing very rapidly.

Why Is My Video Quality Poor?

In order to quickly identify and resolve quality issues with media applications on the network, customers need first to be able to understand how they could get more information regarding those flows and then prepare the network for media troubleshooting.

This can be done directly by activating metrics and fault isolation services on the existing network. As it is really a network solution, the customer can choose to do it before or in conjunction with the deployment of a media flow monitoring and management application. The choice will be mainly done based on the time to resolution of the customer.

As mentioned already in the document, customers need to be able to complement media flow information provided by traditional solutions such as FNF, NBAR2, or Class-Based Quality of Service (CBQoS). This is the key to understanding what is affecting the quality of the media application.

AVC has been specifically developed to add performance metrics for media applications.

Performance Monitor can measure the user traffic, generate alerts based on thresholds, and create reports through multiple management interfaces. It uses class maps to define the traffic to monitor. Customers can assign each media application or, as an immediate action, the one with issues, to a class. Because media applications are usually classified when implementing the right QoS, they can reuse the same class maps, but the combination of Cisco NetFlow and deep packet inspection (NBAR2) can also be used to discover traffic flows and facilitate the traffic selection configuration.

AVC can be easily activated on the network to identify what is happening with a specific media application. For that, deployment consideration is simply about:

- What traffic to monitor (based on DSCP, NBAR, FNF...)
- What information do I need (RTP metrics...)
- Where to measure?
- What service targets (threshold)? Quick and easy way to be alerted as soon as the media flow is encountering packet loss, latency, or jitter above requirements.
- Where to send the information? Which management and monitoring application?

AVC for media monitoring can be enabled directly from the CLI, but it's recommended to provision everything from Cisco Prime Infrastructure by using the predefined template. Details of the configuration can also be viewed before the actual deployment.

AVC calculates RTP packet drops by keeping track of the sequence numbers that are part of the RTP header. Unlike a TCP connection, a media stream based on RTP and User Datagram Protocol (UDP) is always unidirectional. Thus, when applying a performance monitor policy in the input direction on a LAN interface on a branch site's router, you collect RTP metrics only for media streams leaving the site. To collect RTP metrics for media streams entering a branch site, you need to apply the policy either on the WAN interface (input) or on the LAN interface (output).

Another field in the RTP header is the synchronization source identifier (SSRC). This identifier is used to distinguish between different audio and video channels if they share the same UDP session. In the case of the Cisco TelePresence® System, the multiscreen video channels share the same UDP stream (IPsrc, IPdst, and Layer 4 ports). For the Cisco TelePresence System, the SSRC is used to differentiate the unique video channels.

RTP jitter values are calculated by analyzing the time-stamp field in the RTP header. The time stamp does not actually refer to regular time but to ticks of the encoder's clock. For video, the encoding clock rate is usually 90 kHz, and in traditional voice it is 8 kHz. However, with modern wideband audio codecs, the frequency may be a variety of values. Performance Monitor tries to derive the clock rate from the payload type field in the RTP header, so the RTP payload type gives you an idea of the kind of media in an RTP stream. The static RTP payload types can be found on the [IANA website](#).

In order to obtain a deeper understanding of how Cisco Prime Infrastructure could achieve this, please refer to the later "Why Is My Video Quality Poor?" section.

Where in My Network Is Dropping Packets?

Cisco Prime Infrastructure can help pinpoint the actual packet drop location in your network. Please refer to the later "Where in My Network Is Dropping Packets?" section.

Monitor and Troubleshoot TCP Performance

Which Applications May Be Having Performance Issues?

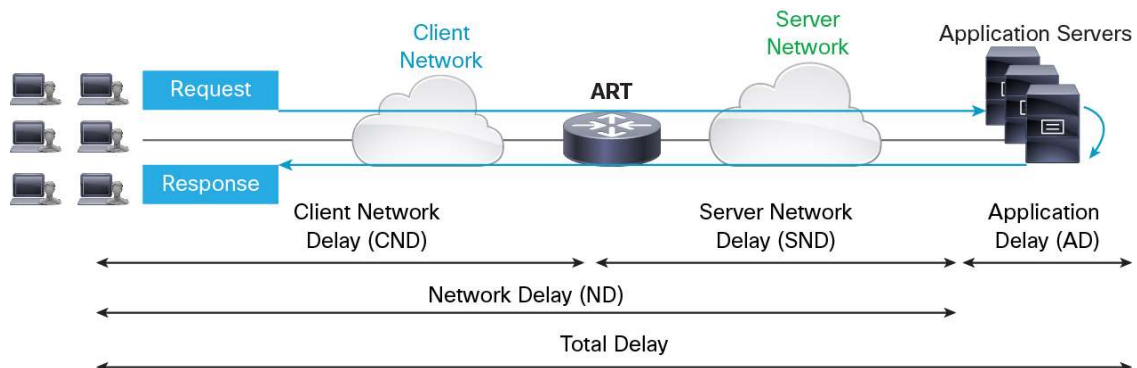
AVC can be activated on the network to identify what is happening with a specific TCP-based application. For that, deployment consideration is simply about:

- What application to monitor
- What information do I need (TCP metrics...)
- Where to measure?
- What service targets (threshold)? Quick and easy way to be alerted as soon as the application is encountering packet loss or delay above requirements
- Where to send the information? Which management and monitoring application

AVC for ART is deployed to get:

- Per application end-to-end latency
- Application response time and transaction time
- Application processing time
- Top conversations per application

AVC performance metrics for TCP-based applications include (list not exhaustive):



- Client network delay
- Server network delay
- Application delay
- Network delay
- Response time
- Transaction time

Checking the response time and transaction time together with the traffic statistics (bytes/sec) helps to understand as to how a specific application performs across the network.

Detect an Application Server Problem:

Typically the application delay will go up. Typically this is caused by the backend database or backend server having some problems. The application delay will shoot up and the network metrics will remain pretty much the same.

Detect the Network Latency Increase Per Application:

When network latency increases, the first thing that increases is response time. As a side effect, transactions will also take longer.

Detect Network Inefficiency (Packet Loss):

As soon as there is packet loss, the network administrator can see that the transaction time also shoots up.

High transaction time is not always bad, because it could be the users downloading a large file.

A network administrator should look at the traffic volume along with the transaction time. If this former decreases when the transaction time increases, it is typically caused by network inefficiency such as packet loss.

AVC for ART can be enabled directly from the CLI, but it's recommended to provision everything from Cisco Prime Infrastructure by using the AVC template. Details of the configuration can be viewed before the actual deployment.

To get more information about this with Cisco Prime Infrastructure, please refer to the later "Which Applications May Be Having Performance Issues?" section.

What Might Cause the Problem - Is Application Slowness Caused by the Network or Application?

AVC with the application response time profile deployed allows to track metrics like:

- Client network delay
- Server network delay
- Application delay
- Network delay

By checking the client, the server, and the application delay, a network operator can point to which part of the network is causing the problem and then navigate to find the root cause.

Detect Application Server Problem:

The application delay will increase. Typically this is caused by the backend database or backend server having problems. The application delay will shoot up and the network metrics will remain pretty much the same.

This helps in understanding and finding the location of the problem:

- Is it a network-based problem? If yes, is it in the WAN or inside the campus?
- Is it an application-based problem?

To get more information about this with Cisco Prime Infrastructure, please refer to the later "What Might Cause the Problem - Is the Application Slowness Caused by the Network or Application?" section.

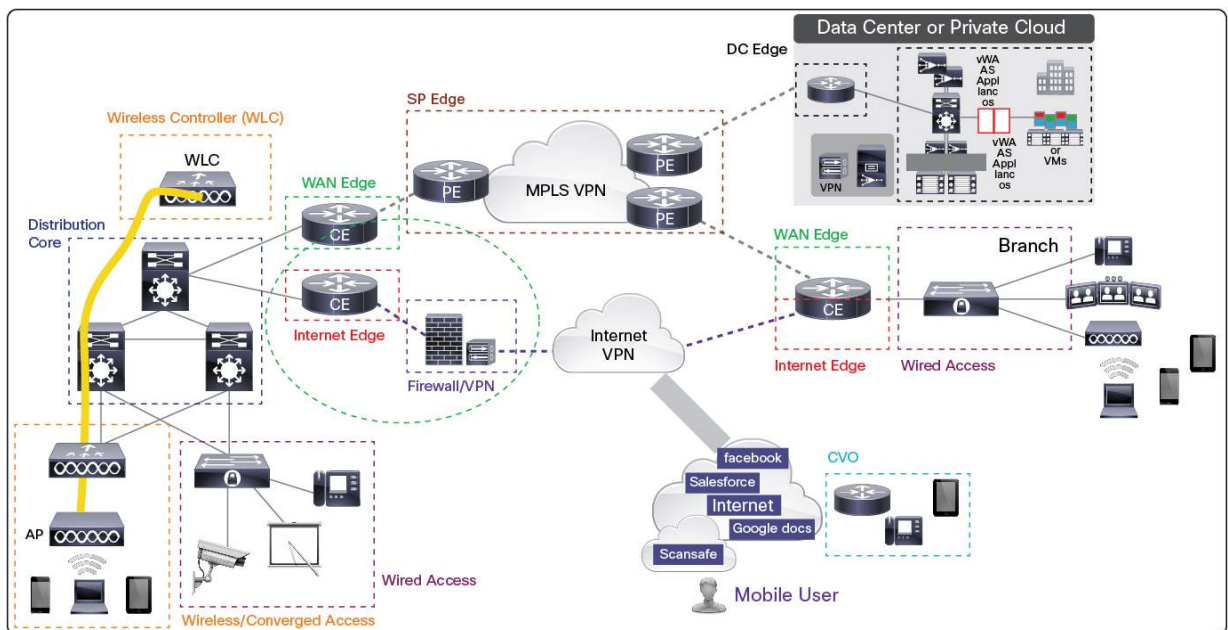
Deployment Scenarios

The need to have application visibility, monitoring, and control exists at every point in the network (PIN). However this requirement is profound in the PINs described in this section. This section provides an overview of the following:

- At which PINs is AVC most relevant and needed and why?
- A representative architecture of each PIN and how AVC features fit in (per PIN)
- What is supported today - AVC features (per PIN)
- Deployment caveats (that are being addressed)

Enterprise Reference Topology

The following illustration is a reference architecture for an enterprise network (high-level view):

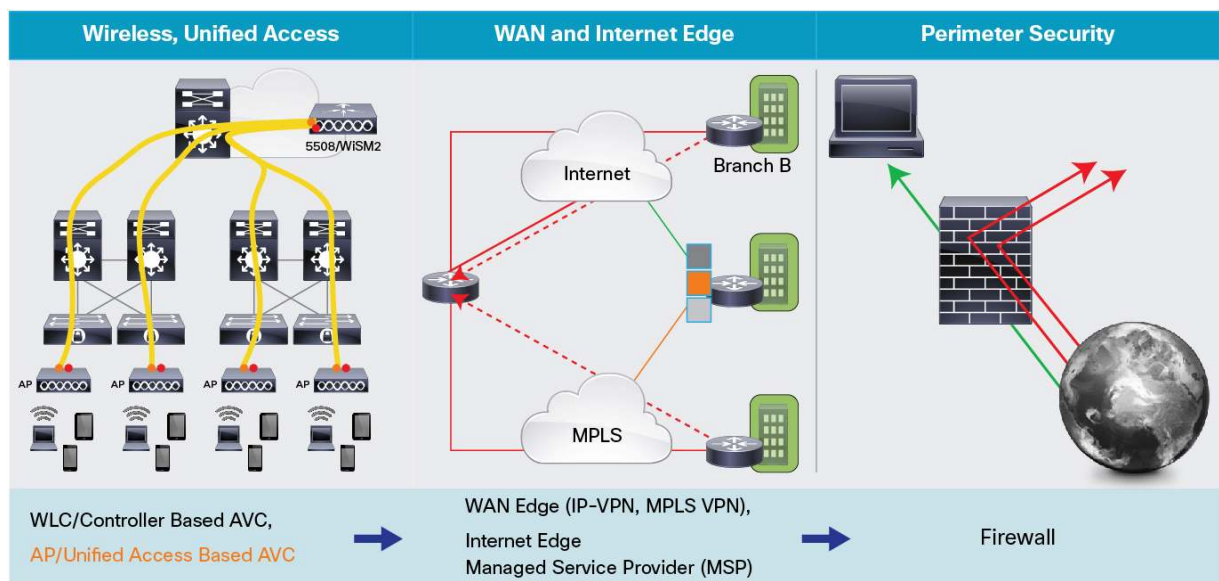


Following are the key PINs:

- Wireless controllers
- Wireless with converged access
- Wired access
- Distribution/core network
- WAN edge
- Internet edge
- Firewall/perimeter security
- Mobile worker/Cisco Virtual Office
- Service provider edge/managed service provider

The points where AVC would be most needed are where there is a compelling need to know the health of applications granularly and to have the ability to ensure their target performances. While these asks apply to all the PINs listed above, AVC can be deployed (in different capacities as explained below) in the more critical PINs, such as the following, today:

- Wireless controllers
- Wireless with converged access (limited capacity or roadmap)
- WAN edge
- Internet edge
- Firewall/perimeter security
- Service provider edge/managed service provider



Broadly, the set of AVC features that would be referenced in this section are:

- | | |
|-----------------------------|---|
| • NBAR2 | (Application visibility) |
| • Flexible NetFlow | (Application visibility and monitoring) |
| • Performance Agent/PerfMon | (Application monitoring) |
| • QoS | (Control) |
| • PfR | (Control) |

AVC at the WAN Edge

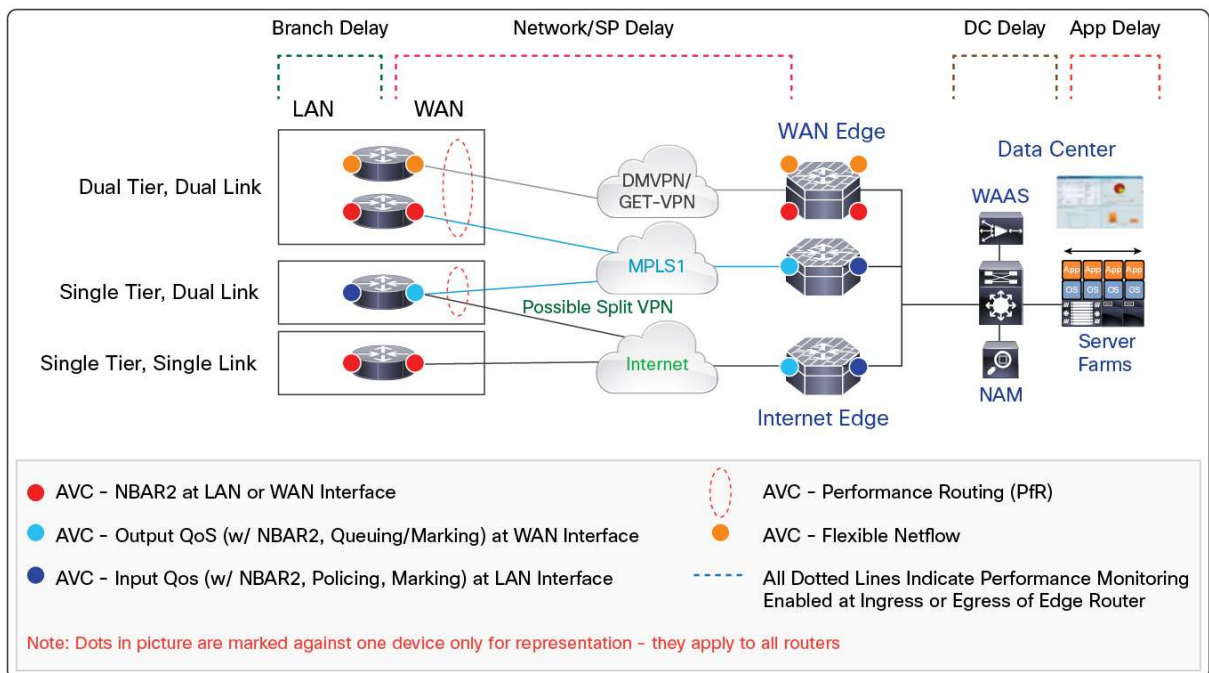
The WAN edge is a point of aggregation of all the traffic from a site/branch towards the headquarters, other sites, or the data center. The available bandwidth at this point might not always be sufficient to run all desired applications with desired levels of performance. The link to the service provider is a premium one with varying costs based on the type of connectivity - Multiprotocol Label Switching (MPLS) VPN, leased lines, IP VPN, and so on. With a greater number of applications **not** being hosted in the branch but outside it, the load on this point increases exponentially, and adding more bandwidth is not always an option. Hence, there is a compelling need to know the applications' granularly, monitor them for performance, and have the appropriate levels of control to make sure business-critical or intended applications get the appropriate treatment in a congested environment.

This level of network visibility is required also to facilitate capacity planning, which is one of the most important exercises in the WAN edge, that is, to know when a bandwidth upgrade is needed (or not).

The key benefits for deploying AVC at the WAN edge:

- Reduced operating expenses (OpEx) - Improved troubleshooting, service-level agreement (SLA) for critical apps
- Reduced capital expenditures (CapEx) - No separate probes, better capacity planning
- Enhanced user and application experience - With network-based solutions
- Optimize WAN costs - Link optimization, business policy-based control

The WAN edge architecture can be of many types - either single tier or dual tier - and have either a single link or dual link. The following illustration depicts not only possible reference topologies but also various AVC features and the points at which they can be deployed in the WAN edge:



The beachhead platforms for the WAN edge are the ISR G2 and ASR 1000, where AVC features listed above can be deployed - typically the ISR G2 at the branch and the ASR 1000 at the headend. Features like NBAR2 are called out at two points - both at the LAN side and at the WAN interface, as they can be applied to either interface. NBAR2 on the LAN interface is used in scenarios where NBAR2 is unable to coexist with other WAN features. The list of deployment caveats is provided later.

AVC at the Internet Edge

The “cloud” has not just transformed IT organizations’ structure drastically but also has changed certain fundamental WAN principles in an enterprise. Traditionally, applications were hosted in a branch, and then they migrated into private data centers in the headquarters or data center. Now, we are seeing a multitude of public-cloud-hosted applications being hosted in the enterprise - SDC, LinkedIn, Office 365, and the likes. These are “business-critical” applications, and the administrator is looking to ensure a good quality of experience for these applications, but they are no longer accessed over the traditional WAN edge - on the branch and the data center, where the administrator had the required control to enforce business policies. These apps are cloud hosted, and the admin has not much control on delivering these applications to the end user.

Also, the Internet links could be best effort or not with a given SLA. Business-critical traffic coming in through such links needs special attention (visibility and monitoring and control) to make sure target performances are met.

The focus, when deploying business critical applications over the cloud, would need to be:

- WAN/cloud performance
- VDI support
- Video quality
- Cloud security
- Management and visibility

This is what makes AVC an important part of the Internet edge deployment.

The deployment model and AVC features at different points continue to remain the same as in the case of the WAN edge (as shown in the illustration above).

AVC for Managed Service Providers (MSPs)

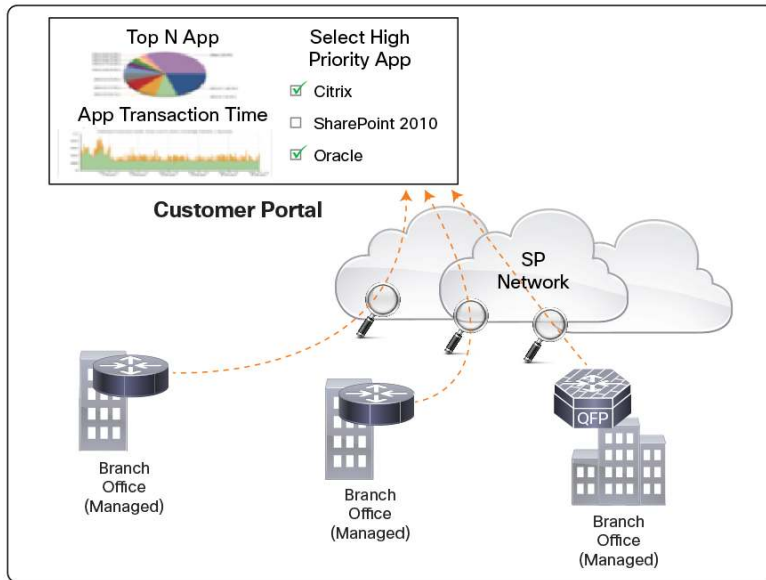
Service providers offer managed services to their customers (typically enterprise customers) to provide enhanced value rather than just ordinary connectivity. There has been a major evolution in terms of what a service provider offers customers - starting from Layer 2 connectivity, Layer 3 VPN connectivity, and managed VPN services (UC, security, triple play) and now moving toward “managed IT services.”

Service providers can now offer application visibility, prioritization, and reporting as part of their managed service offerings that enterprise customers can make use of. It is the responsibility of the service provider to offer these services to customers by abstracting the effort required. The end customer does not need to configure or deploy anything in this case to get the benefit - the service-provider-managed router at the customer premises and the service provider edge router at the provider site offers these capabilities. Service providers can drive incremental revenues, create consulting opportunities, increase customer retention, improve service operation efficiencies, complement hosted services, and lay a strong foundation for application-level SLAs.

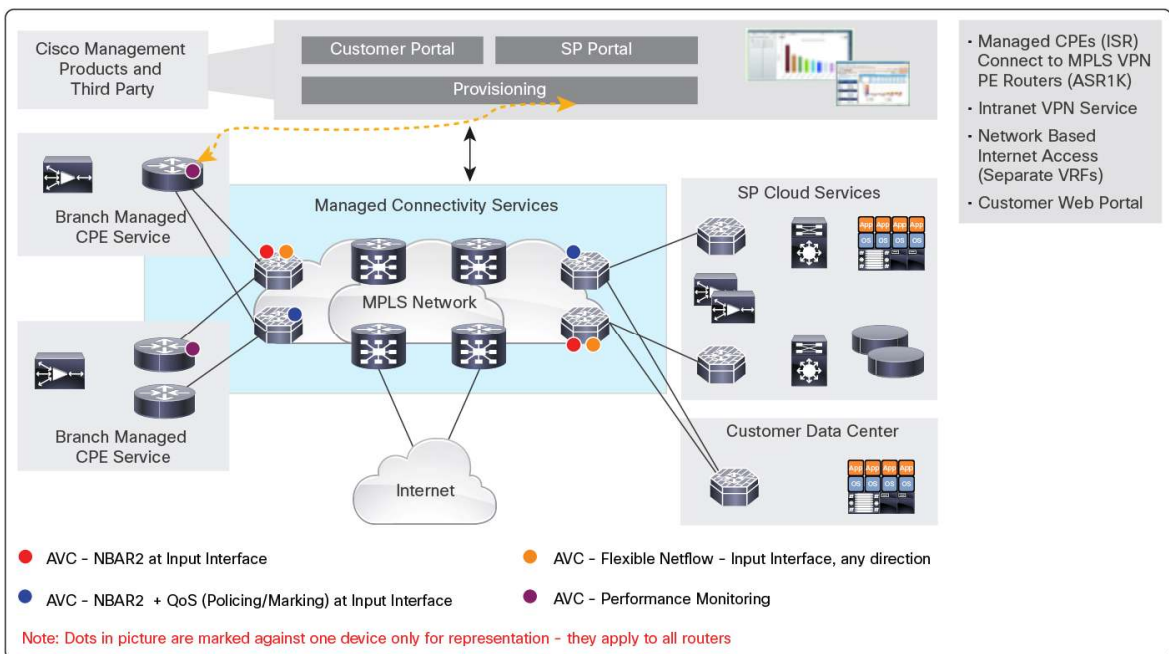
Why use AVC as a managed service:

- Service providers climb up the value chain by offering advanced visibility, prioritization, and reporting to their managed service customers
- Changing key performance indicators (KPIs) are tied to end-user impact and the success rate in solving application performance issues
- Provides a centralized point for looking at network usage and performance data
- Reduces infrastructure costs

- Integrated services - Reduces TCO for the enterprise customer
- Easier rollout of applications for the enterprise admin
- Improves end-user experience for the end customer



The following is a representation of an MSP network and how the different AVC features can be provisioned in such a scenario:



ISR G2 and ASR 1000, in this model too, are the beachhead platforms, and they support the AVC functionality to a large extent. A snapshot of the features and their availability on different platforms in this segment (WAN edge, Internet edge, and managed service providers) can be found in the following table:

Platform	Classification	Performance Collection	Control
800	NBAR2, Metadata	FNF,(Performance Agent)PA, PerfMon -> Unified Monitor (Future)	QoS, PIR
1900-AX	NBAR2, Metadata	FNF, PA, PerfMon -> Unified Monitor (Future)	QoS, PIR
2900-AX	NBAR2, Metadata	FNF, PA, PerfMon -> Unified Monitor (Future)	QoS, PIR
3900-AX	NBAR2, Metadata	FNF, PA, PerfMon -> Unified Monitor (Future)	QoS, PIR
ASR 1000-ASR⁽¹⁾	NBAR2, Metadata	Unified Monitor	QoS, PIR

AVC for Traditional Wireless Deployments (Cisco Unified Wireless Network)

Traditional wireless deployments follow the model of tunneling the traffic from the access point to the Cisco Wireless LAN Controller (WLC) residing typically in the distribution layer. There could be a Layer 2/Layer 3 network between the access point and the WLC, and the client traffic is tunneled inside Lightweight Access Point Protocol (LWAPP) or Control and Provisioning of Wireless Access Points Protocol (CAPWAP) tunnels. This typically means there is not much visibility into client traffic in the access network. The traffic is decapsulated at the WLC, and the WLC has the responsibility of applying client or SSID-based policies, that is, it acts as the point of policy enforcement for wireless traffic.

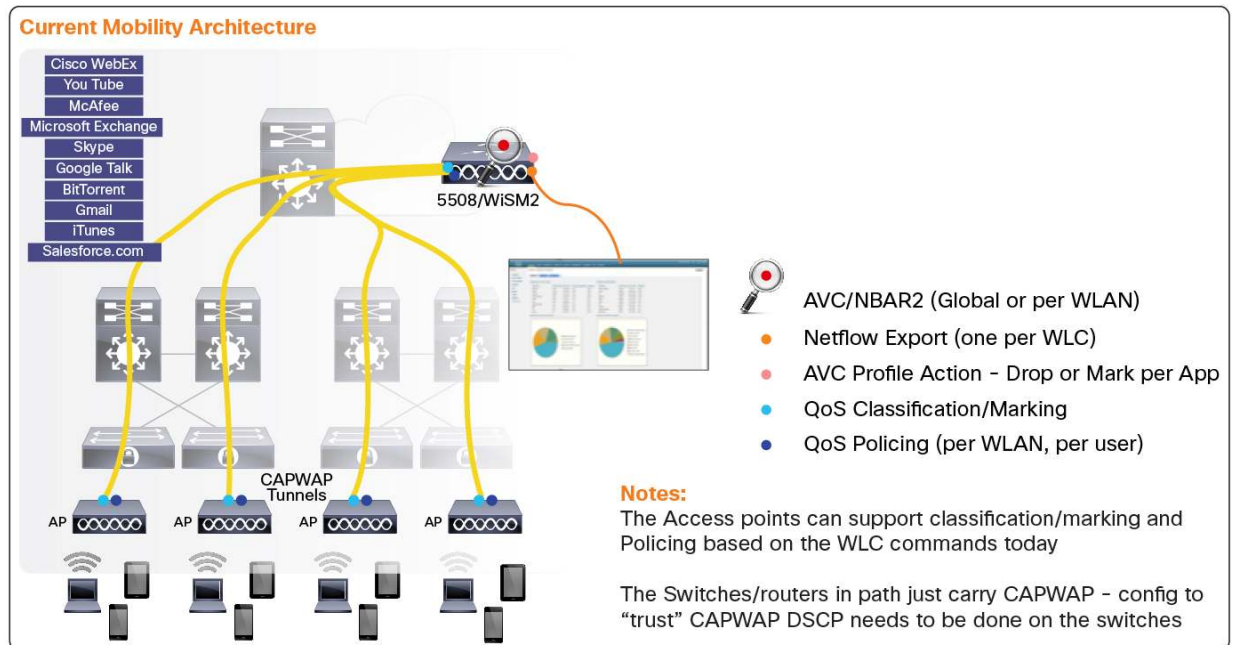
In the wireless world, where bandwidth is scarce and is a heavily shared medium, it becomes very important for the IT administrator to know how the bandwidth is used, what applications are running, are there any heavy-hitting users or applications bringing down the quality of experience for fair users.

With not much support on the access/campus distribution switches today on application visibility, the traditional Cisco Unified Wireless Network model deploys application visibility and export at the WLC where wireless traffic terminates (decapsulated).

Here is why AVC is important in this scenario:

- Wi-Fi is a shared medium with resource contentions - Effective bandwidth sharing is key
- Numerous apps - Voice, video, and data accessed over wireless - IT needs to provide a good user experience
- Detect heavy hitters and rogue applications
- WLC is point of wireless termination - Visibility and control are needed here
- Capacity planning, user baselining, performance assessment

The following is a representation of a Cisco Unified Wireless Network and the points where AVC can be deployed today:



Features like QoS are applied at the access points and the WLC. Note that the legacy QoS data plane does not exist on the access point, and the Cisco Common Classification Policy Language (C3PL) model is not supported yet on the access point. QoS configurations are pushed down to the access point from the controller and the access point can do marking/policing actions both toward the client and the switch (downstream and upstream). Note the QoS cannot be done based on NBAR2, as application visibility is not yet available on the access point (roadmap; see the next section).

The WLC supports NBAR2 for application visibility and can identify applications granularly and has the ability to export to NetFlow collectors. AVC is centrally managed by the WLC using its native GUI: It is possible to get global visibility reports per WLC, SSID-based reports, or client-based reports. WLC does not maintain historic data. To achieve this, one would have to deploy a NetFlow collector and export the data periodically. It is also possible to configure QoS based on precious metals - four categories of QoS. Each SSID/WLAN can belong to one category, and it is possible to specify QoS parameters on a per SSID or a per client basis. A given application can also be dropped by configuring the WLC accordingly. These policies are implemented on the WLC and the access point.

More details on deploying AVC in this scenario can be found at

http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bed910.shtml.

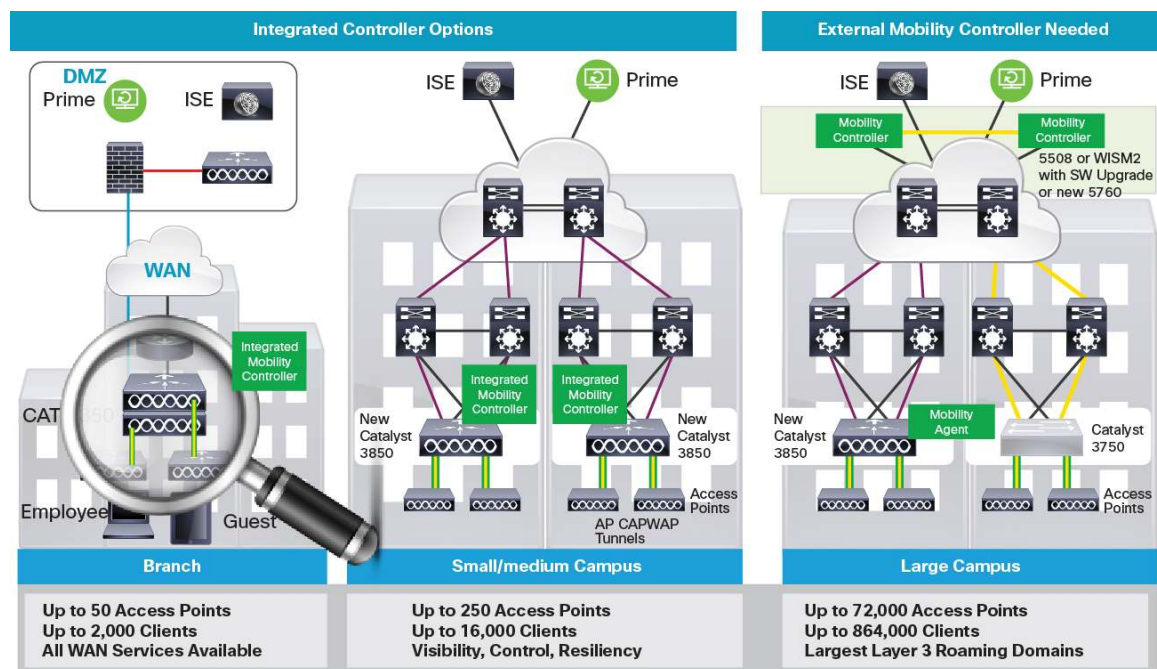
AVC for Converged Access

Note: AVC for converged access is in the roadmap and is being delivered in multiple phases.

Cisco's One approach - One Policy, One Network, and One Management - defines converged access. Increasing wireless traffic in the enterprise calls for architecture in which wireless traffic and wired applications/traffic can be deployed and managed in a consistent way. Having one model for wireless and one for wired is a maintenance challenge, requires deploying policies in different ways at different PINs, and would be need to managed and monitored separately. This is what the converged access model offers:

- Have one policy for wired and wireless clients, that is, policies that can seamlessly “move” when the user migrates from wired to wireless.
- One point of managing the policies - configuration and monitoring. The access device (3850) is capable of terminating wireless, and would be a single point of policy enforcement now. Policies for wireless can be deployed along with wired, at the access unlike the Cisco Unified Wireless Network model where wireless policies were administered on the WLC.
- One management station - Cisco Prime Infrastructure for managing the wired and wireless endpoints and applications in a unified way.

Following is a representation of the possible deployment models for converged access:

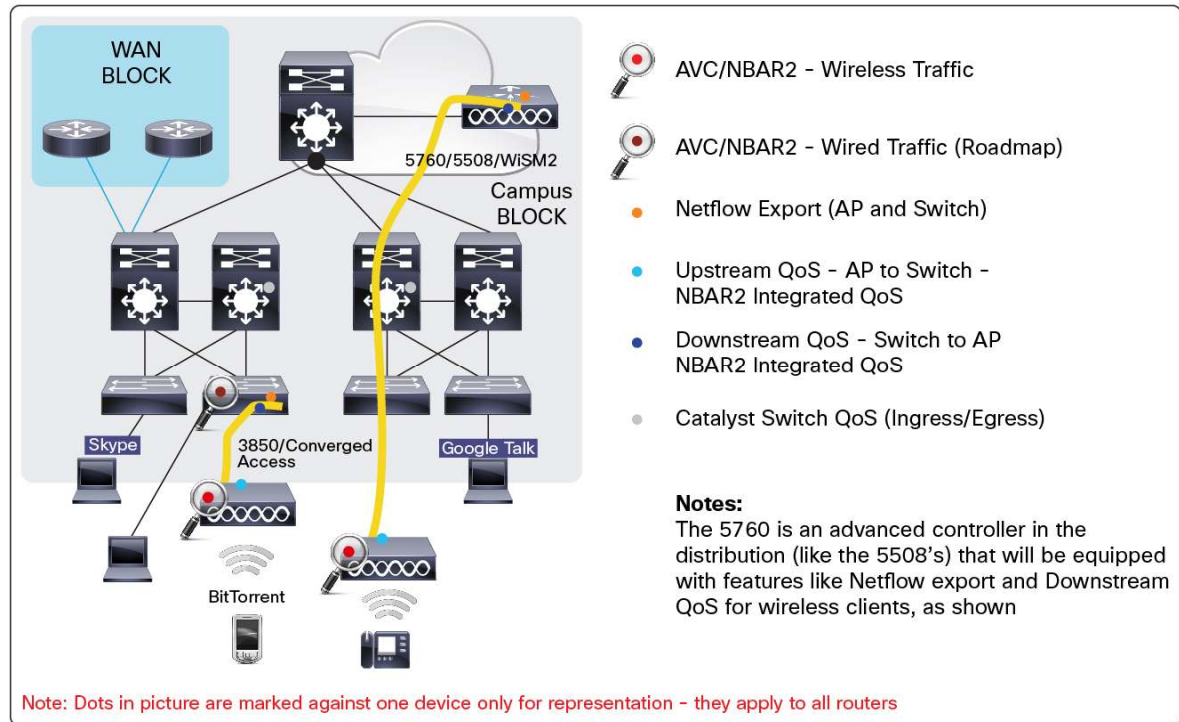


Why AVC is important for converged access:

- 3850 terminates wireless - Wired and wireless traffic converges here.
- Numerous apps - voice, video, and data - are accessed over wireless - IT needs to provide a good user experience for wired and wireless.
- Need common points of policy enforcement - What to prioritize.
- Easy ways to know application performance and visibility for wired and wireless.
- Need for user and application management with a common platform.

The key converged access business use cases where AVC would be imperative are bring your own device (BYOD)/mobility and video.

The following is a representation of the converged access network and where can AVC pictures be deployed:



The differences as compared to the Cisco Unified Wireless Network architecture for AVC would be that NBAR2 and NetFlow export need not happen only at the controller/WLC now. Here is a quick summary of how the features are enforced in this deployment model:

- For wireless traffic, NBAR2 would run on the access point and learn the applications.
- The learned information is sent to the switch using CAPWAP tunnels.
- For wired traffic, NBAR2 runs on the switch (limited Doppler capability and software).
- The switch does the collective NetFlow export for both wired and wireless traffic.
- QoS for downstream traffic (switch to access point) is done on the switch (3850).
- QoS for upstream traffic (access point to switch) is done on the access point - the access point is provisioned from the switch and like the Cisco Unified Wireless Network model has no direct access to the console.

Note that NBAR2 running on the switch would coexist with other Medianet solutions like Media Services and flow metadata that would also be a part of the switch's capabilities.

The following is a summary of what AVC capabilities can be deployed on what devices:

Platform	Classification	Performance Collection	Control
2504/5508/8500 Series WLC	NBAR2 (Version 7.4, PP 2.1) Protocol Pack support future (7.5)	NetFlow (fixed record)	QoS
5760	NBAR2 - Future: Cisco IOS-XE 3.3 (Darya, Q4CY13)	NetFlow (fixed record) for wireless traffic - Future: Cisco IOS-XE 3.3 (Darya, Q4CY13)	App-aware QoS policies for wireless - Future: Cisco IOS XE 3.4 (Amur, 1H CY14)
WISM2	NBAR2 (PP 2.1) Protocol Pack support future (7.5)	Flexible NetFlow (fixed record)	QoS

Platform	Classification	Performance Collection	Control
3850 Wireless	NBAR2 - Future: Cisco IOS-XE 3.3 (Darya, Q4CY13)	NetFlow (fixed record) for wireless traffic - Future: Cisco IOS-XE 3.3 (Darya, Q4CY13)	App-aware QoS policies for wireless - Future: Cisco IOS XE 3.4 (Amur, 1H CY14)

AVC for Perimeter Security/Firewall

AVC for perimeter security/firewalls is very important.

Today applications are complex, their behavior is complex, and their use from a variety of devices and locations is complex. Current access controls are based on IP addresses and ports, which work as the first strong layer of defense but don't go far enough. Where multiple applications traverse a port (like Internet-based applications on port 80) or an application hops ports (like Skype), additional controls are needed that are much more fine-grained. These controls need to identify the user, application, what the user is doing on the application, device characteristics, threat profile of the transaction, and so on.

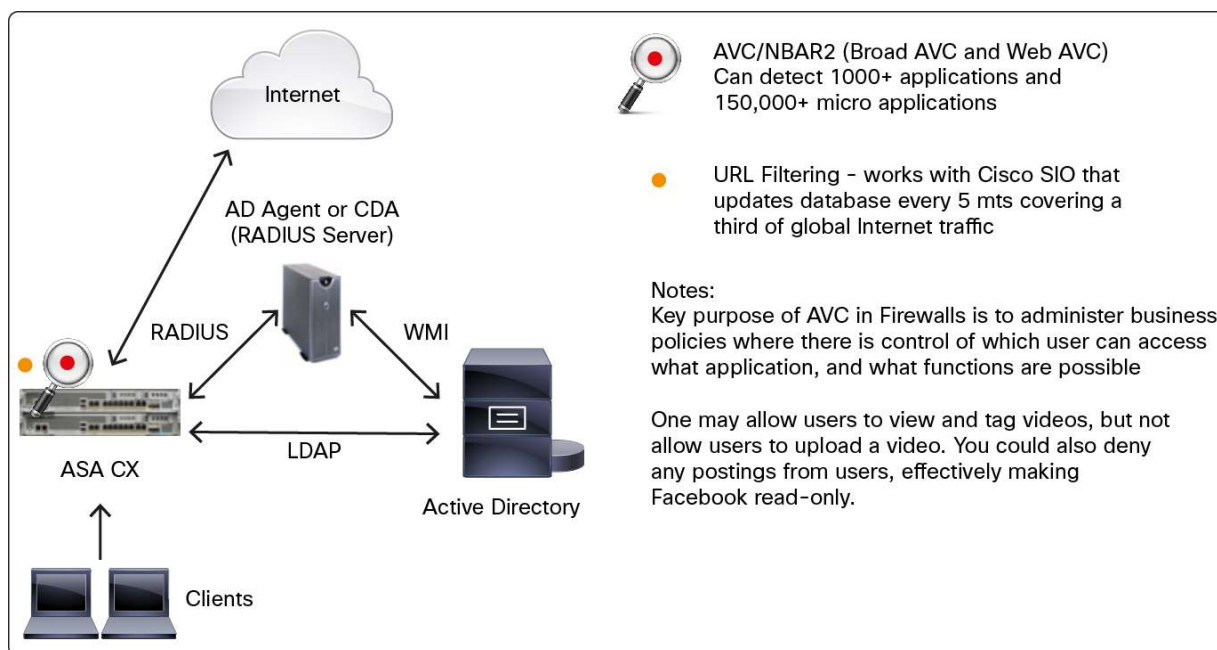
One of the key objectives of a context-aware firewall is to know which applications are being used by which user, when, and what exactly is being done. The ability to control access is totally contextual and the admin needs to be able to enforce policies at the level of business applications.

The need for next-generation firewalls (NGFWs) is to create policies that match the nuanced business needs of today - not just help identify applications, but also microapplications, categories, groups, and so on.

In addition to microapplications, ASA NGFW services also identify the application **behavior**, that is, what action the user is taking within that application. As an example, the Facebook videos category identifies whether the user is uploading, tagging, or posting a video. So an administrator may allow users to view and tag videos, but not allow users to upload a video. You could also deny any postings from users, effectively making Facebook read-only.

The key functions of AVC in the context of firewalls are to provide granular visibility, grouping, and control by allowing or denying access to application.

A typical ASA based AVC deployment would look like the following:



AVC Deployment Caveats

There are a few caveats when deploying AVC. These are prioritized roadmap items for AVC and would be addressed in the near future. If there are workarounds to this caveat, they are listed in the following table:

Today's Limitation	Impact	Workaround
NBAR2 - Cannot run NBAR2 on the WAN when WAAS or WAAS-X is used	<ul style="list-style-type: none">• Can't classify WAN applications using NBAR2• Can't apply QoS policies based on NBAR2 signatures	Apply NBAR2 on the LAN interface
NBAR2 - Cannot run NBAR2 on the WAN when MPLS is used	<ul style="list-style-type: none">• Can't classify WAN applications using NBAR2• Can't Apply QoS policies based on NBAR2 signatures	Apply NBAR2 on the LAN interface
PA can't work with WAAS	<ul style="list-style-type: none">• Inaccurate ART measurements when WAAS is enabled• Required to use NAM for flow agent	Use WAAS flow agent
PA not supporting VRF with overlapping IPs	<ul style="list-style-type: none">• No ART reporting with overlapping IP	N/A
PfR and WAASx can't work together	<ul style="list-style-type: none">• Not a well-tested scenario	N/A
No support for asymmetric routing	<ul style="list-style-type: none">• No NBAR2 classification - Limited QoS• No ART• AVC requires router seeing traffic in both directions	N/A
Can't run NBAR2, PfR on with crypto map/GETVPN	<ul style="list-style-type: none">• NBAR2, PfR cannot be applied to the same interface that has crypto map enabled (GETVPN, traditional IPsec using crypto map)	Run NBAR2 on the LAN interfaces No PfR workaround
PfR's limited scalability	<ul style="list-style-type: none">• Only use PfR for < 200 sites	Target discovery when available
No PfR support with AppNav	<ul style="list-style-type: none">• PfR is not operational with AppNav	N/A
No PfR IPv6 support	<ul style="list-style-type: none">• Can't use PfR with IPv6 traffic/applications	N/A
Can't attach FNF to a virtual template	<ul style="list-style-type: none">• EZ/FlexVPN and PPP can't export NetFlow data	Configure FNF only on LAN interfaces

AVC Enablement with Cisco Prime Infrastructure

Cisco Prime Infrastructure provides a single integrated solution for comprehensive lifecycle management of the wired/wireless access, campus, and branch networks, and rich visibility into end-user connectivity and application performance assurance issues.

The following sections summarize the process to download and install the software and describe the AVC configuration and usage in detail.

Cisco Prime Infrastructure Download

The evaluation version of the Cisco Prime Infrastructure 2.0 software is available from Cisco Marketplace at <http://www.cisco.com/go/nmsevals>. It includes a built-in evaluation license for 60 days, 100 devices.

Installation

The software is packaged as an OVA (Open Virtualization Archive) that comes preinstalled with a 64-bit Red Hat Enterprise Server 5.4 operating system. An Express Edition of the Virtual Appliance is required at a minimum. The ESX/ESXi version supported is 5.0.

For further details on the server specs, please refer to the Cisco Prime Infrastructure Deployment Guide.

Once you download the OVA, use the VMware vSphere client to deploy the OVA. Once the OVA is deployed and the virtual machine is powered on, enter the setup mode and provide all the network details as prompted. This completes the server configuration.

Point the browser to http://IP_Address to access Cisco Prime Infrastructure from the web. Use the root password to log in that you had configured during the server installation. The supported browsers are Internet Explorer (with the Chrome Plug-in), Mozilla Firefox, and Google Chrome.

AVC Configuration

AVC-Supported Platforms

Please refer to the following table, which lists the software versions required for the respective platforms in order to turn on AVC:

Platform	Minimum Software Version Required
ASR 1000	15.3(1)S1 and later
ISR G2	15.2(4)M2 and later
CSR 1000	15.3(2)S
ISR 4451-X	15.3(2)S
WLC	7.4

Prerequisites

The following table lists prerequisites for various device types:

#	Device Type Applicable for	Prerequisite	Link
1	Wired and wireless	Make sure that the devices on which you would like to enable AVC are fully managed (In the Device Work Center [DWC]).	See the "Preparing the Network" and "Device Discovery" sections in the Appendix.
2	Wired and wireless	Make sure that the sites are created and the endpoints (devices) on which you would like to enable AVC are associated with the corresponding sites. This is required to view all the site-related dashlets.	See the "Device Discovery" section in the Appendix.
3	Wired devices	Interface role should be created before using the template.	See the "Interface Roles Configuration" section.

Interface Roles Configuration

The idea behind the interface role is that you group a set of interfaces according to a set of rules and apply the AVC configuration for that group of interfaces. Hence, it is a good practice to assign a meaningful description to all interfaces. A good example is to use an interface description such as the following:

LAN Interfaces: assign name LAN in the description field:

```
interface GigabitEthernet0/0/0
description -- LAN - PARIS --
ip address 10.10.15.1 255.255.255.0
service-policy type performance-monitor input PrmAM_AVC_mon_in
service-policy type performance-monitor output PrmAM_AVC_mon_out
```

WAN Interfaces: assign name WAN in the description field:

```
interface GigabitEthernet0/0/1
description -- WAN - ASR2 -
ip address 100.1.2.1 255.255.255.0
```

Within Cisco Prime Infrastructure, browse to **Design → Shared Policy Objects** and then select **Interface Role**.

Create two new interface roles:



From there you can deploy the AVC template and use one of the two interface roles, LAN or WAN, based on where you would like to apply the AVC features.

Protocol Pack Update

Traditionally, protocols were linked to Cisco operating software and customers had to upgrade Cisco operating software to get new protocol support. Protocol Packs are a set of protocols developed and packaged together, and provide a means to distribute new protocols, protocol updates, and bug fixes outside the Cisco operating software releases, and can be loaded on the network devices without replacing the Cisco operating software.

This is a two-step process. First the user has to download the protocol pack from Cisco.com and apply it on the device. The second step consists of adding this information in Cisco Prime Infrastructure. The following sections detail these two steps.

Download Location

Users can download Cisco IOS (ISR G2) and Cisco IOS-XE (ASR 1000) Protocol Packs from the Cisco.com software download page.

Cisco.com Location for ISR G2:

[Download Home](#) → Products → Routers → Branch Routers → Cisco 3900 Series Integrated Services Routers → Cisco 3945 Integrated Services Routers → software on chassis → NBAR2 Protocol Packs.

Cisco.com Location for ASR 1000:

[Download Home](#) → Products → Routers → Service Provider Edge Routers → Cisco ASR 1000 Series Aggregation Services Routers → Cisco ASR 1006 Router → NBAR2 Protocol Packs.

Applying Protocol Pack on the Devices

The compatible protocol pack must first be copied locally to the router.

Commands	Description
ip nbar protocol-pack <protocol pack file> [force]	Loading the Protocol Pack on to the device. The <protocol pack file> can be loaded from either the disk or flash, that is, anything that is local to the router.
no ip nbar protocol-pack flash0:pp_file	Unloads the previously loaded protocol pack.
show ip nbar protocol-pack active	View the details of the current active Protocol Pack.
show ip nbar protocol-pack <protocol pack file>	View the details of a nonloaded Protocol Pack file.

Applying Protocol Pack on Cisco Prime Infrastructure

Once the device is updated with the new Protocol Pack, the next step is to update Cisco Prime Infrastructure with it. Browse to **Administration → Software Update → Upload Update File**. Now click the browse button to locate the protocol pack ubf file and upload. You will then have to restart the Cisco Prime Infrastructure server by logging into the server as “admin” and performing the following: “ncs stop” followed by “ncs start”.

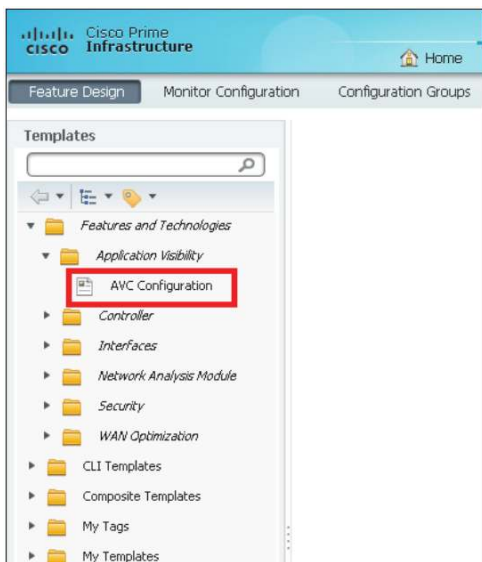
AVC Configuration and Activation

Enabling AVC on Routers

There are two ways in which you can enable AVC on the routers. The first method is by using the AVC configuration template. The second method is a one-click option. Both of these are described below.

Using Template

A predefined AVC template is available that can be used to turn on AVC on the ASR 1000s and the ISR G2s. This option of using the template is helpful when you are trying to enable AVC on a number of devices simultaneously or if you would like to further customize the AVC configuration. Browse to **Design → Feature Design**. Here under the Features and Technologies folder you will find the Application Visibility folder, which contains the AVC template:



This template consists of three main sections.

a. Template Basics

Features and Technologies > Application Visibility

AV Configuration

▼ Template Basic

*Name

Description

Tags

Author

Feature Category **AV Configuration**

This section contains the basic information regarding the template itself. The template name is a mandatory field. You will need to remember this name in order to deploy this template.

b. Device Information

The screenshot shows the 'Device Information' section of a configuration interface. It is divided into two expandable sections: 'Validation Criteria' and 'Template Detail'. Under 'Validation Criteria', there is a field for '*Device Type' with a dropdown menu currently set to 'Routers', and an 'OS Version' field. Under 'Template Detail', there is a field for '*Apply to Interface Role' with a dropdown menu.

This section allows the user to tie the template to a family of device types (for example, Cisco ASR 1000 Series Aggregation Services Routers) or a specific device type (for example, Cisco ASR 1001 Router). It also mandates to choose an Interface Role on which the AVC feature will be enabled. Choose the one that you created in the previous step. The OS Version field is optional.

c. AVC Monitoring Tools Configuration

The next few sections of the template allow the user to configure the different technologies involved with the AVC solution.

1. Traffic Analysis

This section focuses on configuring the traffic statistics that enable the user to view all the applications, top clients, traffic over time, and so on. Choose the traffic type in the “IPs, Subnets” field.

The screenshot shows the 'Traffic Statistics' configuration section. It includes a toggle switch for 'On/Off', a dropdown menu for 'IPs, Subnets' currently set to 'Any IPv4', and a label for 'Applications' set to 'ANY'. Below these fields is an 'Advanced Options' link.

2. HTTP URL Visibility

This section primarily focuses on HTTP URL Visibility. Choose individual IP's or a Subnet to enable this feature in the “IPs, Subnets” field by clicking the Down arrow icon as shown below.

The screenshot shows the 'HTTP URL Visibility' configuration section. A dropdown menu for 'IPs, Subnets' is open, showing options: 'Any IPv4', 'IPv4 Host', 'IPv4 Subnet', 'Any IPv4' (highlighted), and 'Any IPv6'. The background shows the 'On/Off' toggle, the 'IPs, Subnets' field, and a list of applications including 'Flash Myspace' and 'RealMedia Traffic'. There are also minus and plus buttons for the application list, and 'OK' and 'Cancel' buttons for the dropdown.

Pick the applications that you are interested in monitoring. These applications are based on HTTP as the underlying protocol. By default, 32 applications are chosen. Note that this feature is not applicable for the ISR G2 routers. You could use the Advanced Options to change the sampling rate and the direction.

3. Application Response Time

This section focuses on configuring Cisco IOS Performance Agent to collect the application response time metrics to measure the end-user's experience. Choose individual IP's or a subnet to enable this feature in the "IPs, Subnets" field. For the "Applications" field, either use the default option, "Any TCP", or choose from the list of NBAR applications, categories, or attribute values.

The screenshot shows the "Application Response Time" configuration panel. It includes a toggle switch for "On" and "Off". The "IPs, Subnets" field is a dropdown menu currently set to "Any IPv4". The "Applications" field is a dropdown menu currently set to "Any TCP". Below these fields is an "Advanced Options" section with a "Sampling Rate" dropdown menu set to "No Sampling".

You could use the Advanced Options to change the sampling rate.

4. Voice/Video Metrics

This section focuses on turning on some of the Medianet capabilities. It deals with exporting RTP metrics for the RTP-based traffic. Choose individual IPs or a subnet to enable this feature in the "IPs, Subnets" field.

The screenshot shows the "Voice/Video Metrics" configuration panel. It includes a toggle switch for "On" and "Off". The "IPs, Subnets" field is a dropdown menu currently set to "Any IPv4". The "Applications" field is a dropdown menu currently set to "Real-time Transport P... Telepresence Media".

For the "Applications" field, you can choose either "Real Time Protocol" or "Telepresence Media" or both.

Tip: By default all of the above four technologies are enabled. You can turn off any that are not required.

Once the above template is configured, click **Save as New Template**. Choose the folder where you would like to place the template and click **Save**. You will see the template appear under the folder you had previously chosen. You will now have the option to deploy this template, that is, to push this configuration onto the device. Click **Deploy**. It will then take you to the **Template Deployment - Prepare and Schedule** screen as shown below.

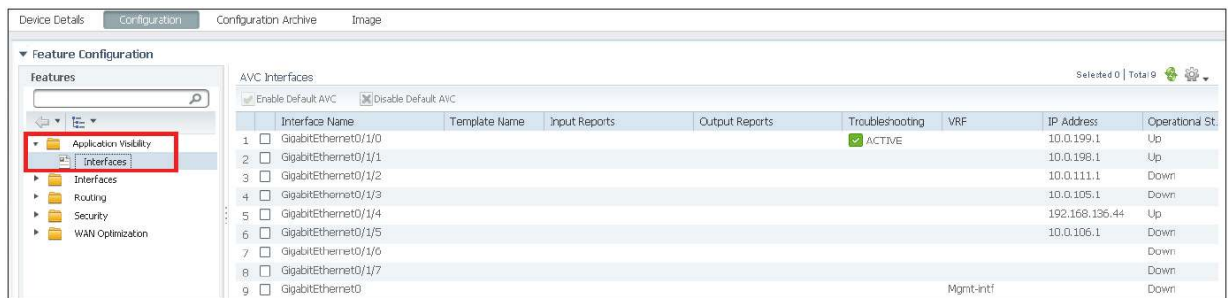
The screenshot shows the "Device Selection" screen. It includes a checkbox for "Show All Devices" which is checked. Below this is a table with columns: Name, Description, Type, IP Address/DNS, and Vendor. The table lists several device groups: ALL, Device Type, Site Groups, and User Defined. The "Show" dropdown menu is set to "All".

Name	Description	Type	IP Address/DNS	Vendor
<input type="checkbox"/> ALL	All Members			
<input type="checkbox"/> Device Type	Device Type			
<input type="checkbox"/> Site Groups	Site Groups			
<input type="checkbox"/> User Defined	User Defined Device Groups			

Select the device(s) that you would like to deploy with this template to enable AVC. By default, this shows only supported devices; that is, even if you select ALL, you will see all of the supported devices only and not all the devices in your inventory. You can preview the CLI by clicking the CLI Preview tab. Then click OK. By default, this job is scheduled to run immediately. For a future date and time, look at the Schedule section at the bottom of the Template Deployment screen. Once this is done, the job is created to deploy the template. Once the job has completed, then AVC is turned on, on your respective devices. To view the status of the job, browse to **Administration → Jobs Dashboard → User-Defined**.

One-Click Enablement Through DWC

This option is useful when you would like to turn on AVC for a particular supported device with all the AVC configuration options as seen in the template in the previous section. The prerequisite is that the device on which you would like to enable AVC should already be managed by Cisco Prime Infrastructure. Browse to **Operate → Device Work Center**. Locate the device on which you would like to enable the AVC feature. You can either filter by the device name or the IP address from the device table or use the site groups or device type to identify the device. Once you identify the device, click the device to view detailed information. Click **Configuration → Application Visibility → Interfaces** as shown below:



Select an interface on which you would like to enable AVC and click the **Enable AVC** button. Select the IPV4 default Policy. This one-click action will enable AVC on the device chosen.

Note that this one-click action is enabled only if previously there was no AVC configuration through the template. Addition and disable is only available to default AVC policy deployed through this one click.

Enabling AVC on Wireless Controllers

In order to enable AVC on the controllers, NetFlow should first be configured since the application-related metrics are exported through NetFlow to Cisco Prime Infrastructure. For this, an exporter must first be configured and then the monitor and finally AVC configuration. If NetFlow is already configured then you can skip the two following steps and directly configure AVC.

Exporter Configuration

Browse to **Design → Feature Design → Features and Technologies → Controller → NetFlow** and click **Exporter**. Fill in the template name, exporter name. The exporter IP will be the Cisco Prime Infrastructure's IP address. The port would be 9991.

The screenshot shows the 'Feature Design' tab with the 'Monitor Configuration' sub-tab selected. The left sidebar shows a tree view of templates, with 'NetFlow' expanded and 'Exporter' selected. The main area displays the 'Exporter' configuration form. The 'Template Basic' section includes fields for *Name, Description, Tags, and Author (set to 'prime'). The 'Validation Criteria' section includes *Device Type (set to 'CUWN (default)') and OS Version. The 'Template Detail' section includes fields for Exporter Name, Exporter IP, and Port Number (set to 0).

Click **Save as New Template**. Choose the folder where this template is to be saved. Then click **Deploy**, which then launches the screen to choose the device on which this template has to be deployed. Once this step is completed, you can see the status of this job at **Administration → Jobs Dashboard**.

Monitor Configuration

Browse to **Design → Feature Design → Features and Technologies → Controller → NetFlow** and click **Monitor**. Fill in the template name, and for the exporter name, pick the exporter that was configured in the previous step. Note that unless the exporter template created in the previous step is deployed on the WLC, it will not show up here as an option in the drop-down list for the Exporter name field in this Monitor template.

The screenshot shows the 'Feature Design' tab with the 'Monitor Configuration' sub-tab selected. The left sidebar shows a tree view of templates, with 'NetFlow' expanded and 'Monitor' selected. The main area displays the 'Monitor' configuration form. The 'Template Basic' section includes fields for *Name, Description, Tags, and Author (set to 'prime'). The 'Validation Criteria' section includes *Device Type (set to 'CUWN (default)') and OS Version. The 'Template Detail' section includes fields for Monitor Name, Record Name (set to 'ipv4_client_app_flow_record'), and Exporter Name (set to 'none').

Save this template and deploy it on the WLC.

AVC Profile Configuration

The AVC profile provides the “control” to the AVC solution. This profile allows you to take appropriate actions on the specific applications once recognized. For example, if you would like to drop all the YouTube traffic, then you can use the AVC profile to do so.

Browse to **Design → Feature Design → Features and Technologies → Controller → Application Visibility and Control → AVC Profile**. Fill in the template name, device type, and the AVC profile name. Add a row to the AVC rules list. Here you will be able to pick an application from the drop-down list and tag appropriate actions to this application, for example, Mark or Drop. Click **Save**. Below is the screenshot.

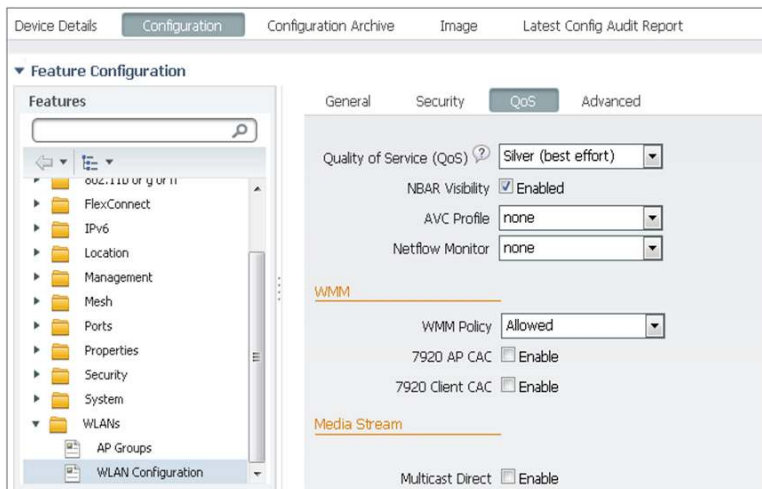
The screenshot displays the 'AVC Profile' configuration page. On the left, a tree view shows the navigation path: **Features and Technologies** > **Application Visibility** > **Controller** > **802.11** > **802.11a or n** > **802.11b or g or n** > **Application Visibility And Control** > **AVC Profile**. The main configuration area is titled 'Features and Technologies > Controller > Application Visibility And Control' and 'AVC Profile'. It contains several sections: 'Template Basic' with fields for Name, Description, Tags, Author (set to 'prime'), and Feature Category (set to 'AVC Profile'); 'Validation Criteria' with fields for Device Type (set to 'CUWN (default)') and OS Version; and 'Template Detail' which includes an 'AVC Profile Name' field and an 'AVC Rule List' table. The table has columns for Application Name, Application Group Name, Action, DSCP, and DSCP value (0 to 63). A single rule is listed with Application Name 'youtube', Application Group Name 'voice-and-video', Action 'Drop', and DSCP value '0'. The table also shows 'Selected 1 | Total 1' and 'Show All' options.

This is not a mandatory requirement. You will only need to create an AVC profile if you would like to control the specific application.

AVC Configuration

AVC configuration is applied to a specific WLAN. If the WLAN is already created, then the below steps help you to enable AVC.

From the Device Work Center, locate the WLC and browse to **Configuration → WLANs → WLAN Configuration**. Click the WLAN on which you would like to enable AVC and browse to the QOS section. Here select the QOS, enable NBAR, and pick the NetFlow monitor and the AVC profile that you have configured in the previous steps.

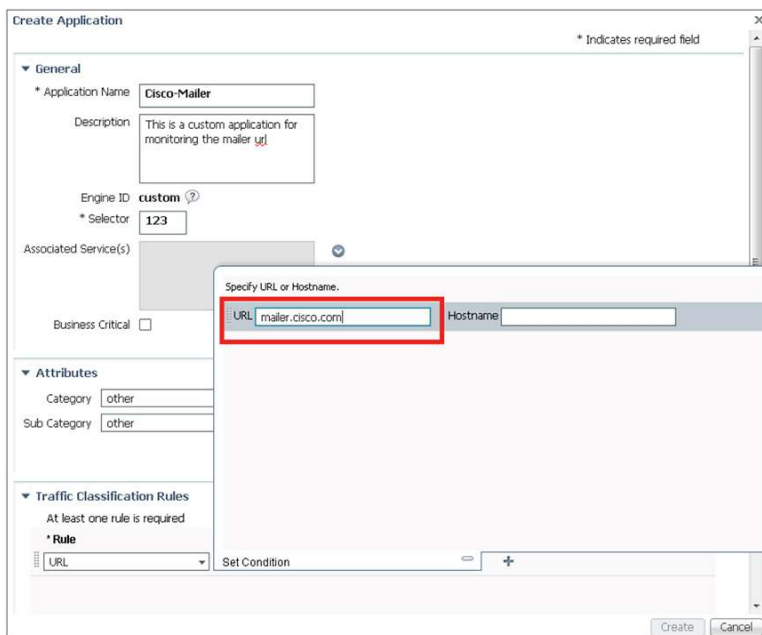


Once you save this template, AVC is turned on for the WLC.

If you need to configure a new WLAN in order to enable AVC, in situations where a new site is to be created for example, then you can use the WLAN template available under **Design → Feature Design → Controller → WLAN's → WLAN Configuration**. Here specify all the details for this new WLAN and browse to the QoS tab and enable NBAR Visibility. Also add the AVC profile and NetFlow monitor as configured in the previous sections.

Custom Application Creation

Cisco Prime Infrastructure helps to create custom applications that you can deploy on the device and let Cisco Prime Infrastructure monitor these applications. Browse to **Operate → Applications and Services**. Click the **Create** button. Provide an application name and the selector ID. Check the **Business Critical** box if you would like this custom application to be marked so. Refer to the later "Which Applications May Be Having Performance Issues?" section to obtain a deeper understanding of monitoring business-critical applications. Scroll down to the Traffic Classification Rules section. To create a URL-based application, choose the rule as **URL** and provide the URL info as shown below. Then click the **Create** button.



Then choose this application created and follow the next set of screens, which helps to deploy this configuration on the device.

Advanced System Settings

There are some settings in Cisco Prime Infrastructure that need to be looked at closely before you start to manage the network. Settings according to common operational practices are already configured, but you may need to tweak the settings based on the network you are managing. You can access the settings by navigating to **Administration → System Settings**.

Data Retention

This menu item within system settings allows you to specify how much data is to be stored in Cisco Prime Infrastructure. By default you can store the performance data as short, medium, and long-term data for 7, 31, and 378 days, respectively. You can increase these numbers based on the hard drive space that is provided to Cisco Prime Infrastructure.

Data De-duplication

This menu item within system settings allows you to change the data source for a given site. For example, if you have a NAM at the San Francisco branch as well as NetFlow data being sent from that branch, how would Cisco Prime Infrastructure know which source to use? While this can be done automatically, you can override the system and define a specific source for a particular site at this location.

Monitoring/Visualizing AVC

Cisco Prime Infrastructure provides a very easy and flexible model for monitoring your wired/wireless network. Cisco Prime Infrastructure allows you to define or "design" monitoring templates that dictate how and what you want to monitor. You can then turn on monitoring by deploying the monitoring template. The results are then shown in the form of dashboards, dashlets, and reports.

Monitoring Dashboards

The Dashboards that provide Assurance-related information are:

- a. Operate → Performance → Service Assurance
- b. Operate → Performance → Service Health
- c. Operate → Detail Dashboards (all of the dashboards)

Use Cases Workflow

The following sections describe how Cisco Prime Infrastructure can be used to visualize application visibility. For an overview of all the use cases, please refer to the "AVC Technology Overview" section.

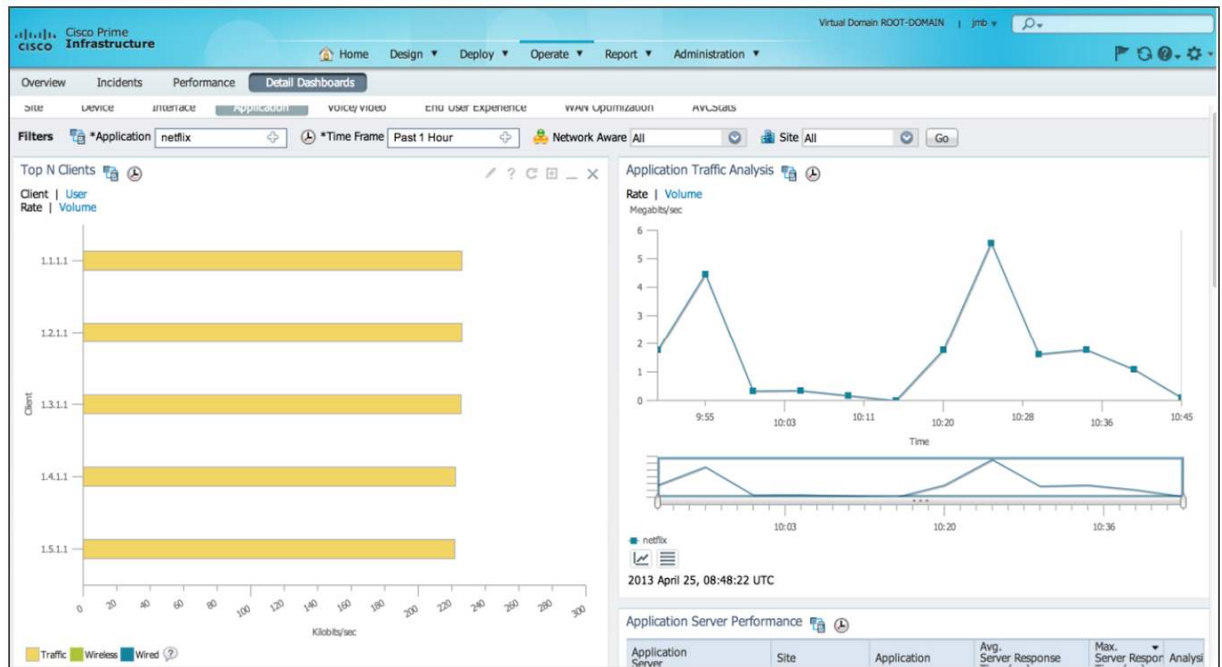
Discover Application Usage in the Network

Top Applications

Global View

For a global view of all application running across your network, browse to **Operate → Performance or Home → Performance** and select **Service Assurance**.

By clicking a specific application in the Top N Applications dashlet, you are redirected to the Application detail dashboard tab where you get all the details about this application. In this example, we can look at the Netflix application and get the IP addresses of the most demanding users:



You can list the top clients as well as the top servers by looking at the Top N Clients and Top N Servers dashlets.

This could be useful to track who is using this application. If Cisco Prime Infrastructure is linked to Cisco ISE, then you will obtain the username instead of the IP address.

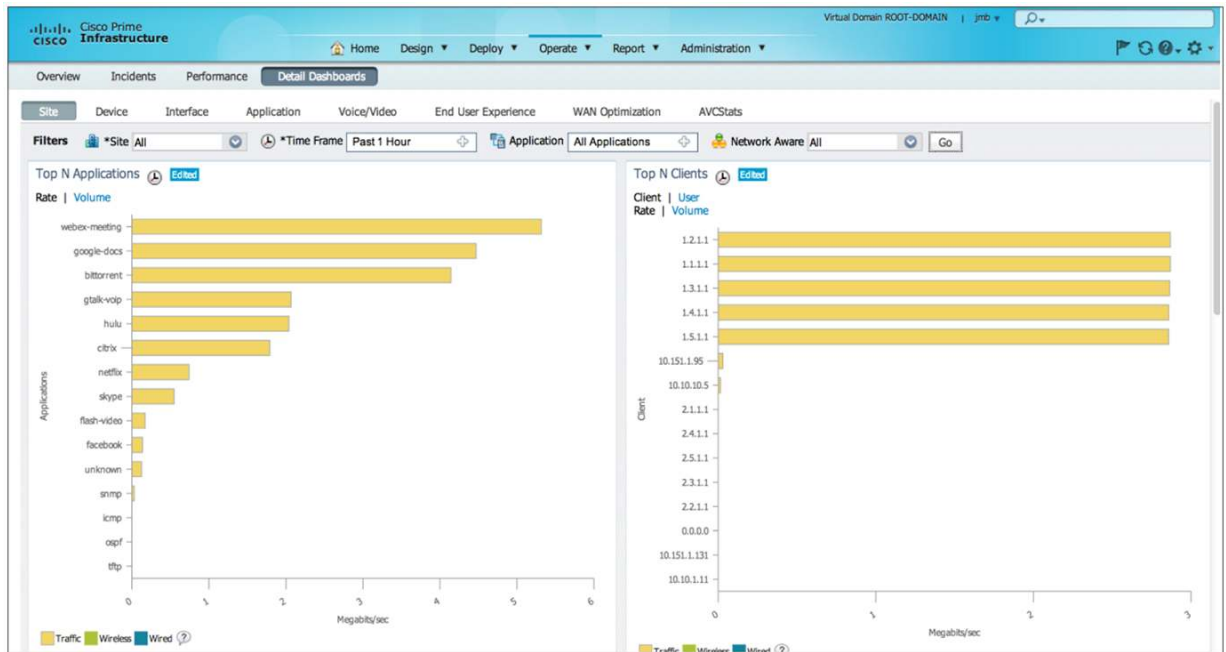
The dashlet Application Traffic Analysis is also a good way to track the bandwidth usage for this application over time.

Detailed View

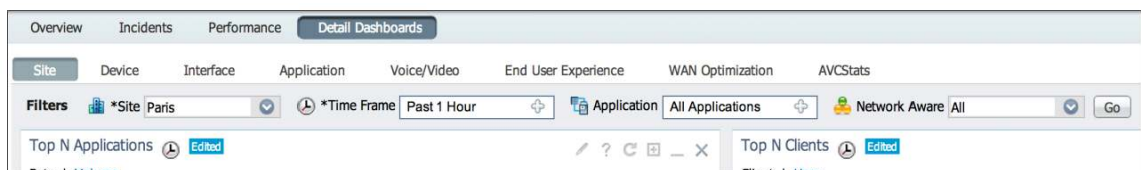
The **Home → Performance → Service Assurance** dashboard is a first step to check the overall application usage. But you may want to navigate for details on a specific site or on a specific device, or even to a specific interface to track a potential issue.

Browse to **Operate → Detail Dashboards** or **Home → Detail Dashboards** and select the **Site** tab.

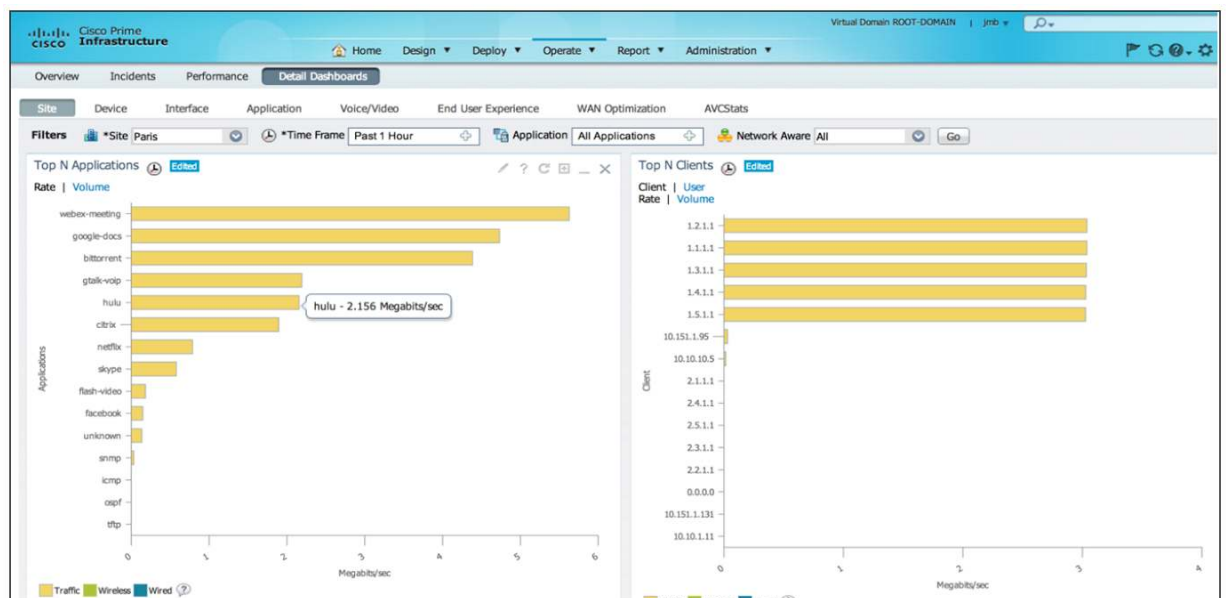
One of the main dashlets is the Top N Applications, which will give you the top 15 applications running over your network. This is the same dashlet that we have used before.



But note that you have a new option with the Filters ribbon above the current dashboard:



You can filter by site (here the filter is based on the Paris site) to get details on a specific site.



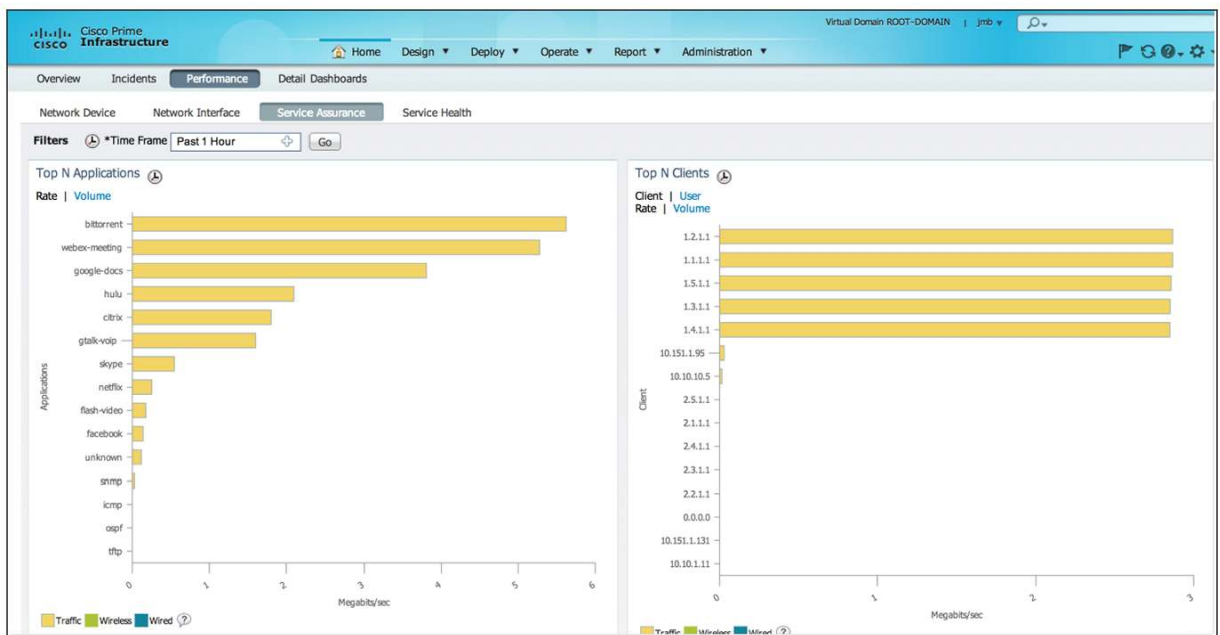
From there you can also navigate to a specific application for the Paris site and check the usage in terms of rate and bandwidth.

Top Talkers (Client and Server)

Global View

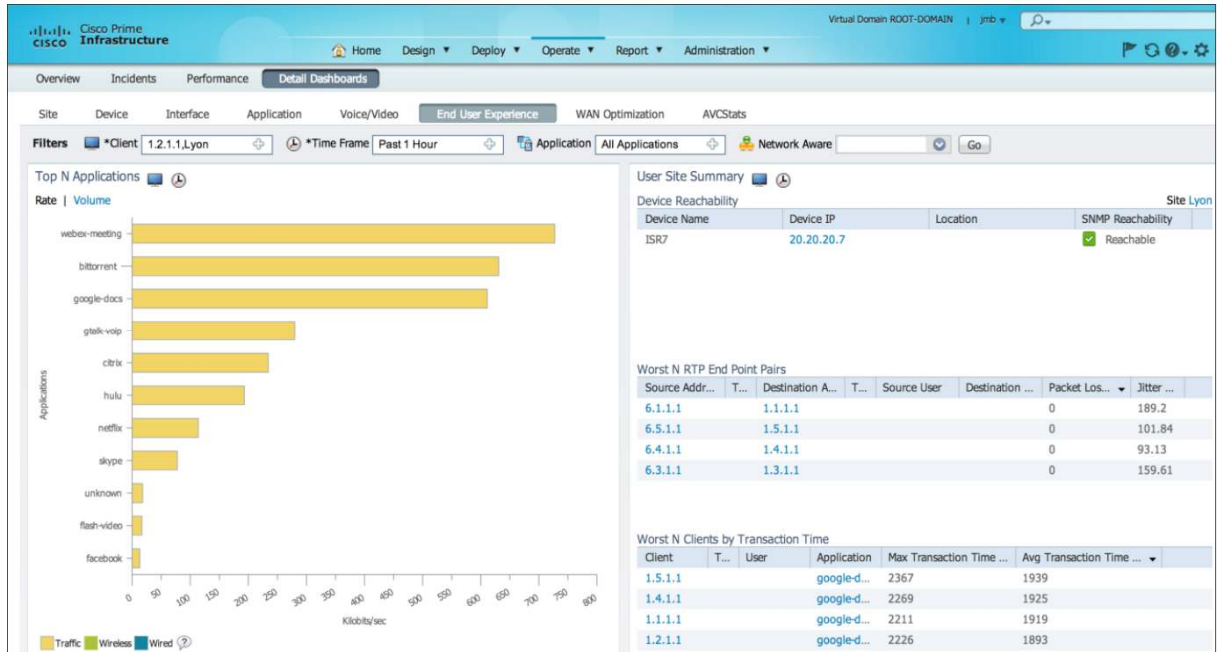
Browse to **Operate → Performance** or **Home → Performance** and select **Service Assurance** tab. You can get the list of top clients as well as the top servers in addition to the top applications.

- The dashlet called Top N Clients, which will give you the list of the source top talkers in terms of bandwidth usage.
- The dashlet called Top N Servers, which will give you the list of the destination top talkers in terms of bandwidth usage.



As mentioned before, when you click a specific application in the Top N Applications dashlet, you are redirected to the **Operate → Detail Dashboard → Application** tab where all the information listed is related to this application. You can get the list of the top clients for this application.

When you click a specific IP address in the client or server dashlet, you are redirected to a more detailed view under End User Experience. In this example you can see that IP address 1.2.1.1/32 is in the Lyon site:



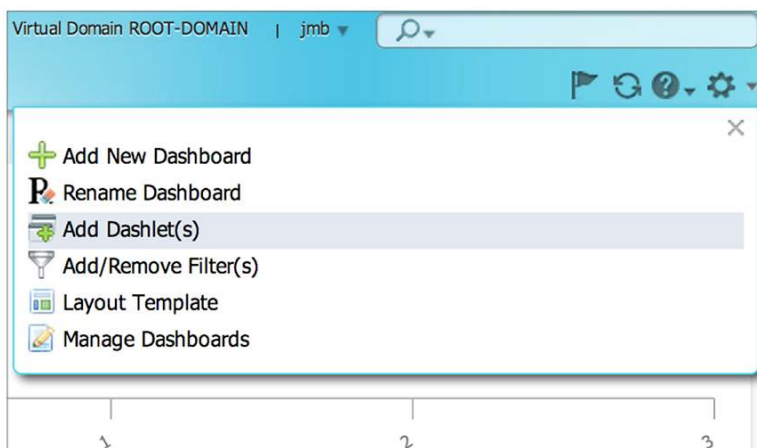
Detailed View with Filtering Options

If you want additional filtering options, for example, you want to get the top talkers on a specific site, then you have to browse to **Operate → Detailed Dashboard** (or **Home → Detailed Dashboard**) and select the **Site** tab. You can also get the list of top clients in addition to the top applications by checking the dashlet called Top N Clients. This is the same dashlet as in the Service Assurance dashboard describe above.

Note that you also get a split between the wireless clients and the wired clients.

You can also have the list of the top servers by adding the Top N Servers dashlet to this page (this is not enabled by default on this dashboard with Cisco Prime Infrastructure 2.0).

Click in the top right and select **Add Dashlet(s)**.

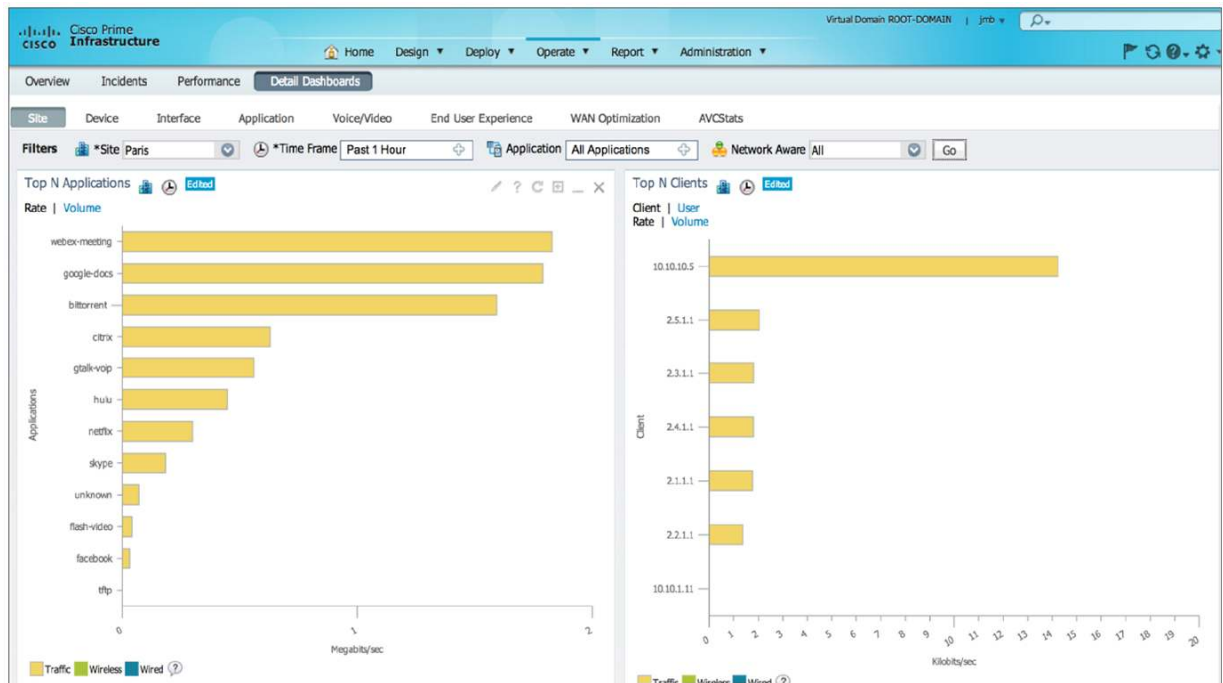


Then select Top N Servers under the Site dashlets.

This example is a good illustration of the flexibility - you can personalize all dashboards by adding dashlets. You can also create an additional dashboard and add the dashlets that you want.

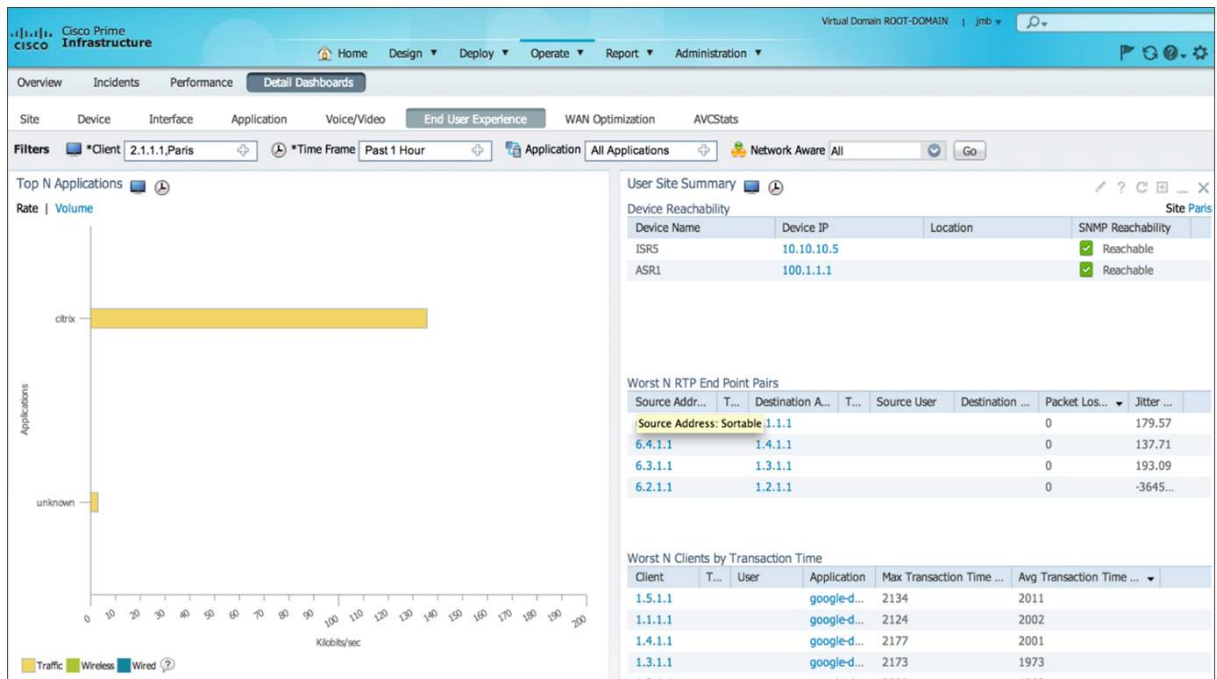
As mentioned before, when you click a specific application in the Top N Applications dashlet, you are redirected to the **Operate** → **Detail Dashboard** → **Application** tab where all the information listed is related to this application. You can get the list of the top clients/servers for this application.

Now, we can filter on the Paris site. In the filter ribbon, select Paris:



Now you get the top clients and servers for the Paris site. You also get the top application as explained before.

From there you either click an application and go to the Application detailed dashboard or click a specific address and go the End User Experience detailed dashboard.



Busiest Site/Location

Browse to **Operate** → **Detail Dashboards** and click **Application**. You can look at the Worst N Sites by ART Metrics. This would give you an idea as to how busy the sites are that they start experiencing larger transaction times for the applications.

Overview Incidents Performance Detail Dashboards				
Site	Device	Interface	Application	Voice/Video End User Experience
Filters *Application All Applications + *Time Frame Past 1 Hour +				
Worst N Sites by ART Metrics				
Selected Metric : Transaction Time				
Site	Application	Maximum Transaction Time (ms)	Average Transaction Time (ms) ▼	
India Branch	sap	153100	37903	
India Branch	citriximacient	161188	21765	
RTP Branch	unknown	61956	20558	
Management Apps	cisco-callmanager	28119	17774	
Amsterdam Branch	unknown	14600	11948	

You can also browse to **Operate** → **Performance** and click **Service assurance**. You can look at the Top N WAN Interfaces.

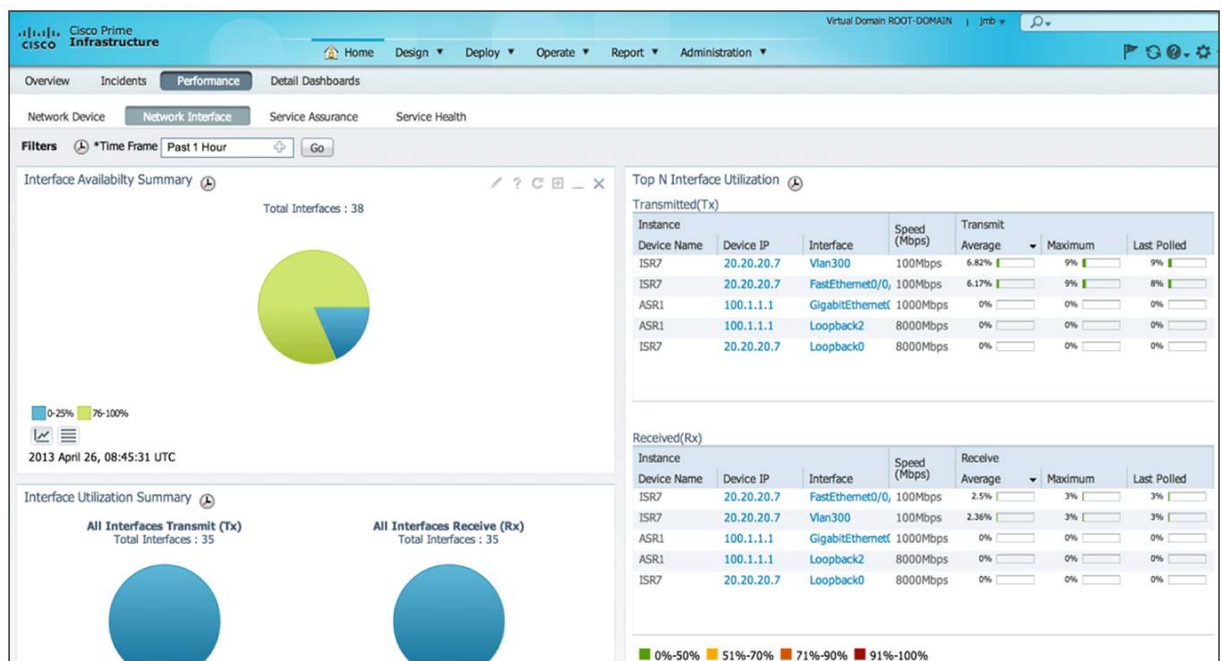
Site	Device	Interface	Maximum Utilization	Average Utilization
London Branch	10.11.1.1	GigabitEthernet0/0	86% <div><div></div></div>	77.48% <div><div></div></div>
Los Angeles Branch	10.0.102.2	GigabitEthernet0/0	5% <div><div></div></div>	2.29% <div><div></div></div>
Unassigned	10.0.103.1	GigabitEthernet0/1	2.5% <div><div></div></div>	2.29% <div><div></div></div>
Unassigned	192.168.152.1	GigabitEthernet0/1	3% <div><div></div></div>	2.17% <div><div></div></div>
New York Branch	10.0.104.2	GigabitEthernet0/0	3% <div><div></div></div>	2.09% <div><div></div></div>

■ 0%-50%
 ■ 51%-70%
 ■ 71%-90%
 ■ 91%-100%

This gives you a good idea as to how the WAN interfaces are utilized at the different sites where the highest utilization points to a site being busy.

Application Throughput over Time over an Interface

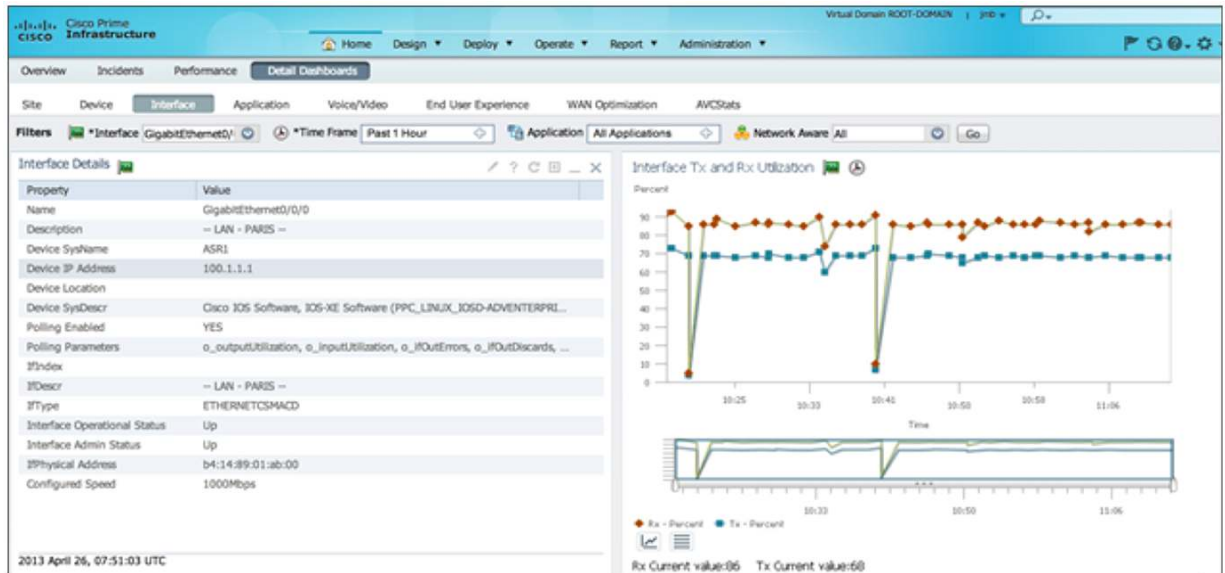
A first step would be to check the top interface utilization. Browse to **Home → Performance → Network Interface**.



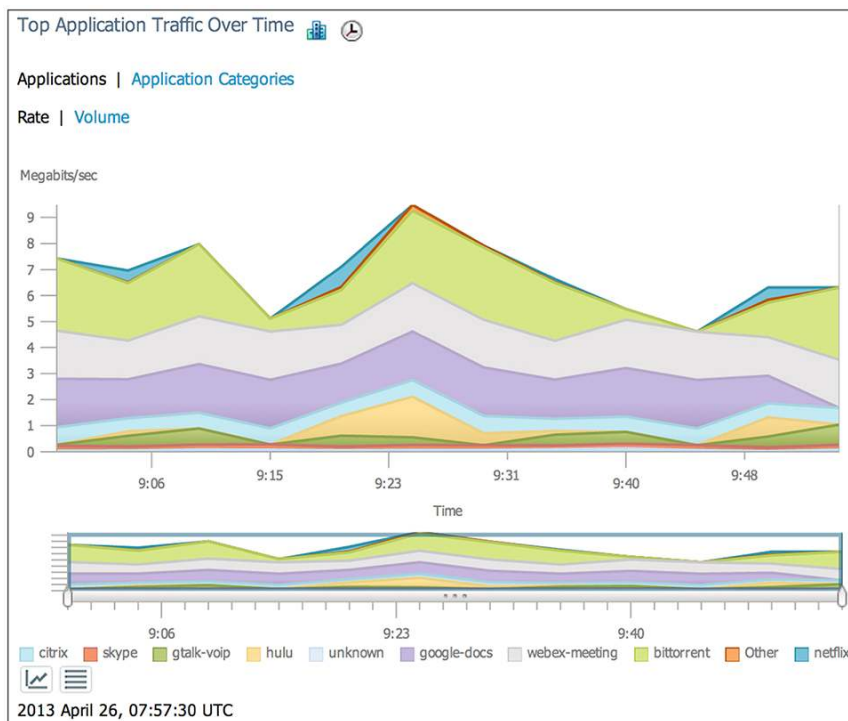
The interesting dashlet here is Top N Interface Utilization. From there you can click a specific interface and you will be redirected to the **Detail Dashboard → Interface**.

You can also directly go to **Home → Detail Dashboard → Interface**.

You will have to select an interface. Select the site name, device, and then the interface you want to monitor and you will be redirected to the Interface detail dashboard:

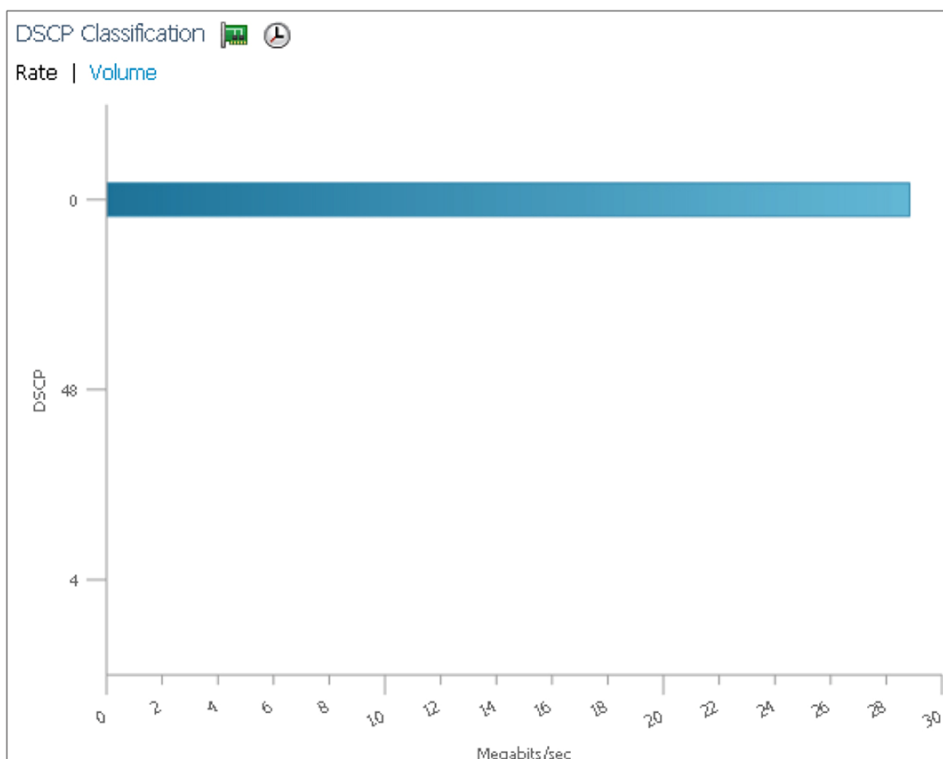
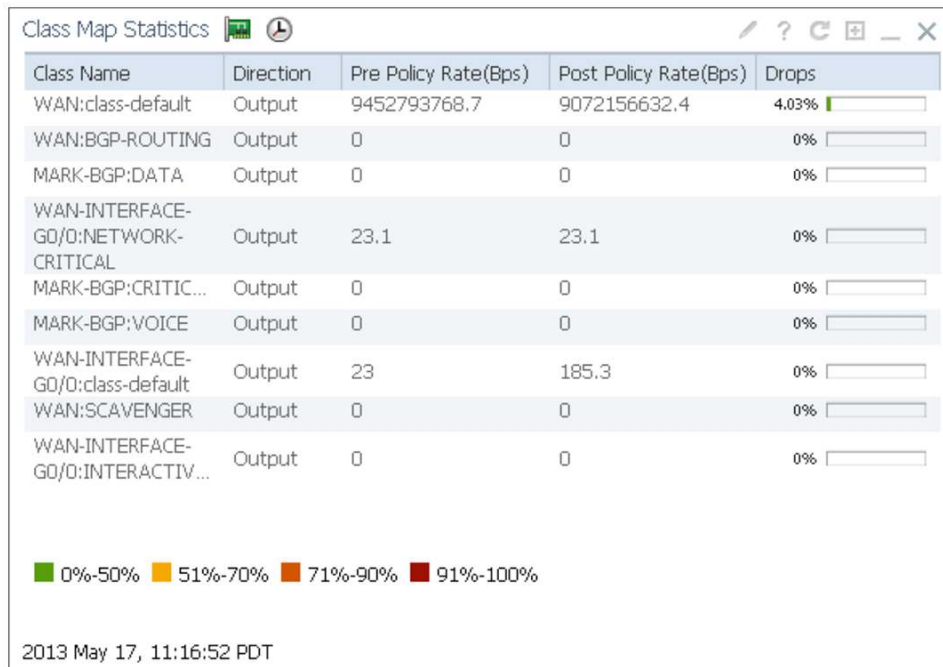


Among all the dashlets presented in this page, application usage is of great interest: Top Application Traffic over Time.



You can switch between applications and application categories.

Some of the other dashlets that are of interest in the Interface dashboard are the Class Map Statistics and the DSCP Classification dashlets. These provide the QOS information regarding the marked values on that particular interface for the applications.



Identify an Enterprise's Own Applications and Create Custom Apps to Monitor

In Cisco Prime Infrastructure, the custom apps are created as follows: Browse to **Operate** → **Applications and Services**.

The screenshot shows the Cisco Prime Infrastructure web interface. The top navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', and 'Administration'. The 'Operate' tab is selected. Below the navigation bar, the 'Applications and Services' section is active. On the left, there is a 'Services' sidebar with a search bar and a list of service categories. The main area displays a table of 'All Applications'. The table has columns for Application Name, Business Criticality, Category, Sub Category, P2P, Tunnel, and Encrypted. The 'Create' button is visible in the top navigation bar.

Application Name	Business ...	Category	Sub Category	P2P	Tunnel	Encrypted
001myapp	No	other	other	Unassigned	Unassigned	Unassigned
3com-amp3	No	other	other	Unassigned	Unassigned	Unassigned
3com-tsmux	No	obsolete	other	Unassigned	Unassigned	Unassigned
3gpp2-a10-pkts	No	other	other	Unassigned	Unassigned	Unassigned
3gpp2-a10-ubs	No	other	other	Unassigned	Unassigned	Unassigned
3gpp2-a11	No	other	other	Unassigned	Unassigned	Unassigned
3pc	No	layer3-over-ip	other	Unassigned	Unassigned	Unassigned
802-1ad	No	other	other	Unassigned	Unassigned	Unassigned
802-1ah	No	other	other	Unassigned	Unassigned	Unassigned
914c/g	No	net-admin	remote-access-terminal	No	No	No
9991netflow	No	other	other	Unassigned	Unassigned	Unassigned
9pfs	No	net-admin	storage	No	No	No
aarp	No	other	other	Unassigned	Unassigned	Unassigned
acap	No	net-admin	network-management	No	No	No
acas	No	other	other	Unassigned	Unassigned	Unassigned
accessbuilder	No	other	other	Unassigned	Unassigned	Unassigned
accessnetwork	No	other	other	Unassigned	Unassigned	Unassigned
acp	No	other	other	Unassigned	Unassigned	Unassigned
acr-nema	No	Industrial-protocols	other	No	No	No
active-directory	No	net-admin	network-management	No	No	No

Click the **Create** button and you will see a screen shot similar to the following:

The screenshot shows the 'Create Application' dialog box. It has a title bar with 'Create Application' and a close button. Below the title bar, there is a note: '* Indicates required field'. The dialog is divided into two main sections: 'General' and 'Attributes'. The 'General' section contains the following fields: 'Application Name' (required), 'Description', 'Engine ID' (set to 'custom'), 'Selector' (required), 'Associated Service(s)' (with a dropdown arrow), and 'Business Criticality' (checkbox). The 'Attributes' section contains the following dropdown menus: 'Category' (set to 'other'), 'Sub Category' (set to 'other'), 'P2P' (set to 'Unassigned'), 'Tunnel' (set to 'Unassigned'), and 'Encrypted' (set to 'Unassigned').

Traffic Classification Rules

At least one rule is required

* Rule	Condition
Protocol	Set Condition

Applicable for ASR, ISR and NAM devices.
Applicable for ASR and ISR devices.
Other rules are applicable for Prime Infrastructure only.

Create Cancel

Here you can specify a name for your custom application and key in a selector ID. You can also mark it as business critical. By doing so, Cisco Prime Infrastructure performs an automated baselining regarding the application performance across all sites and can be viewed under **Operate → Performance → Service Health**. The attributes help you to pick a particular category/subcategory that you want this custom application to be a part of. There are different ways to classify this custom application traffic, which you will find in the Traffic Classification Rules section. You can classify this traffic based on protocol and port number, DSCP value, RTP payload type, server IP, or a specific URL. Then save this and deploy this template on the device for which you would like to start classifying this custom application.

Monitor and Troubleshoot Voice and Video Performance

Why Is My Video Quality Poor?

In order to trace the cause for poor video quality, let us first look at the video streams. Go to **Operate → Detail Dashboards** and click the **Voice/Video** tab. Here you can view the RTP conversations with the RTP Conversations Details dashlet.


RTP Conversations Details

Troubleshoot


	Source A...	Type	Destinatio...	Type	Sou...	De...	Jitter (...)	Packet Loss (%)	MOS	
<input type="radio"/>	10.2.12.13		10.15.12.13				27.7	7	3.72	
<input type="radio"/>	10.2.12.15		10.15.12.15				28.5	7	3.61	
<input type="radio"/>	10.2.12.20		10.15.12.20				29.7	7	3.65	
<input type="radio"/>	10.2.12.14		10.15.12.14				27.3	7	3.64	
<input type="radio"/>	10.2.12.13		10.15.12.13				27.2	7	3.64	
<input type="radio"/>	10.2.12.13		10.15.12.13				28.4	7	3.68	

If your call quality is affected by jitter, packet loss, or latency, you will be able to find this information in the above dashlet.

Apart from this, these could be situations in which there are other users in the same site who are experiencing the same poor quality. The following dashlets point out the packet loss and jitter from an enterprise perspective:

Worst N RTP Streams By Packet Loss 

RTP Streams	Maximum Packet Loss (%)	Average Packet Loss (%)	Minimum Packet Loss (%)
San Jose Campus to Los Angeles Branch	5.1	3.1	0.9
San Francisco Branch to Denver Branch	6.6	3	0
Los Angeles Branch to San Jose Campus	6.2	2.9	0
New York Branch to Los Angeles Branch	4.2	2	0
Denver Branch to San Francisco Branch	4.3	2	0

Worst N RTP Streams by MOS 

RTP Streams	Max. MOS	Avg. MOS	Min. MOS
Los Angeles Branch to San Jose Campus	3.78	3.76	3.72
San Jose Campus to New York Branch	4.29	4.28	4.27
San Jose Campus to RTP Branch	4.29	4.28	4.26
New York Branch to San Jose Campus	4.3	4.29	4.29
San Jose Campus to Los Angeles Branch	4.3	4.29	4.27


Worst N Site to Site Connections by KPI  Edited

Connections	Max. Jitter (ms)	Avg. Jitter (ms)	Min. Jitter (ms)
New York Branch to Los Angeles Branch	5.56	4.93	4.69
RTP Branch to San Jose Campus	2.76	2.74	2.71
Management Apps to Unassigned	2.21	1.93	1.68
San Jose Campus to Management Apps	1.66	1.66	1.65












Where in My Network Is Dropping Packets?

Once you have identified the session with the poor quality, you can further trace the path from the source to destination or vice-versa and further look at the quality metrics on the devices along the path.

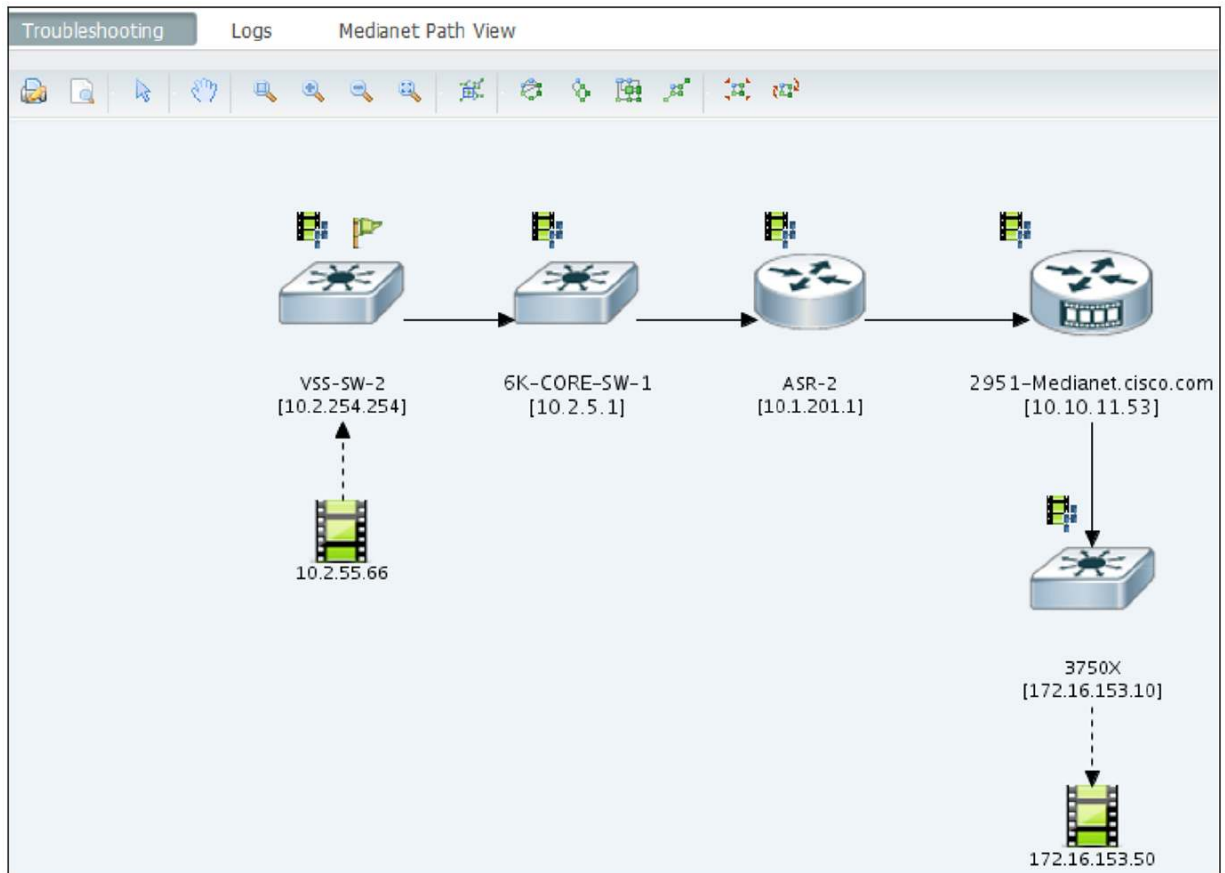
Browse to **Operate → Detail Dashboards** and click the **Voice/Video** tab. You can look at the RTP Conversation Details dashlet and click the conversation that you would like to troubleshoot as shown below:

RTP Conversations Details 

Troubleshoot ▾

Trace Service Path		T...	Source User	Destination ...	Jitter (...)	Packet Loss (%)	MC
Analyze on Multiple Data Sources					29	7	
<input type="radio"/>	10.2.12.15		10.15.12.15		28.3	6	
<input type="radio"/>	10.2.12.15		10.15.12.15		28.8	6	
<input type="radio"/>	10.2.12.15		10.15.12.15		27.6	6	
<input type="radio"/>	10.2.12.15		10.15.12.15		25.3	6	
<input type="radio"/>	10.2.12.20		10.15.12.20		29.5	6	

Click **Trace Service Path**. Below is the path that the RTP stream takes from the source to the destination.



Additionally, when you click the routers in the path, you will see various statistics like the CPU, memory, packet loss, latency, and other information for that particular router.



Monitor and Troubleshoot TCP Performance

Which Applications May Be Having Performance Issues?

A first step is to check the overall network health. Browse to **Home** → **Performance** → **Service Health**.

The screenshot shows the Cisco Prime Infrastructure interface. The top navigation bar includes Home, Design, Deploy, Operate, Report, and Administration. The main navigation tabs are Overview, Incidents, Performance (selected), and Detail Dashboards. Under Performance, there are sub-tabs for Network Device, Network Interface, Service Assurance, and Service Health (selected). A filter section shows a time frame of 'Past 1 Hour'. The 'Site-Application Health Summary' table displays health status for two sites, Lyon and Paris, across two applications: rtp and webex-meeting. Lyon shows a green bar for rtp and a red bar for webex-meeting. Paris shows green bars for both.

Site	rtp	webex-meeting
Lyon	Green	Red
Paris	Green	Green

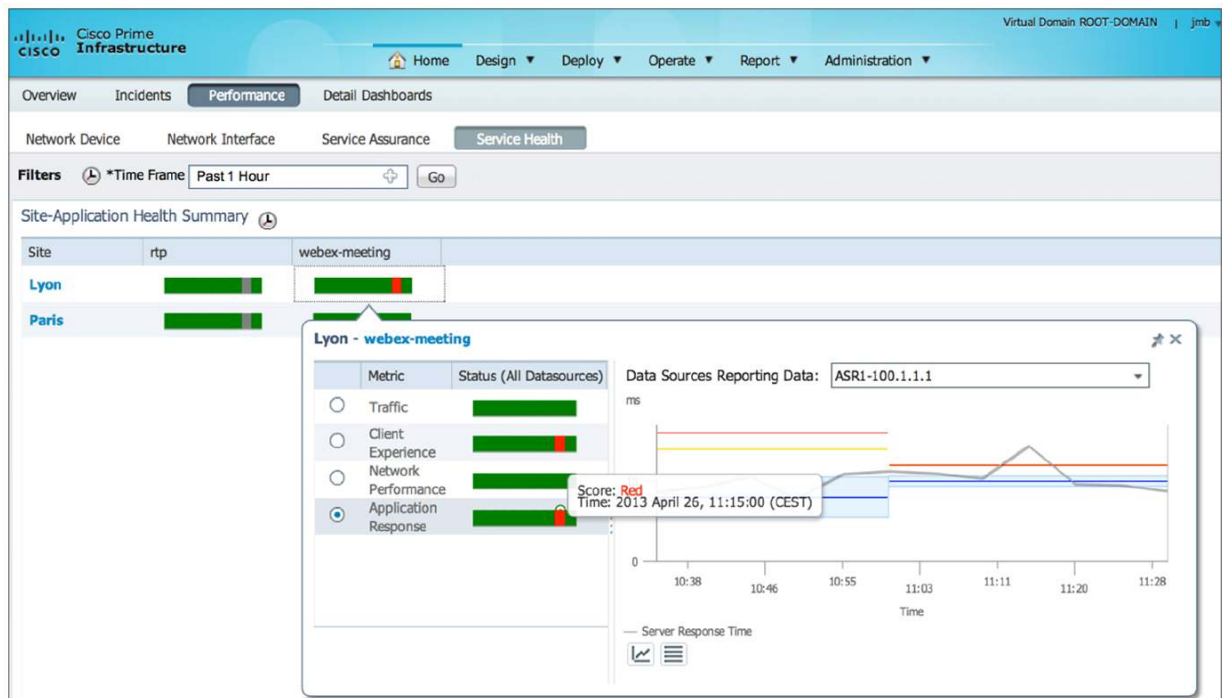
You will only have applications listed as business critical in this dashboard.

This is defined by default with the Protocol Pack, but you can also tune that by going to **Operate** → **Application and Services**.

The screenshot shows the Cisco Prime Infrastructure 'Applications and Services' dashboard. The top navigation bar includes Home, Design, Deploy, Operate (selected), Report, and Administration. The main navigation tabs are Applications and Services (selected) and Application Server Management. The 'All Applications' table lists various applications with columns for Application Name, Business Criticality, Category, Sub Category, P2P, Tunnel, and Encrypted. A red box highlights the 'Business Criticality' column, which shows 'No' for all listed applications.

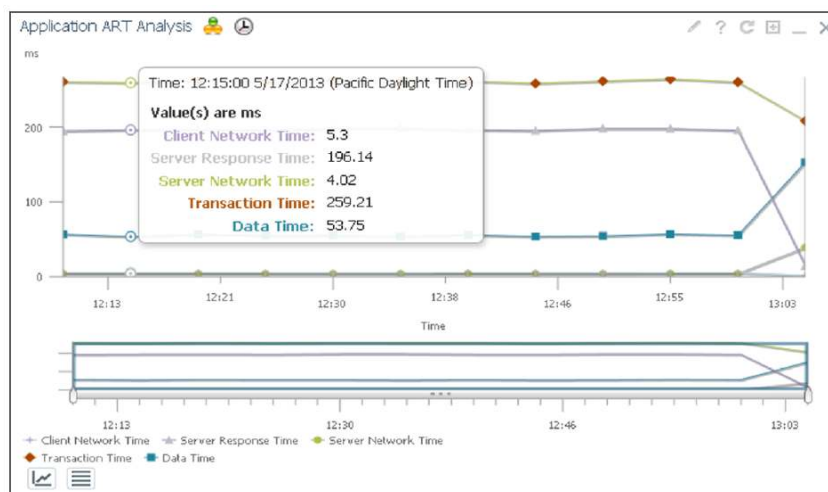
Application Name	Business Criticality	Category	Sub Category	P2P	Tunnel	Encrypted
001myapp	No	other	other	Unassigned	Unassigned	Unassigned
3com-amp3	No	other	other	Unassigned	Unassigned	Unassigned
3com-tsmux	No	obsolete	other	Unassigned	Unassigned	Unassigned
3gpp2-a10-plts	No	other	other	Unassigned	Unassigned	Unassigned
3gpp2-a10-ubs	No	other	other	Unassigned	Unassigned	Unassigned

In the **Home → Performance > Service Health** window you can quickly check whether something is going wrong in terms of performance. Orange or red means something has greatly changed from the average observed. It works on the concept of automatic baselining. Cisco Prime Infrastructure calculates the standard deviation. If your current value exceeds this value by 2 times, you will see a yellow indication. If it exceeds the value by 3 times, you will see a red indication. When you click a specific application for a specific site, you get the details in terms of traffic and performance:



What Might Cause the Problem - Is Application Slowness Caused by the Network or Application?

Browse to **Operate → Detail Dashboards** and click the **Application** tab. Here you will be able to find out the ART metrics for a specific application for a specific site or for your entire enterprise. You can look at the Application ART Analysis dashlet, which gives you a good breakdown of the metrics to classify whether it is a client side issue or a server side issue as shown below.






You can also look at the Application Server Performance dashlet to check whether it is the application response time that is slowing down the application.

Application Server Performance  

Application Server	Site	Application	Avg. Server Response Time (ms)	Max. Server Response Time (ms)	Analysis
192.168.138.202	Management Apps	cisco-callmanager	23586	23820	
192.168.138.134	Management Apps	filenet	15000	15000	
192.168.138.123	Management Apps	https	10905	12422	
192.168.152.11	Amsterdam Branch	ssh	4127	10000	
192.168.138.201	Management Apps	cisco-callmanager	6700	6916	

There is also the Worst N Sites by ART Metrics dashlet that gives you an overall idea regarding the ART metrics on an enterprise level.

Worst N Sites by ART Metrics        

Selected Metric : Transaction Time

Site	Application	Maximum Transaction Time (ms)	Average Transaction Time (ms)
India Branch	sap	154445	42908
RTP Branch	unknown	98920	27008
India Branch	citriximaclient	143128	21495
Management Apps	cisco-callmanager	27053	18002
Management Apps	filenet	15001	15001

Troubleshooting

AVC Configuration Through DWC

If you have enabled AVC through the Device Work Center, then you will see the input and output reports having the details as shown in the following illustration. This confirms that AVC is turned on.

Device Details **Configuration** Configuration Archive Image

Feature Configuration

Features

Application Visibility

Interfaces



Routing

Security

WAN Optimization

AVC Interfaces

☒ Enable Default AVC ☒ Disable Default AVC

Selected 0 | Total 9  

	Interface Name	Template Name	Input Reports	Output Reports	Troubleshooting	VRF	IP Address	C
1	<input type="checkbox"/> GigabitEthernet0/1/0				<input checked="" type="checkbox"/> ACTIVE		10.0.199.1	U
2	<input type="checkbox"/> GigabitEthernet0/1/1		ART (IPv4), HTTP (IPv4),...	ART (IPv4), HTTP (IPv4),...			10.0.198.1	U
3	<input type="checkbox"/> GigabitEthernet0/1/2						10.0.111.1	D
4	<input type="checkbox"/> GigabitEthernet0/1/3						10.0.105.1	D
5	<input type="checkbox"/> GigabitEthernet0/1/4						192.168.136.44	U
6	<input type="checkbox"/> GigabitEthernet0/1/5						10.0.106.1	D
7	<input type="checkbox"/> GigabitEthernet0/1/6							D
8	<input type="checkbox"/> GigabitEthernet0/1/7							D
9	<input type="checkbox"/> GigabitEthernet0							D

Mgmt-intf

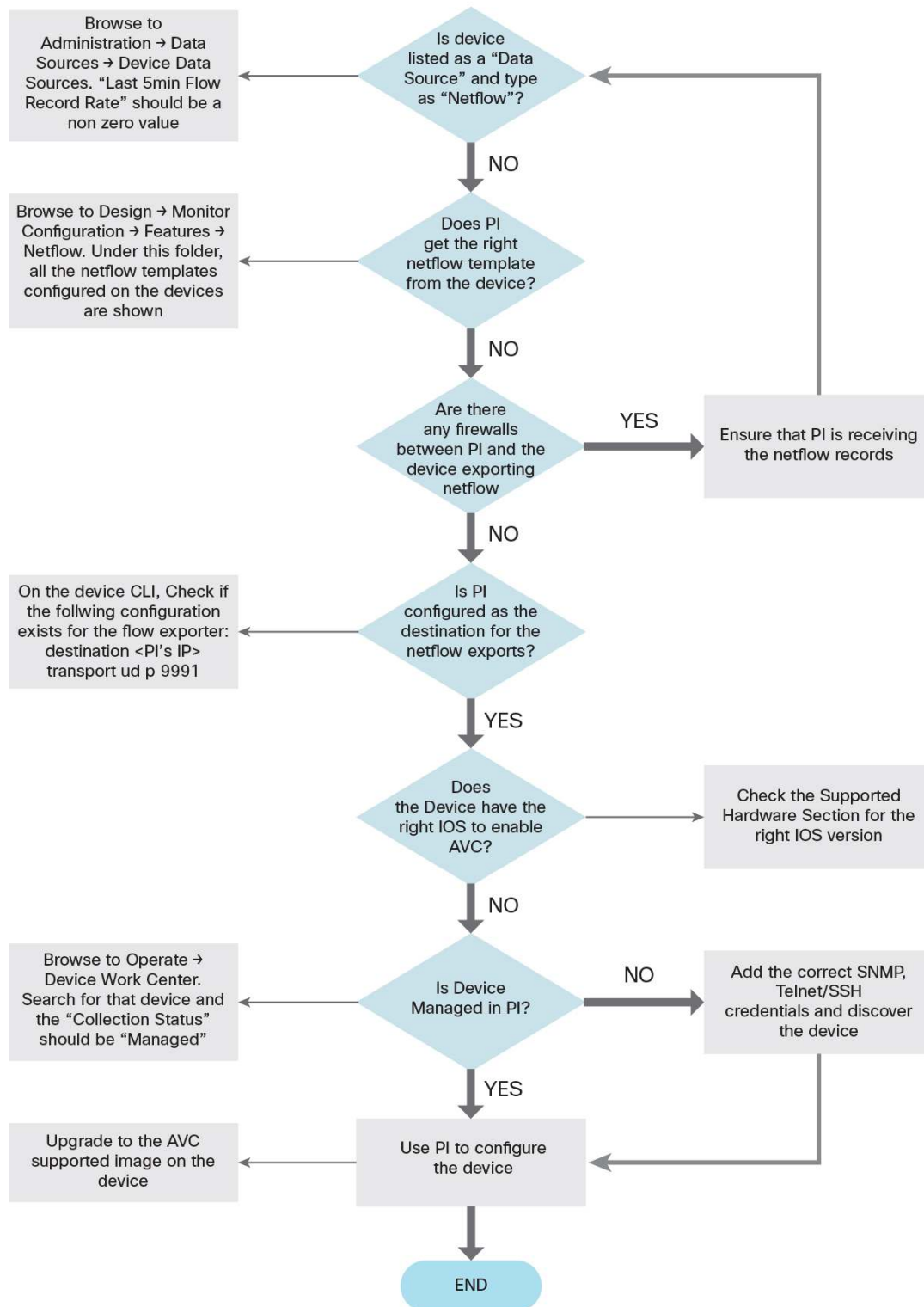
Is Cisco Prime Infrastructure Receiving NetFlow Data?

In order for Cisco Prime Infrastructure to receive NetFlow data, it must first receive the NetFlow templates. A quick way to verify this is to browse to **Administration → System Settings → Data Sources**. For each of the data source, you can use the quick view to see all the templates configured on this particular device. You can even click the template, which would cross launch to the Monitoring Template page, and look at the NetFlow structure.

Troubleshooting Flowchart

The following is a flowchart that can help to debug why the Assurance-related dashlets are not populated with data.

AVC Troubleshooting



Appendix

Preparing the Network

The routers/switches should have Simple Network Management Protocol (SNMP) and Telnet/SSH enabled for them to be successfully managed. And the wireless controllers and the access points should have SNMP, Telnet/SSH, and HTTP access.

Configuring SNMP

Cisco Prime Infrastructure supports all versions of SNMP: v1, v2c, and v3 (noAuthNoPriv, authNoPriv, authPriv).

- a. Enabling SNMP on Routers/Switches

For most devices, the following syntax should work for SNMP v1/v2c:

#configure terminal

#snmp-server community pu61c RO (using "public" is not recommended)

#snmp-server community pr1vat3 RW (using "private" is not recommended)

- b. Enabling SNMP on Wireless Controllers

From the WLC web GUI, navigate to **Management > Communities** (under SNMP). Click **New** to create a new SNMP v1/v2c community. An SNMP v3 community can be configured by going to the SNMP v3 user from the left panel menu.

Enabling Telnet/SSH

- a. Enabling Telnet/SSH on Routers/Switches

Below is the configuration that should work on most of the routers/switches:

```
line vty 0 4
  access-class vty_access in
  privilege level 15
  login local
  transport input telnet ssh
```

- b. Enabling Telnet/SSH on Wireless Controllers

From the WLC web GUI, navigate to **Management > Telnet-SSH** to open the Telnet-SSH Configuration page. Allow either the Telnet or SSH sessions.

Device Discovery

Before you use Cisco Prime Infrastructure to configure AVC functionality, you will need to discover/add the devices in Cisco Prime Infrastructure. You will also need to create sites and associate the devices to the respective sites in order to get detailed information about application visibility from a site, device perspective. You will also need to configure Interface roles to apply the AVC configuration on. And finally you need to identify the WAN interfaces in order to collect/monitor the application traffic over the WAN.

The sections below briefly describe the process to achieve the above.

Browse to **Operate → Discovery (Under Device Work Center)**. You can either create a new template under the discovery settings and add the protocol settings and the credential information and discover the network devices or you can import a comma-separated value (CSV) file with the device information (IP address, SNMP credentials, and so on).

Once you have all your devices discovered and managed by Cisco Prime Infrastructure, browse to **Design → Site Map Design** and create new sites, campus, buildings, and so on. Or you can use the **Design → Automatic Hierarchy Creation** to create sites based on regex of the name. Then browse to **Design → Endpoint Site Association** and associate the endpoints to the respective sites.

Browse to **Design → Feature Design → Shared Policy Objects**. Click the Interface Role under the shared folder. Here you can create interfaces on which you would like to enable AVC.

Browse to **Design → Port Grouping** and filter on the Interfaces to select the WAN interfaces and add them to the WAN Interfaces group.

Configuring Medianet

While troubleshooting the voice/video performance, Mediatrace can be enabled in order to pinpoint the router in the path that is affecting the performance.

Cisco Prime Infrastructure has predefined templates for enabling Mediatrace. Navigate to **Design → Feature Design → CLI Templates → System Templates - CLI**. You will see two templates for mediatrace, as shown in the following figure:



The HTTP-HTTPS Server and WSMA Configuration-IOS template enables Cisco Prime Infrastructure to interact with the device using HTTP/HTTPS.

A screenshot of a 'Template Detail' form. At the top, there is a dropdown arrow and the text 'Template Detail'. Below this are two tabs: 'CLI Content' and 'Form View'. The 'Form View' tab is selected and highlighted. The form contains several configuration fields, each with a label and a value or a dropdown menu. The fields are: 'Server Action' with a dropdown menu showing 'No Change'; '*Port [1024-65535, default:80(HTTP),443(HTTPS)]' with a text input field; 'Authentication Action' with a dropdown menu showing 'No Change'; 'Authentication Method' with a dropdown menu showing 'aaa'; 'Access List Action' with a dropdown menu showing 'No Change'; 'ACL Number/Name' with a text input field; and 'WSMA Action' with a dropdown menu showing 'No Change'.

From the above screenshot, choose HTTP/HTTPS for the Server Action. If you need additional authentication then choose the corresponding Authentication Action. Enable Access List Action if required. Finally enable WSMA Action.

The Mediatrace-Responder-Configuration is required to configure the responder/probe to collect the data. The steps for deploying the template remain the same as with any other CLI template. Note that the first two templates for enabling Medianet do not have any variables.

TIP: Make sure that a user is defined in the device with privilege level 15 for the Web Services Management Agent (WSMA) to work.

Detailed CLI Configuration for AVC

Please refer to the following links to configure the CLI for the AVC functionality on the ASR 1000 Series and ISR G2 routers.

Cisco IOS XE Software: http://www.cisco.com/en/US/docs/ios/solutions_docs/avc/ios_xe3_8/avc_config.html.

Cisco IOS Software: http://www.cisco.com/en/US/docs/ios-xml/ios/wan_waas/configuration/15-mt/cfg-avc-mace.html.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)