AVC Solution Guide with Cisco Prime Infrastructure
Contents

Scope ................................................................................................................. 4

AVC Solution Overview ...................................................................................... 4
  Getting Visibility .......................................................................................... 4
  Today’s Challenges .................................................................................... 4
  What Is Application Visibility and Control? ............................................... 5
  How Does Application Visibility and Control Work? ............................... 6

AVC Technology Overview ............................................................................... 7
  Presentation ............................................................................................... 7
  NBAR2 ...................................................................................................... 7
  Flexible NetFlow ...................................................................................... 7
  Performance Collection ............................................................................. 8
  Reporting Tools ......................................................................................... 8
  Control ....................................................................................................... 9

Use Cases Overview ......................................................................................... 9
  Discover Application Usage in the Network .............................................. 10
    Top Applications .................................................................................. 11
    Top Talkers (Client or Server) .............................................................. 13
    Busiest Site/Location ........................................................................... 15
    Application Throughput over Time over an Interface ......................... 15
    Identify an Enterprise’s Own Applications and Create Custom Apps to Monitor ....................................................... 15
    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 ...................................... 20
    Which Applications May Be Having Performance Issues? ..................... 20
    What Might Cause the Problem - Is Application Slowness Caused by the Network or Application? ................................. 22

Deployment Scenarios ..................................................................................... 22
  Enterprise Reference Topology ................................................................. 23
  AVC at the WAN Edge ............................................................................ 24
  AVC at the Internet Edge .......................................................................... 25
  AVC for Managed Service Providers (MSPs) ............................................ 26
  AVC for Traditional Wireless Deployments (Cisco Unified Wireless Network) ................................................................. 27
  AVC for Converged Access .................................................................... 29
  AVC for Perimeter Security/Firewall ....................................................... 31
  AVC Deployment Caveats ......................................................................... 32

AVC Enablement with Cisco Prime Infrastructure ............................................ 32
  Cisco Prime Infrastructure Download ...................................................... 32
  Installation ............................................................................................... 32
  AVC Configuration ................................................................................... 33
    AVC-Supported Platforms .................................................................... 33
    Prerequisites ......................................................................................... 33
    Readiness Assessment .......................................................................... 33
    NBAR2 Protocol Pack Update ............................................................... 34
    Interface Roles Configuration ............................................................... 34
    AVC Configuration and Activation ........................................................ 35
      Enabling AVC on Routers ................................................................. 35
      Enabling AVC on Wireless Controllers ........................................... 40
    Custom Application Creation ............................................................... 43
    QoS Configuration ................................................................................ 43
    Advanced System Settings .................................................................... 48
      Data Retention .................................................................................. 49
      Data De-duplication .......................................................................... 49
    Monitoring/Visualizing AVC ................................................................. 49
      Monitoring Dashboards ..................................................................... 49
    Use Cases Workflow ............................................................................... 49
      Discover Application Usage in the Network ...................................... 49
Identify an Enterprise's Own Applications and Create Custom Apps to Monitor ........................................ 57
Monitor and Troubleshoot Voice and Video Performance .............................................................................. 58
Monitor and Troubleshoot TCP Performance .............................................................................................. 61
QoS Monitoring ............................................................................................................................................... 63
Troubleshooting ............................................................................................................................................... 64
Is Cisco Prime Infrastructure Receiving NetFlow Data? .............................................................................. 64
Troubleshooting Flowchart .......................................................................................................................... 64

Appendix ....................................................................................................................................................... 66
Preparing the Network .................................................................................................................................. 66
Configuring SNMP ......................................................................................................................................... 66
Enabling Telnet/SSH ....................................................................................................................................... 66
Device Discovery ............................................................................................................................................. 66
Configuring Medianet .................................................................................................................................... 67
Detailed CLI Configuration for AVC ........................................................................................................... 68
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 3.0

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 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 that 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:

- **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).

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:

<table>
<thead>
<tr>
<th>Performance Collection</th>
<th>Voice and Video Performance (Media Monitoring)</th>
<th>Critical Applications Performance (Application Response Time)</th>
</tr>
</thead>
<tbody>
<tr>
<td>30% of Bandwidth</td>
<td>Is Voice and Video</td>
<td>40% of Bandwidth</td>
</tr>
<tr>
<td>Is Critical Applications</td>
<td></td>
<td>Is Critical Applications</td>
</tr>
</tbody>
</table>

Traffic Statistics

<table>
<thead>
<tr>
<th>Skype</th>
<th>BitTorrent</th>
<th>MSN Messenger</th>
<th>Google Talk</th>
<th>Gmail</th>
<th>Microsoft Live Meeting</th>
<th>iTunes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VQIP</td>
<td>SAP</td>
<td>FLV Player</td>
<td>YouTube</td>
<td>McAfee</td>
<td>Windows Server Update Services</td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td>My SQL</td>
<td>QuickTime Player</td>
<td>Rhapsody</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citrix</td>
<td>Netflix</td>
<td>Cisco WebEx</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Traffic Statistics</th>
<th>URL Visibility</th>
<th>Application Response Time</th>
<th>Media Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Application Usage Per Client IP/Subnet/Site</td>
<td>- Most Visited Web-Site</td>
<td>- Per-Application End-to-End Latency</td>
<td>- Per-Stream Jitter and Packet Loss</td>
</tr>
<tr>
<td>- Top Clients Per Application</td>
<td>- Per-URL Application Response Time</td>
<td>- Application Response Time &amp; Transaction Time</td>
<td>- RTP Conversations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Application Processing Time</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Top Conversation Per Application</td>
<td></td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Yesterday Applications</th>
<th>Today Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Cisco WebEx</td>
</tr>
<tr>
<td>FTP</td>
<td>iCloud</td>
</tr>
<tr>
<td>POP3</td>
<td>Google Docs</td>
</tr>
<tr>
<td>IMAP</td>
<td>Microsoft Office 365</td>
</tr>
<tr>
<td>HTTPS</td>
<td>McAfee</td>
</tr>
<tr>
<td>SMTP</td>
<td>YouTube</td>
</tr>
<tr>
<td></td>
<td>Microsoft Exchange</td>
</tr>
<tr>
<td></td>
<td>Skype</td>
</tr>
<tr>
<td></td>
<td>BitTorrent</td>
</tr>
<tr>
<td></td>
<td>Skype</td>
</tr>
<tr>
<td></td>
<td>Pandora</td>
</tr>
<tr>
<td></td>
<td>Google Talk</td>
</tr>
<tr>
<td></td>
<td>Microsoft Office SharePoint Server 2007</td>
</tr>
<tr>
<td></td>
<td>Salesforce.com</td>
</tr>
<tr>
<td></td>
<td>Windows Server Update Services</td>
</tr>
</tbody>
</table>

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:

```
1 Byte 3 Bytes
├── Engine ID ├── 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 perspective, 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, referer, 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

                                     Input                  Output
                                      -------              -------
  Protocol                 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
                          994000                   1005000
  google-docs             663653                   531562
                          845095007                73970024
                          402000                   11000
                          1824000                  171000
  netflix                 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 Dashboard ➔ Overview 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

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

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 Dashboard ➔ Overview ➔ Service Assurance
- Global view with filter options: Dashboard ➔ Performance

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 Dashboard ➔ Overview ➔ 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 Dashboard ➔ Overview ➔ Service Assurance:

Click unknown and you are redirected to Dashboard ➔ Performance ➔ 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:

<table>
<thead>
<tr>
<th>Application</th>
<th>Protocol</th>
<th>Port</th>
<th>bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>unknown</td>
<td>udp</td>
<td>3000</td>
<td>593,851,228</td>
</tr>
<tr>
<td>youtube</td>
<td>tcp</td>
<td>8080</td>
<td>306,770,502</td>
</tr>
<tr>
<td>unknown</td>
<td>udp</td>
<td>2055</td>
<td>157,948,250</td>
</tr>
<tr>
<td>unknown</td>
<td>tcp</td>
<td>9102</td>
<td>144,215,386</td>
</tr>
<tr>
<td>dns</td>
<td>udp</td>
<td>53</td>
<td>118,617,995</td>
</tr>
</tbody>
</table>

Thursday, July 23 2015 at 13:24 PM
NBAR2 allows defining custom-based applications in addition to applications defined in the active Protocol Pack:

![NBAR2 Custom Application Definition](image)

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:

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

You can check with the following command:

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

<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>id</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>001myapp</td>
<td>60002</td>
<td>Custom</td>
</tr>
</tbody>
</table>
```

**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

```bash
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:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Classification</th>
<th>Performance Collection</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>800</td>
<td>NBAR2, Metadata</td>
<td>FNF, (Performance Agent)PA, PerfMon -&gt; Unified Monitor (Future)</td>
<td>QoS, PfR</td>
</tr>
<tr>
<td>1900-AX</td>
<td>NBAR2, Metadata</td>
<td>FNF, PA, PerfMon -&gt; Unified Monitor (Future)</td>
<td>QoS, PfR</td>
</tr>
<tr>
<td>2900-AX</td>
<td>NBAR2, Metadata</td>
<td>FNF, PA, PerfMon -&gt; Unified Monitor (Future)</td>
<td>QoS, PfR</td>
</tr>
<tr>
<td>3900-AX</td>
<td>NBAR2, Metadata</td>
<td>FNF, PA, PerfMon -&gt; Unified Monitor (Future)</td>
<td>QoS, PfR</td>
</tr>
<tr>
<td>ASR 1000</td>
<td>NBAR2, Metadata</td>
<td>Unified Monitor</td>
<td>QoS, PfR</td>
</tr>
</tbody>
</table>

**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.

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:

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

<table>
<thead>
<tr>
<th>Platform</th>
<th>Classification</th>
<th>Performance Collection</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>WISM2</td>
<td>NBAR2 (PP 2.1)</td>
<td>Flexible NetFlow (fixed record)</td>
<td>QoS</td>
</tr>
<tr>
<td></td>
<td>Protocol Pack support future</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3850 Wireless</td>
<td>NBAR2 - Future: Cisco IOS-XE</td>
<td>NetFlow (fixed record) for wireless traffic - Future: Cisco IOS-XE 3.3 (Darya, Q4CY13)</td>
<td>App-aware QoS policies for wireless - Future: Cisco IOS XE 3.4 (Amur, 1H CY14)</td>
</tr>
<tr>
<td></td>
<td>3.3 (Darya, Q4CY13)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

AVC/NBAR2 (Broad AVC and Web AVC)
Can detect 1000+ applications and 150,000+ micro applications

- URL Filtering – works with Cisco SIO that updates database every 5 mts covering a third of global Internet traffic

Notes:
Key purpose of AVC in Firewalls is to administer business policies where there is control of which user can access what application, and what functions are possible

One 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.
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:

<table>
<thead>
<tr>
<th>Today's Limitation</th>
<th>Impact</th>
<th>Workaround</th>
</tr>
</thead>
</table>
| NBAR2 - Cannot run NBAR2 on the WAN when WAAS or WAAS-X is used | • 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 | • 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 | • 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 | • No ART reporting with overlapping IP | N/A |
| PIR and WAASx can’t work together | • Not a well-tested scenario | N/A |
| No support for asymmetric routing | • No NBAR2 classification - Limited QoS  
• No ART  
• AVC requires router seeing traffic in both directions | N/A |
| Can’t run NBAR2, PIR on with crypto map/GETVPN | • NBAR2, PIR 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 PIR workaround |
| PIR’s limited scalability | • Only use PIR for < 200 sites | Target discovery when available |
| No PIR support with AppNav | • PIR is not operational with AppNav | N/A |
| No PIR IPv6 support | • Can’t use PIR with IPv6 traffic/applications | N/A |
| Can’t attach FNF to a virtual template | • 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 3.0 software is available from Cisco Marketplace at [http://www.cisco.com/go/nmsevals](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](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:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Minimum Software Version Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR 1000</td>
<td>15.3(1)S1 and later</td>
</tr>
<tr>
<td>ISR G2</td>
<td>15.2(4)M2 and later</td>
</tr>
<tr>
<td>CSR 1000</td>
<td>15.3(2)S</td>
</tr>
<tr>
<td>ISR 4451-X</td>
<td>15.3(2)S</td>
</tr>
<tr>
<td>WLC</td>
<td>7.4</td>
</tr>
</tbody>
</table>

Prerequisites

The following table lists prerequisites for various device types:

<table>
<thead>
<tr>
<th>#</th>
<th>Device Type Applicable for</th>
<th>Prerequisite</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wired and wireless</td>
<td>Make sure that the devices on which you would like to enable AVC are fully managed (In the Device Work Center [DWC]).</td>
<td>See the “Preparing the Network” and “Device Discovery” sections in the Appendix.</td>
</tr>
<tr>
<td>2</td>
<td>Wired and wireless</td>
<td>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.</td>
<td>See the “Device Discovery” section in the Appendix.</td>
</tr>
<tr>
<td>3</td>
<td>Wired devices</td>
<td>Interface role should be created before using the template.</td>
<td>See the “Interface Roles Configuration” section.</td>
</tr>
</tbody>
</table>

Readiness Assessment

The Readiness Assessment allows you to analyze the routers in your network and determine whether these devices are capable of running AVC. The assessment provides a pie-chart-based analysis detailing some of the device information and its capability to run AVC. This assessment also recommends appropriate actions for the users in order to successfully enable AVC.

Browse to Services ➔ Application Visibility and Control ➔ Readiness Assessment to view this feature. As a prerequisite to this step, make sure that the routers are added into Cisco Prime Infrastructure and are managed completely. If the devices are not managed fully, then the recommended action is to check the device inventory.
The table view provides all the relevant information for the devices, like the Device IP, IOS version, and so on, and also suggests whether these devices are AVC capable or not. The users can also quickly find out whether AVC has been enabled on these routers.

Some of the checks performed include the appropriate hardware, minimum Cisco IOS/IOS-XE Software image, active AVC license, latest protocol pack, and so on.

**NBAR2 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.

Newer protocol packs are often released and now can be easily updated on the routers using Cisco Prime Infrastructure. This is a two-step process; that is, the user downloads the appropriate protocol pack and distributes it on the routers using Cisco Prime Infrastructure and at the same time the user needs to obtain a UBF file released for Cisco Prime Infrastructure, which is a software update file to be added on to the Cisco Prime Infrastructure instance so that Cisco Prime Infrastructure can now recognize the newer application’s signatures. The UBF file can be downloaded from cisco.com and applied to Cisco Prime Infrastructure by browsing through Administration → Software Update.

Browse to Services → Application Visibility & Control → NBAR2 Protocol Pack Management. Using the Import option, you can download the protocol pack of your choice either locally from a file or from a URL. You can then schedule a job to download this protocol pack and store it on Cisco Prime Infrastructure’s repository.

Once you download the protocol pack, there are two options to distribute it. You can choose either to distribute it immediately using the Distribute option, during which the current protocol pack becomes the active one on the selected device, or to use the Distribute with ISSU option to have this as a standby protocol pack that becomes the active one after an image update.

For more details, please refer to the End User Guide.


**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:

```cpp
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:

```cpp
interface GigabitEthernet0/0/1
description -- WAN - ASR2 --
ip address 100.1.2.1 255.255.255.0
```
Within Cisco Prime Infrastructure, browse to **Configuration → Shared Policy Objects** and then select **Interface Role**.

Create two new interface roles:

Create two new interface roles:

![Configuration / Templates / Shared Policy Objects](image)

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.

**AVC Configuration and Activation**

**Enabling AVC on Routers**

There are multiple ways to enable AVC on the routers. If this is your first time with AVC, then you can use the one-click option to enable it on a single or multiple interface of a router. If you are more or less familiar with it, then you can use the template option to enable AVC on multiple devices based on the interface role. The third option is to enable AVC on multiple interfaces and multiple devices for which you could use the location- and device-based filters. This method will also allow you to configure QoS if needed.

**One-Click Using the Device Menu**

This option is useful when you would like to enable AVC on a single device that has been managed by Cisco Prime Infrastructure. Browse to **Configuration → Network Devices**.
Locate the device on which you would like to enable the AVC feature. Click the device name, which will take you to the Device Details page. Click Configuration → App Visibility & Control → App Visibility. Select the interface or interfaces on which you would like to enable AVC and click the App Visibility button. This will provide you with four options. The first 2 options only provide the Application Visibility, that is, the application classification using NBAR2. The last two options also provide the application performance metrics, that is, ART (Application Response Time) Metrics, as well as the Voice and Video metrics.

Select the interface on which you would like to enable AVC.

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. You can verify whether AVC has already been enabled on the interface by viewing the AVC Status column. If this interface had already been configured with AVC, then the AVC Policy column shows whether the AVC enablement was through a template or the one-click option. If the one-click option was previously used, then the AVC policy shows as Default. If templates were used, it shows the name of the template.

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 Configuration → Templates. Here under the Features and Technologies folder you will find the App Visibility & Control folder, which contains the AVC template:
This template consists of three main sections.

a. Template Basics

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

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.

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.
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.

   ![Application Response Time](image)

   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.

   ![Voice/Video Metrics](image)

   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.

![Device Selection](image)
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  \rightarrow  Jobs  \rightarrow  User-Defined.

Using the Interfaces Configuration Menu

This method is very useful when the user would like to enable AVC on multiple devices at multiple locations on many interfaces using a rule-based selection process for the interfaces.

Browse to Services  \rightarrow  Application Visibility & Control  \rightarrow  Interfaces Configuration. Here you can use the filter to select the interfaces on which you would like to enable AVC. This is a very comprehensive filter that provides various options to choose the interfaces like the location, App Visibility Status, QoS Status, and so on.

Use the Enable App Visibility button at the top to enable AVC. This will again provide you with the four options. The first 2 options only provides the Application Visibility, that is, the application classification using NBAR2. The last two options also provide the application performance metrics, that is, ART metrics as well as the voice and video metrics.
**Note:**

If you have enabled AVC using the one-click option from the Device Page or template or by using the Interfaces Configuration Page, you can now disable them all in this Interfaces Configuration Page.

**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 Configuration ➔ Templates ➔ 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.
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.

![Monitor Configuration Screenshot](image)

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 **Configuration ➔ Templates ➔ 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.
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 Services ➔ Application Visibility & Control ➔ 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.

QoS Configuration
Cisco Prime Infrastructure provides an out-of-the-box experience for configuring QoS on routers. Based on Cisco Validated Designs, users can now configure 5-, 8-, or 12-class QoS policies based on port numbers, DSCP markings, or NBAR2 application categories. The users can also configure their own custom QoS policies and monitor them. Both making and shaping of the traffic are possible with this interface.

Browse to Services ➔ Application Visibility & Control ➔ Interfaces Configuration. Here, along with QoS, you can also enable AVC. The first step is to choose an interface or a list of interfaces for which you would like to enable QoS. For example, you can use the filter to mark and shape the traffic on all of your WAN interfaces across multiple WAN routers.
Using the Interfaces Configuration Page

We will first look at how we could classify and mark the traffic. Browse to Services → Application Visibility & Control → Interfaces Configuration Ingress QoS Configuration. Here you first choose an interface or a list of interfaces for which you would like to mark the traffic.

Click Enable QoS. This will open a pop-up window where you can further create your QoS profile. Since we first would like to classify the traffic on the ingress, select Enable QoS on Ingress.

Use the menu to select the appropriate profile. By default, the QoS profiles for 5-, 8-, and 12-class models are defined. Here the user can change the NBAR/Layer3-Layer4 classification to the corresponding QoS class as well as associate the current application name to a different NBAR subcategory. For example, you could have the http application added to the other NBAR subcategory and further add this other NBAR Layer 3-Layer 4 classification to the Scavenger QoS class.
Users can also create custom QoS profiles based on these out-of-the-box 5-, 8-, and 12-class policies. For this, in the same pop-up window, choose Create Profile. In the Profile pop-up, choose the appropriate class. You can now make the same changes to the classification pattern as above.

Traffic classification can also be performed based on the traditional Layer3-Layer 4 ports, DSCP markings, or IP address. If you would like to classify the traffic purely based on the traditional methods, then create the custom profile and delete all the existing entries. Click Add and choose L3/L4 in the pop-up list. This pop-up provides you with the option to configure QoS based on DSCP values, IP address or ports.
After you create the profile using any of the previous methods, you now have two job options to copy your running configuration to startup configuration and achieve the configuration after you deploy the profile. Just before deploying the configuration, you also have the option to view the CLI. Finally, click Deploy. This creates a job, and the user can view the status of this deployment or job under Administration → Jobs.

Next we will look at the QoS configuration on the egress interface for both marking and shaping the traffic. In the same Interfaces Configuration page, select the appropriate interface and click Enable QoS. Select Enable QoS on Egress.

Here the classification can be done based on DSCP markings (choose Classify based on DSCP) or NBAR application categories. For NBAR application categories, choose Classify based on Profile. Creating this classification profile is similar to what we have done above for the ingress QoS classification profile.

Once completed, you can now choose to take action on the traffic. Using the same Enable QoS window for which you just performed the classification, launch the pop-up for action profiles under QoS Action. Here, you can view the default 5-, 8-, and 12-class action profiles along with the option to create your own custom profile.
If you would like to change the default options of the allocated bandwidth percentage, shaping rate, and so on, then you must use Create Profile, which will enable you to create your own action profile based on the defaults. For this, click Create Profile and choose the appropriate 5-, 8-, or 12-class profile. Here you can add the shaping rate for that particular interface. You can further change the BW percentage allocated to the corresponding QoS classes. You can further remark this traffic, for example, if it is intended to go to a service provider.

Once done, click OK and you have the similar job options as well as the ability to preview the CLI before this configuration.
QoS Profiles

You can also choose to create the QoS profiles first and then choose to deploy these profiles at a later point in time using the Interfaces Configuration page. Browse to Services → Application Visibility & Control → AVC Profiles.

Here you will see the QoS classification profiles and QoS action profiles. If you created custom profiles as explained in the previous section, these custom profiles should appear here. You can also choose to add new custom profiles right from this page as well. Click the Add button and choose the appropriate profile. These new profiles are created the same way as explained above.

If you have created custom profiles in this page, then you can browse to the Interfaces Configuration page, select the interface or interfaces on which you would like to configure these profiles, and click the Enable QoS button. In the pop-up, choose the profiles that you just created and deploy them.

Update QoS Configuration

By using Cisco Prime Infrastructure, you can not only deploy a new QoS configuration but also update the same. For example, on a set of interfaces, you would like to change the shaping rate, then browse to the AVC Profiles page, select the corresponding QoS action profile and make the necessary changes. You will then see a warning saying that the current changes have not been deployed yet. If you would like to proceed further, browse to the Interfaces Configuration page and click Update QoS. You do not have to select the interfaces at this point. Once you click the Update QoS button, Cisco Prime Infrastructure will automatically provide the list of device IPs that had the configuration that you just made a change to. You can then select the devices and continue, and this will update the current QoS policies.

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 → Settings → 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. Dashboard → Overview → Service Assurance
b. Services → Application Visibility and Control → Service Health
c. Dashboard → Performance (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 Dashboard → Overview 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 Youtube 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 Dashboard → Overview → 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 Dashboard → Performance 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 San Francisco site) to get details on a specific site.

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

**Top Talkers (Client and Server)**

**Global View**

Browse to **Dashboard ➔ Overview** 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 **Dashboard ➔ Performance ➔ 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 details for the IP address 10.0.211.102:
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 Dashboard → Performance 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).

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 Dashboard → Performance → 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 San Francisco site. In the filter ribbon, select San Francisco:

![Top N Applications and Top N Clients](image)

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

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

![Busiest Site/Location](image)

**Busiest Site/Location**

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

<table>
<thead>
<tr>
<th>Site</th>
<th>Device</th>
<th>Interface</th>
<th>Maximum Utilization</th>
<th>Average Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>London Branch</td>
<td>10.11.1.1</td>
<td>GigabitEthernet0/0</td>
<td>8%</td>
<td>77.46%</td>
</tr>
<tr>
<td>Los Angeles Branch</td>
<td>10.0.102.2</td>
<td>GigabitEthernet0/0</td>
<td>5%</td>
<td>2.23%</td>
</tr>
<tr>
<td>Unassigned</td>
<td>10.0.103.1</td>
<td>GigabitEthernet0/1</td>
<td>2.5%</td>
<td>2.23%</td>
</tr>
<tr>
<td>Unassigned</td>
<td>192.168.152.1</td>
<td>GigabitEthernet0/1</td>
<td>3%</td>
<td>2.17%</td>
</tr>
<tr>
<td>New York Branch</td>
<td>10.0.104.2</td>
<td>GigabitEthernet0/0</td>
<td>3%</td>
<td>2.09%</td>
</tr>
</tbody>
</table>

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**

The first step would be to check the top interface utilization. Browse to Dashboard → Overview → 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 Dashboard → Performance → 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.

### Class Map Statistics

<table>
<thead>
<tr>
<th>Class Name</th>
<th>Direction</th>
<th>Pre Policy Rate(Bps)</th>
<th>Post Policy Rate(Bps)</th>
<th>Drops</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN:class-default</td>
<td>Output</td>
<td>9452793768.7</td>
<td>9072156632.4</td>
<td>4.03%</td>
</tr>
<tr>
<td>WAN:BGP:ROUTING</td>
<td>Output</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>MARK-BGP:DATA</td>
<td>Output</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>WAN-INTERFACE-GO:D:NETWORK-CRITICAL</td>
<td>Output</td>
<td>23.1</td>
<td>23.1</td>
<td>0%</td>
</tr>
<tr>
<td>MARK-BGP:CRITICAL</td>
<td>Output</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>MARK-BGP:VOICE</td>
<td>Output</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>WAN-INTERFACE-GO:D:class-default</td>
<td>Output</td>
<td>23</td>
<td>185.3</td>
<td>0%</td>
</tr>
<tr>
<td>WAN:SCAVENGER</td>
<td>Output</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>WAN-INTERFACE-GO:D:INTERACTIVE</td>
<td>Output</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>

#### Color Legend
- 0%-50%
- 51%-70%
- 71%-90%
- 91%-100%

2013 May 17, 11:16:52 PDT
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 Services  Application Visibility & Control  Applications and Services.

Click the Create button and you will see a screen shot similar to the following:
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 Service ➔ Application Visibility and Control ➔ 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 Dashboard ➔ Performance and click the Voice/Video tab. Here you can view the RTP conversations with the RTP Conversations Details dashlet.
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:

<table>
<thead>
<tr>
<th>Worst N RTP Streams By Packet Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP Streams</td>
</tr>
<tr>
<td>San Jose Campus to Los Angeles Branch</td>
</tr>
<tr>
<td>San Francisco Branch to Denver Branch</td>
</tr>
<tr>
<td>Los Angeles Branch to San Jose Campus</td>
</tr>
<tr>
<td>New York Branch to Los Angeles Branch</td>
</tr>
<tr>
<td>Denver Branch to San Francisco Branch</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Worst N RTP Streams by MOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP Streams</td>
</tr>
<tr>
<td>Los Angeles Branch to San Jose Campus</td>
</tr>
<tr>
<td>San Jose Campus to New York Branch</td>
</tr>
<tr>
<td>San Jose Campus to RTP Branch</td>
</tr>
<tr>
<td>New York Branch to San Jose Campus</td>
</tr>
<tr>
<td>San Jose Campus to Los Angeles Branch</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Worst N Site to Site Connections by KPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>New York Branch to Los Angeles Branch</td>
</tr>
<tr>
<td>RTP Branch to San Jose Campus</td>
</tr>
<tr>
<td>Management Apps to Unassigned</td>
</tr>
<tr>
<td>San Jose Campus to Management Apps</td>
</tr>
</tbody>
</table>
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 Dashboard ➔ Performance 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:

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 Services → Application Visibility and Control → Service Health.

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 Services → Application Visibility & Control → Application and Services.

In the Services → Application Visibility and Control → 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 Dashboard → Performance 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.

<table>
<thead>
<tr>
<th>Application Server</th>
<th>Site</th>
<th>Application</th>
<th>Avg. Server Response Time (ms)</th>
<th>Max. Server Response Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.138.202</td>
<td>Management Apps</td>
<td>cisco-callmanager</td>
<td>23356</td>
<td>23820</td>
</tr>
<tr>
<td>192.168.138.134</td>
<td>Management Apps</td>
<td>filenet</td>
<td>15000</td>
<td>15000</td>
</tr>
<tr>
<td>192.168.138.123</td>
<td>Management Apps</td>
<td>https</td>
<td>10905</td>
<td>12422</td>
</tr>
<tr>
<td>192.168.152.11</td>
<td>Amsterdam Branch</td>
<td>ssh</td>
<td>4127</td>
<td>10000</td>
</tr>
<tr>
<td>192.168.138.201</td>
<td>Management Apps</td>
<td>cisco-callmanager</td>
<td>6700</td>
<td>6916</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Site</th>
<th>Application</th>
<th>Maximum Transaction Time (ms)</th>
<th>Average Transaction Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>India Branch</td>
<td>sap</td>
<td>154445</td>
<td>42908</td>
</tr>
<tr>
<td>RTP Branch</td>
<td>unknown</td>
<td>98920</td>
<td>27008</td>
</tr>
<tr>
<td>India Branch</td>
<td>citrixmadcent</td>
<td>143128</td>
<td>21495</td>
</tr>
<tr>
<td>Management Apps</td>
<td>cisco-callmanager</td>
<td>27053</td>
<td>10002</td>
</tr>
<tr>
<td>Management Apps</td>
<td>filenet</td>
<td>15001</td>
<td>15001</td>
</tr>
</tbody>
</table>

**QoS Monitoring**

Cisco Prime Infrastructure provides dashboards to quickly view the QoS statistics across the interfaces. In order to view the QoS statistics, browse to Dashboard → Performance → Interface. You can view the Class Map Statistics dashlet to understand the QoS classes and their corresponding drops. You can use the Top QoS Class Map Statistics Trend dashlet to view the effect of the QoS classes on the applications.
In the Interface Details dashlet, you can also view the current QoS profile that is applied and click it to make changes to the QoS profile. Once a change is made, you can then use the Top QoS Class Map Statistics Trend dashlet to quickly understand the changes, since this dashlet is updated every 5 minutes.

![Top QoS Class Map Statistics Trend](image)

**Troubleshooting**

**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

Browse to Administration → Data Sources → Device Data Sources. “Last 5min Flow Record Rate” should be a non-zero value.

Is device listed as a “Data Source” and type as “Netflow”?

NO

Browse to Design → Monitor Configuration → Features → Netflow. Under this folder, all the netflow templates configured on the devices are shown.

Does PI get the right netflow template from the device?

NO

Are there any firewalls between PI and the device exporting netflow?

NO

On the device CLI, check if the following configuration exists for the flow exporter:

- destination <PI’s IP>
- transport udp 9991

Is PI configured as the destination for the netflow exports?

YES

Ensure that PI is receiving the netflow records.

NO

Does the Device have the right IOS to enable AVC?

YES

Check the Supported Hardware Section for the right IOS version.

NO

Add the correct SNMP, Telnet/SSH credentials and discover the device.

NO

Is Device Managed in PI?

YES

Upgrade to the AVC supported image on the device.

Use PI to configure the device.

END

NO

Browse to Operate → Device Work Center. Search for that device and the “Collection Status” should be “Managed”.
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 Inventory ➔ Discovery 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 Maps → Site Maps and create new sites, campus, buildings, and so on. Or you can use the Maps → Automatic Hierarchy Creation to create sites based on regex of the name. Then browse to Services → Application Visibility & Control → Endpoint Association and associate the endpoints to the respective sites.

Browse to Configuration → Templates → 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 Inventory → Grouping → Port 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 Configuration → Templates → Features & Technologies → 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.

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.
