Contents

- 1 AVC Solution Overview
  - 1.1 Getting Visibility
  - 1.2 Today Challenges
  - 1.3 What is Application Visibility and Control?
  - 1.4 How does Cisco AVC Solution Work?
- 2 Cisco Application Visibility and Control (AVC) Technical Overview
  - 2.1 Presentation
  - 2.2 Application Recognition
    - 2.2.1 Next Generation NBAR (NBAR2)
    - 2.2.2 NBAR2 Protocol Pack
    - 2.2.3 NBAR2 Custom Protocol
    - 2.2.4 NBAR2 Application Attributes
  - 2.3 Performance Collection and Exporting
    - 2.3.1 Based on Flexible NetFlow
    - 2.3.2 Monitoring Profiles and Performance Collection
    - 2.3.3 Traffic Statistics
    - 2.3.4 URL Visibility
    - 2.3.5 Application Response Time
    - 2.3.6 Media Monitoring
  - 2.4 Network Management
  - 2.5 Control
    - 2.5.1 QoS with NBAR2
    - 2.5.2 Performance Routing
  - 2.6 Conclusion
  - 2.7 For More Information

AVC Solution Overview

Getting Visibility

Network operators want 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 that can be used to classify flows range from IP addresses, port numbers, DSCP markings (assuming that the operator has classified applications based on DSCP markings), and application names using NBAR, among other techniques.

Today Challenges

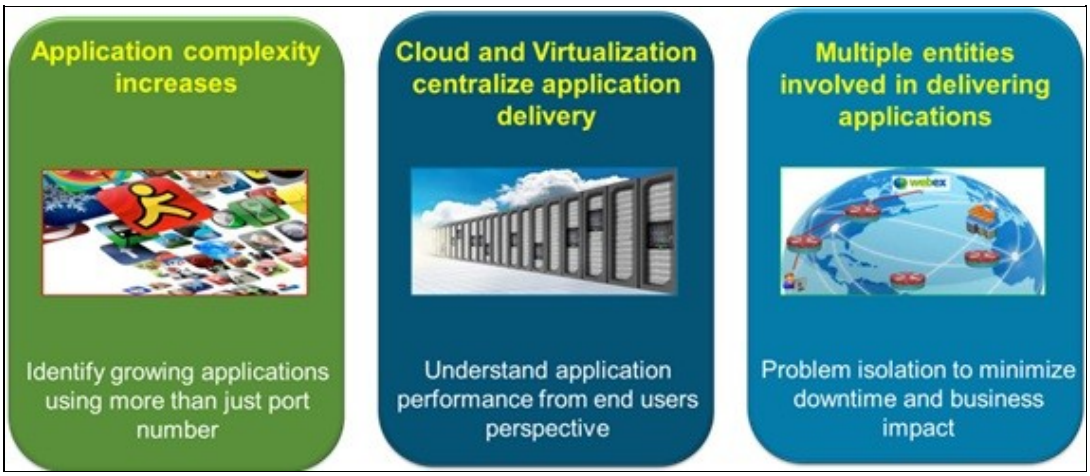

Figure 1. Challenges in monitoring and controlling application delivery in today?s network

There are several trends in the today enterprises that drive requirements to build application awareness within the network. 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. In addition, consolidation of the data center in order to reduce overhead and operating expenses requires the network to carry much greater volume of both business and recreational traffic. Network admins need to gain visibility into different types of traffic their performance in greater detail to be able to quickly isolate and troubleshoot application performance issues. They need the ability to granularly define policy to control and tune the performance of these different applications.

Cisco Application Visibility and Control (AVC) can be used to gather further insight into the health of these flows by collecting statistics such as packet loss, jitter, round-trip-time and bandwidth used for the individual flows.

What is Application Visibility and Control?

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

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

Figure 2. What is Cisco Application Visibility and Control (AVC)

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 use which results in better end user experiences. Cisco AVC is enabled in Cisco IOS and IOS XE software.

How does Cisco AVC Solution Work?

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

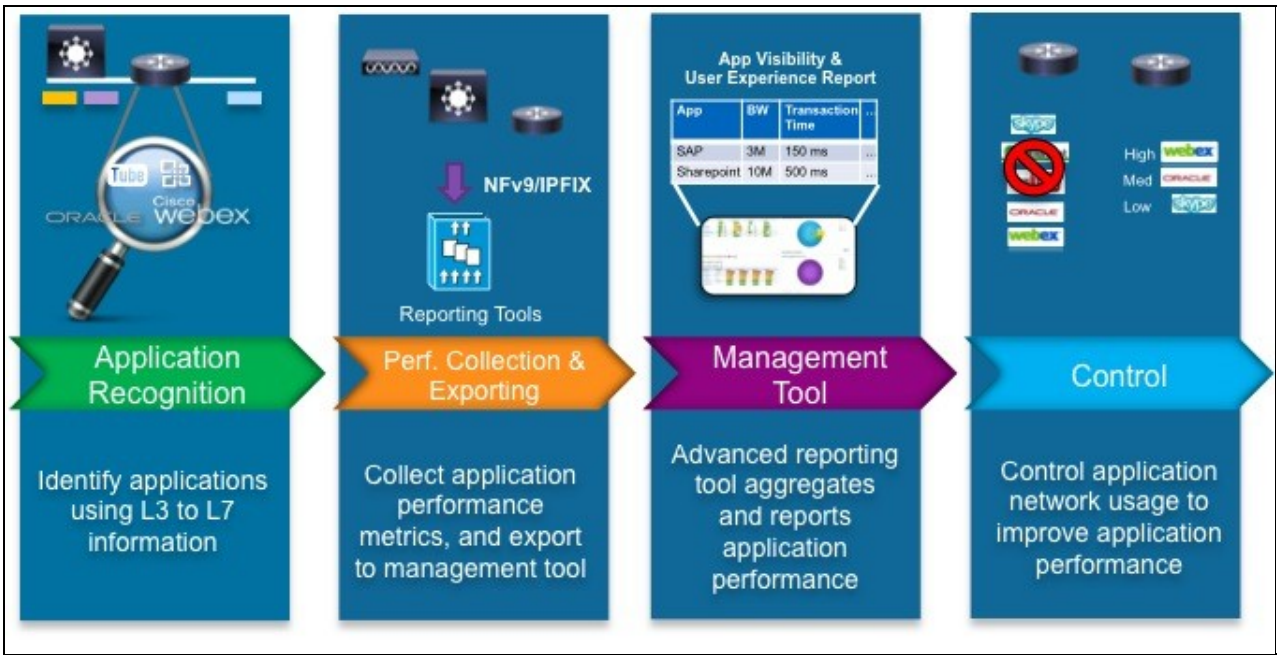

Figure 3. Cisco AVC Functional Components

Cisco AVC solution leverages multiple technologies to recognize, analyze, and control over 1000 applications including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based

applications. Cisco AVC has the following functional components:

1. **Application Recognition:** With Cisco AVC, Cisco ASR 1000, ISR-G2 and Cisco Wireless Controllers can identify over 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.
2. **Performance Collection and Exporting:** Cisco AVC utilizes 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 format such Netflow Version 9 and IPFIX.
3. **Management Tool:** With open flow export format such as Netflow Version 9 and IPFIX, data exported by AVC can be consumed by Cisco Prime Infrastructure and other third-party network management tools. This gives customers flexibility to utilize Cisco management tool or to leverage management tool of their choices.
4. **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)

Cisco Application Visibility and Control (AVC) Technical Overview

Presentation

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

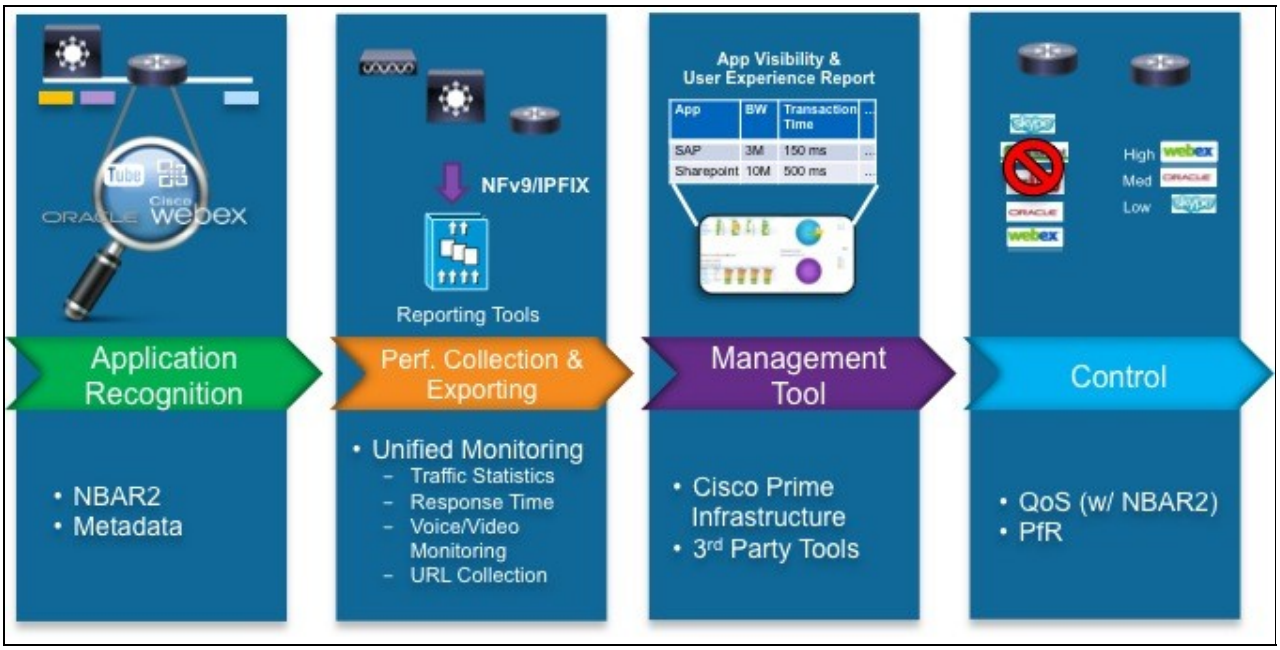

Figure 4. Cisco AVC Technology Blocks

Application Recognition

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

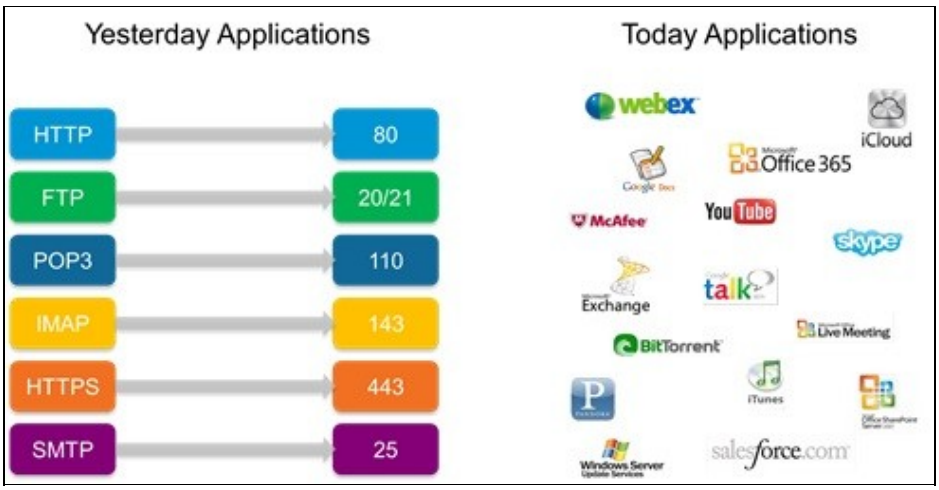

Figure 5. Evolution of types of applications seen in enterprise

Next Generation NBAR (NBAR2)

NBAR2 is Cisco?s cross platform Deep Packet Inspection (DPI) and Field Extraction (FE) technologies. NBAR2 is supported on Cisco ASR 1000 and ISR G2.

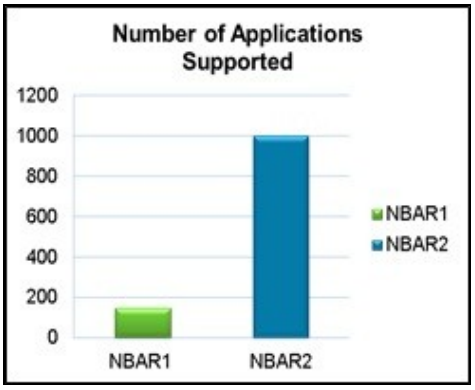

Figure 6. NBAR1 vs NBAR2 Number of Supported Applications

NBAR2 brings a number of major enhancements over the legacy NBAR (NBAR1).

- Detect over one thousand applications in its first release. Its heuristic analysis engine allows NBAR2 to identify applications regardless of ports applications may be running on.
- Support of NBAR2 Protocol Pack (PP) allows updating application signature while the routers are running. New Protocol Pack is released every month.
- Application categorization uses NBAR2 attributes to group similar applications to simplify application management for both classification and reporting
- Extract information from application such as HTTP URL, HTTP User Agent, SIP URL, for export or classification.

For more information on NBAR2, please visit http://www.cisco.com/go/nbar

Within AVC, there are currently three key uses of NBAR2.

1. **Application accounting:** This can be provided through CLI ip nbar protocol-discovery, enabling on interface(s). Through CLI show ip nbar protocol-discovery, users can get a snapshot of applications seen through the interface, along with traffic rate and volume, in both byte and packet unit. The same information is also available through NBAR MIBs.
2. **Classification:** By using NBAR2 in the class-map, routers can identify traffic by NBAR2 application signature. This allows per-application policy control such as QoS, e.g. limit traffic rate for Netflix, Pandora, and iTunes applications, or guarantee bandwidth for business applications such as WebEx, Office 365, or Sharepoint.
3. **Reporting:** By leveraging Flexible Netflow infrastructure to export application information provided by NBAR2 through opened export format such as Netflow Version 9, or IP Flow Information Export (IPFIX) protocol.

NBAR2 Protocol Pack

NBAR2 provides an ability to update and add application signatures while the routers are in service. This is done by loading a NBAR2 Protocol Pack file. NBAR2 Protocol Pack consists of all the available signatures packaged together into a single file. NBAR2 Protocol Pack is available for downloading on Cisco website in the same place where the IOS software for the particular routers is posted. NBAR2 Protocol Pack is created for every supported IOS and IOS XE releases, and is dependent on the IOS and IOS XE releases.

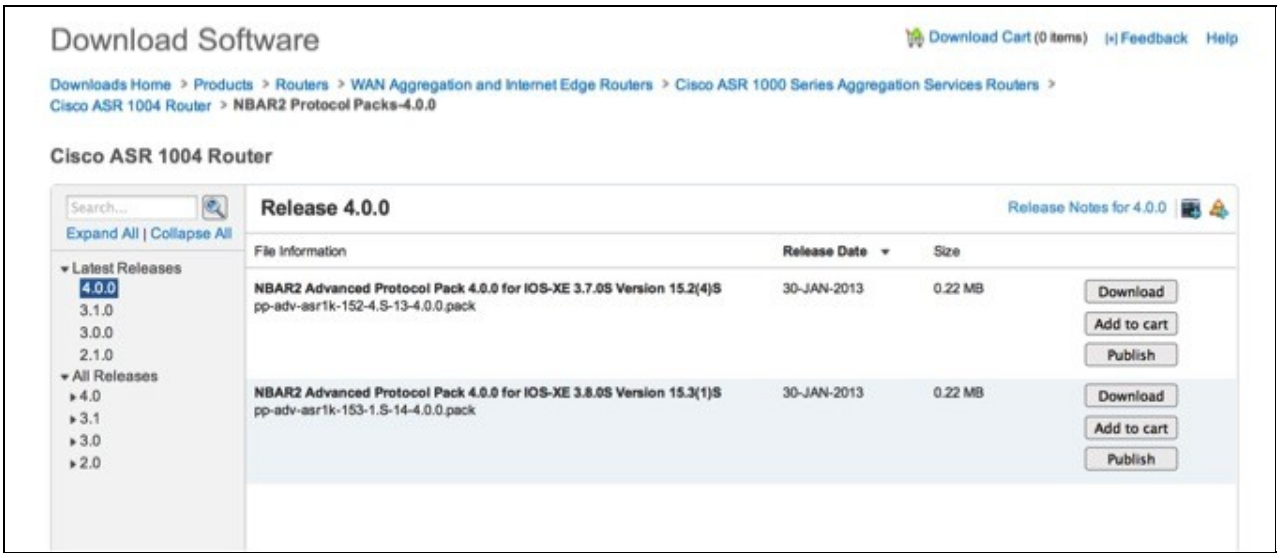

Figure 7. Example of NBAR2 Protocol Pack Location

Following describes steps to load protocol pack.

Step 1: Locate the NBAR2 Protocol Pack for your router platform and your running IOS image on Cisco website. Download the NBAR2 Protocol Pack to the local file system of the router

```
router#dir bootflash:pp-adv-asr1k-15.2(04)S-13-1.1(0).pack

Directory of bootflash:/pp-adv-asr1k-15.2(04)S-13-1.1(0).pack
48785 -rw- 188131 Sep 6 2012 21:24:52 -07:00 pp-adv-asr1k-15.2(04)S-13-1.1(0).pack
```

Step 2: Issue the following configuration command for NBAR2 to use the NBAR2 Protocol Pack on the local file system instead of the one bundled with IOS or IOS XE image

```
router#(config)#ip nbar protocol-pack flash:pp-adv-asr1k-15.2(04)S-13-1.1(0).pack
```

Step 3: Verify that the new NBAR2 Protocol Pack is loaded and is in effect

```
router#show ip nbar protocol-pack active

ACTIVE protocol pack:
Name: Advanced Protocol Pack
Version: 3.0
Publisher: Cisco Systems Inc.
File: flash:pp-adv-asr1k-15.2(04)S-13-1.1(0).pack
```

NBAR2 Custom Protocol

There may be applications that are not yet identified by NBAR2. Such applications include custom or home-grown enterprise applications which may run on specific TCP or UDP ports, or internal web-based applications. NBAR2 provides ability for users to define these applications, call custom protocol, using CLI ip nbar custom. Following describes supported methods for defining custom applications

- TCP or UDP port and range of ports
- ASCII or binary pattern up to the first 255 bytes of TCP or UDP payload
- HTTP URL ? any combination of hostname as in the HTTP message host field, and URI, e.g. http://www.cisco.com/go/avc, www.cisco.com is the host portion, while the go/avc is the URI portion.

NBAR2 Application Attributes

NBAR2 provides six pre-defined attributes for every application to group applications of similar types. This simplifies the classification rules and reporting by matching applications using attributes in class-map, or reporting based on attributes.

Table 1. List of NBAR2 attributes

NBAR2 Attribute	What it is used for
Category	

	First level grouping of applications with similar functionalities
Sub-category	Second level grouping of applications with similar functionalities
Application-group	Grouping of applications based on brand or application suite
P2P-technology?	Indicate application is peer-to-peer
Encrypted?	Indicate application is encrypted
Tunneled?	Indicate application uses tunneling technique

The values of these six NBAR2 attributes are pre-defined for every application recognized by NBAR2, including custom applications. Users can choose to reassign the attribute values of any NBAR2 application by using CLI ip nbar attribute-set and ip nbar attribute-map.

Below table shows all the six attributes and all the possible values.

Table 2. List of NBAR2 attributes and supported values

NBAR2 Category	NBAR2 Sub-category	NBAR2 Application Group		P2P Technology	Encrypted	Tunnel
browsing	authentication-services	apple-talk-group	skype-group	n	n	n
business-and-productivity-tools	backup-systems	banyan-group	smtp-group	y	y	y
email	client-server	bittorrent-group	snmp-group	unassigned	unassigned	unassigned
file-sharing	commercial-media-distribution	corba-group	sqlsvr-group			
gaming	control-and-signaling	edonkey-emule-group	stun-group			
industrial-protocols	database	fasttrack-group	telepresence-group			
instant-messaging	epayement	flash-group	tftp-group			
internet-privacy	file-sharing	fring-group	vmware-group			
layer2-non-ip	inter-process-rpc	ftp-group	vnc-group			
layer3-over-ip	internet-privacy	gnutella-group	wap-group			
location-based-services	license-manager	gtalk-group	webex-group			
net-admin	naming-services	icq-group	windows-live-messanger-group			
newsgroup	network-management	imap-group	xns-xerox-group			
obsolete	network-protocol	ipsec-group	yahoo-messenger-group			
other	other	irc-group				
trojan	p2p-file-transfer	kerberos-group				
voice-and-video	p2p-networking	ldap-group				
	remote-access-terminal	netbios-group				
	rich-media-http-content	nntp-group				
	routing-protocol	npmp-group				
	storage	other				
	streaming	p2p-file-transfer				
	terminal	pop3-group				
	tunneling-protocols	prm-group				
	voice-video-chat-collaboration	skinny-group				

Performance Collection and Exporting

Based on Flexible NetFlow

All the information collected and exported by AVC is done through Flexible Netflow infrastructure which 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 which analyzes performance metrics for voice, video, and TCP applications. All information is aggregated and then exported through open export format such as Netflow Version 9 and IP Flow Information Export (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.

Flexible Netflow (FNF), Netflow version 9, and IPFIX

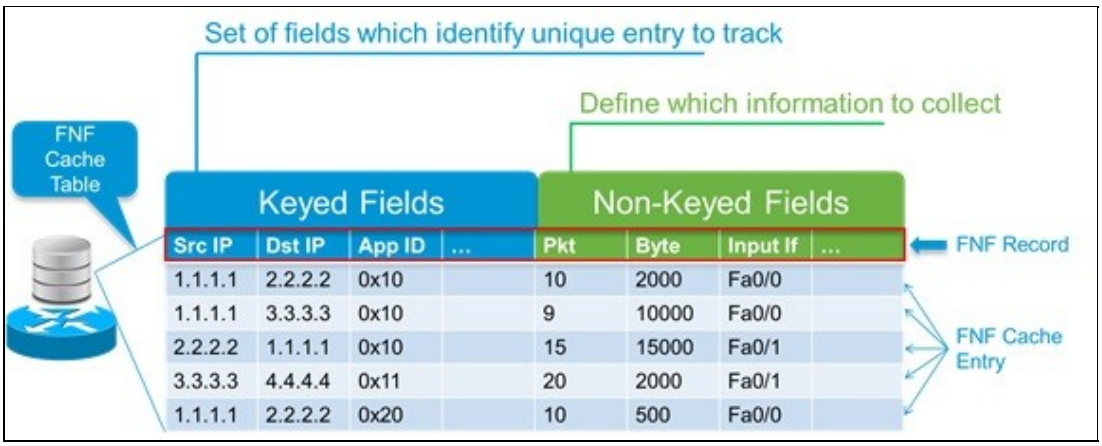

Figure 8. Flexible Netflow Concept ? Keyed fields vs Non-keyed fields. Each of the above row is a cache entry in FNF cache table.

By utilizing Flexible Netflow infrastructure, users have complete control of what information to collect and how it is aggregated by defining what is called FNF record. A FNF record consists of FNF keyed fields and non-keyed fields. Keyed fields are all field(s) which 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 NBAR2 application
- **Collect traffic between two end-points:** Keyed fields are source and destination IP addresses
- **Collect application usage between two end-points:** Keyed fields are source, destination IP addresses, and NBAR2 application

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

For every FNF record, a FNF cache table is created to track and store FNF cache entry. A new FNF cache entry is created when the keyed field(s) of the packet does not match existing FNF cache entry. Otherwise, only the non-keyed fields are updated, e.g. byte count is incremented. The whole FNF cache table is exported either at regular interval or when an event is triggered, e.g. transaction ends. Flexible Netflow infrastructure allows multiple FNF records, each one aggregating or collecting different information. For example, there may be one FNF record which collects application statistics, and other FNF records which collects various performance information.

Netflow version 9 and IPFIX are the export protocols of choices for AVC, because they can accomodate flexible record format and multiple records required by Flexible Netflow infrastructure.

Implementing application visibilty in AVC is simply defining various FNF records to collect the following information,

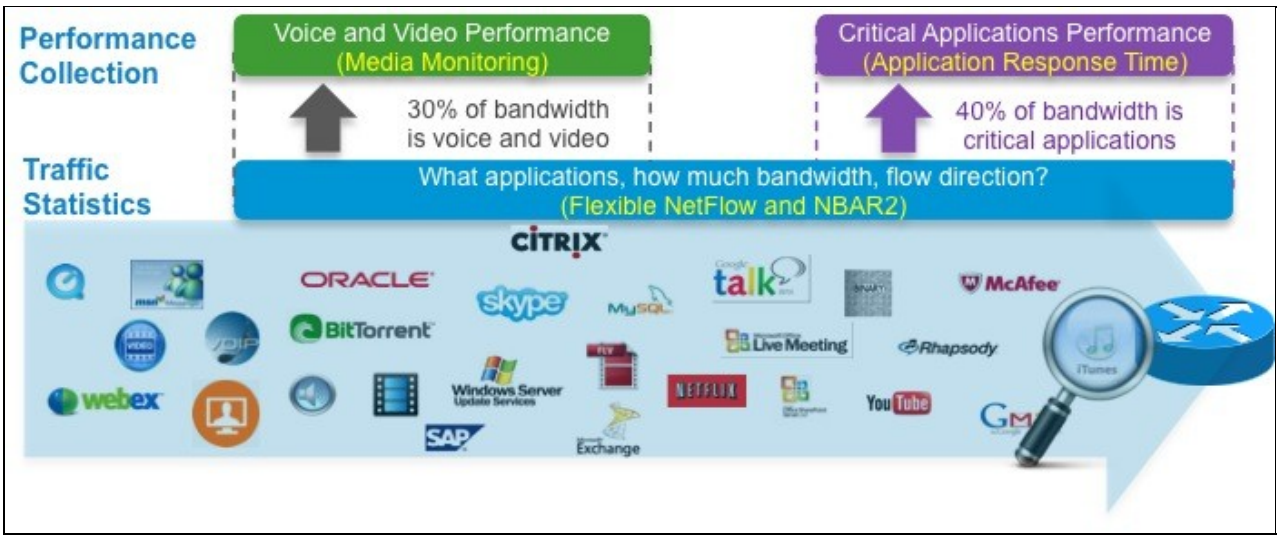

Figure 9. Performance Collection and Exporting Components

Monitoring Profiles and Performance Collection

Based on all FNF records and Performance metrics that we have embedded in Cisco's platforms, the following monitoring profiles have been defined. This is based on customer and Service Providers feedback and can be extended moving forward:

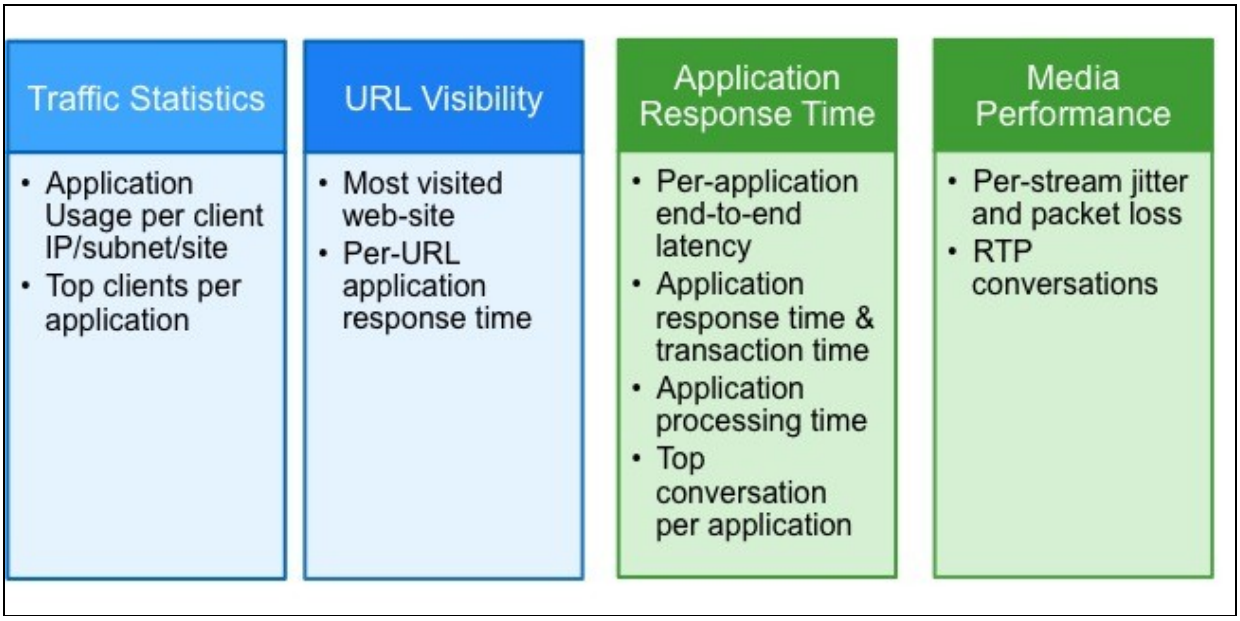

Figure 10. What do we want to monitor?

Performance Collection utilizes specific engines to report performance metrics. All engines analyze and calculate performance metrics from traffic in real time. They also utilize NetFlow version 9 or IPFIX to

export these metrics.

Traffic Statistics

AVC provides the ability to report applications statistics. Application information such as Sharepoint, Netflix, or Google Docs, which is provided by NBAR2, is exported in a FNF field called ***Application ID***. Extracted information such as URI or Hostname is exported in another FNF field called ***Extracted Field***. By having these application related fields along with other information from 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 which include, but are not limited to, top talkers, top applications, visited websites or top clients.

The Global Application Id is a unique Id per application reported of all DPI engines in Cisco:

- IOS ISR, IOS-XE ASR1k, Network Analysis Module, IOS Firewall
- Future: WAAS Express, etc?

is a single field composed of two parts:

- 1 byte of Classification Engine ID. The Classification Engine can be considered as a specific registry for application assignments.
- 3 bytes of Selector ID. The Selector ID length varies depending on the Classification Engine ID.

Figure 11. Application ID Format

Classification Engine ID: A unique identifier for the engine that determined the Selector ID. Thus, the Classification Engine ID defines the context for the Selector ID. Values can be IANA (L3 protocol, L4 port), NBAR (NBAR2 custom application) or Cisco (NBAR2 Deep Packet Inspection).

```
router#show flow exporter option application engines
Engine: prot (IANA_L3_STANDARD, ID: 1)
Engine: port (IANA_L4_STANDARD, ID: 3)
Engine: NBAR (NBAR_CUSTOM, ID: 6)
Engine: cisco (CISCO_L7_GLOBAL, ID: 13)
```

- Selector ID: A unique identifier of the application for a specific Classification Engine ID.

The list of all applications can be found on Cisco Prime Infrastructure, and also directly on the router by looking at the exporter option application table:

```
router#show flow exporter option application table

Engine: cisco (CISCO_L7_GLOBAL, ID: 13)
```

```
appID  Name                 Description
-----  ----                 -----------
13:495  ms-office-365       Microsoft Office 365
13:497  ms-update           Microsoft Update Service

[snip]
```

For more information, refer to the Cisco proposed format in RFC6759

URL Visibility

This monitoring profile provides web browsing activity report such as top domains or hit counts.

Application Response Time

Application Response Time (ART) is an engine which reports approximately 30 performance metrics for TCP traffic.

Application Response Time (ART) engine inspects TCP headers and performs internal timestamping of packets. By inspecting the TCP header sent by client or server, it is able to differentiate request and response messages which are part of each transaction within a TCP connection. It also uses the internal timestamp information and TCP sequence number to calculate various latency metrics such as response time, transaction time, network delay, and application delay. Users can use these metrics to proactively monitor the performance of critical TCP applications and to troubleshoot and isolate problems between network and application.

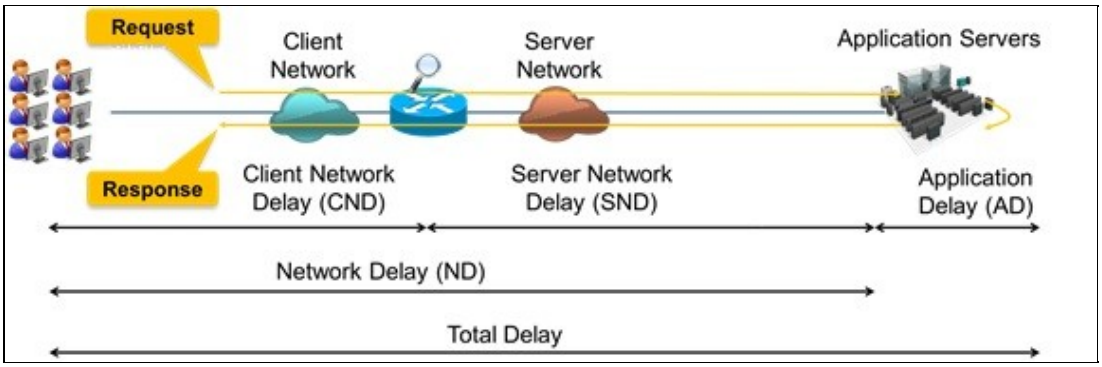

Figure 12. Application Response Time metrics break down.

Total Delay corresponds the total response time experienced by the end users. This includes the time to deliver the request to the application servers, the time to deliver the response back to the clients, and time for

application servers to process the transaction. By providing these latency metrics broken down into Network Delay and Application Delay, users can determine if the impact to application performance, as an increase to Total Delay, is due to the increase in Network Delay or Application Delay. In addition, since the ART engine inspects traffic between client and server, it can also further separate the Network Delay into the Client Network Delay (CND) and Server Network Delay (SND). This allows further isolation of potential network problem into the client or server side. If the ART engine is enabled on the branch router such as ISR G2, CND approximates LAN delay while the SND approximates WAN delay, and vice versa if ART engine is enabled on the headend router.

Media Monitoring

Media Monitoring (MMON) is an engine which reports performance metrics for RTP traffic.

Media Monitoring (MMON) engine collects performance information such as jitter and packet loss for RTP traffic, in addition to per-stream byte count and packet count, at the granularity of SSRC level. This is done by inspecting the timestamp and sequence number information in RTP header, and comparing the expected received packets with received packets, in order to provide loss packets and loss rate. RTP payload type in the RTP header provides information about the clock rate.

Network Management

All the information exported by AVC is opened standard, Netflow Version 9 and IPFIX. This allows both Cisco and 3rd party network management tool products to support AVC. For the current list of 3rd party products which support AVC, please visit http://developer.cisco.com/web/avc

Figure 13. Network management for AVC

Cisco Prime Infrastructure can also configure AVC monitoring for both the ISR G2 and ASR1000. With its one-click configuration, AVC can be enabled on a device within minutes. For bulk deployment, an AVC configuration template is also provided.

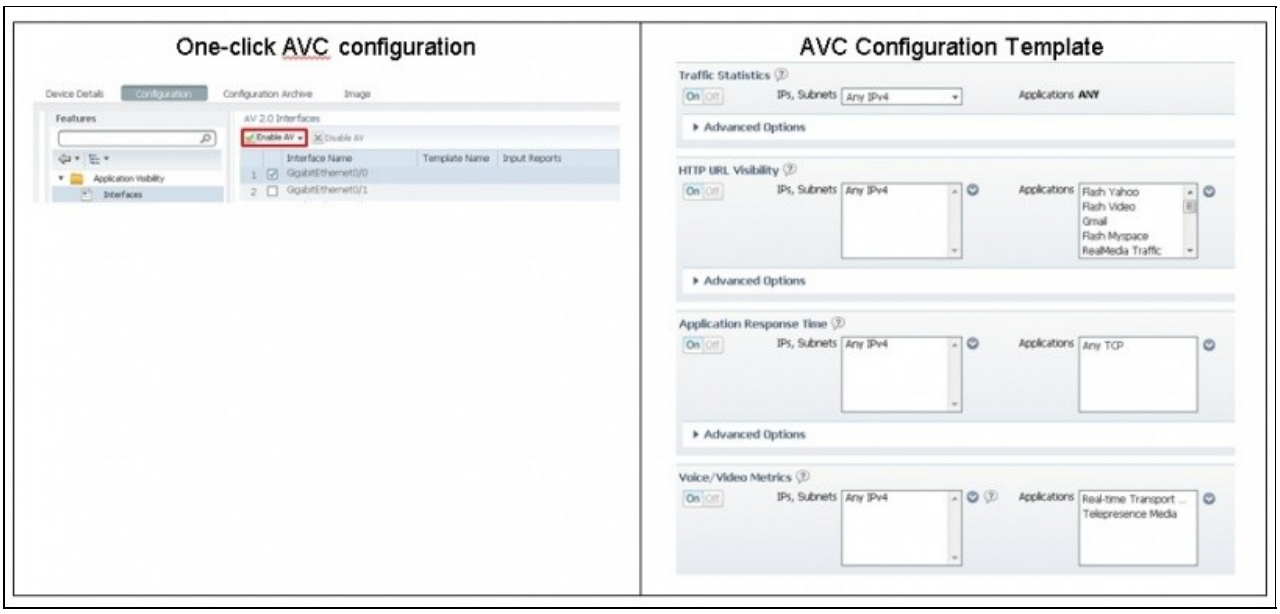

Figure 14. AVC configuration in Cisco Prime Infrastructure

The data provided by AVC can be used for multiple purposes, proactive monitoring, capacity planning, and troubleshooting both infrastructure and application performance issues. The types of reports which can be generated by AVC include, but are not limited to:

- **Top N report:** Top applications, top clients, top servers, top URLs
- **Throughput:** Application distribution over interface
- **Application Performance:** Latency, data transfer time, application latency
- **Voice and Video Performance:** Jitter, Voice conversation report

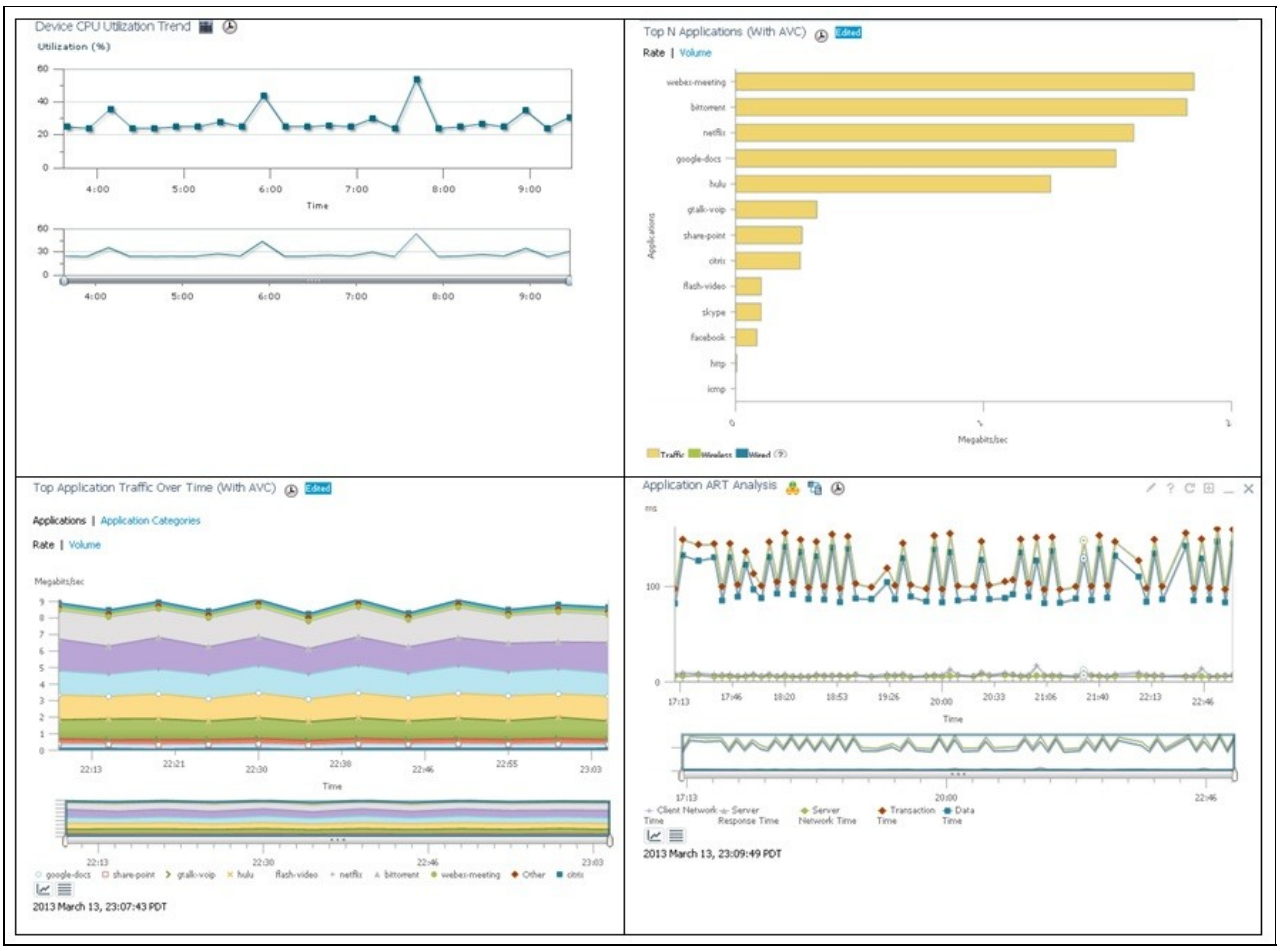

Figure 15. Sample reports from Cisco Prime Infrastructure

Control

AVC utilizes two technologies to provide application-level control to provide application bandwidth and path control.

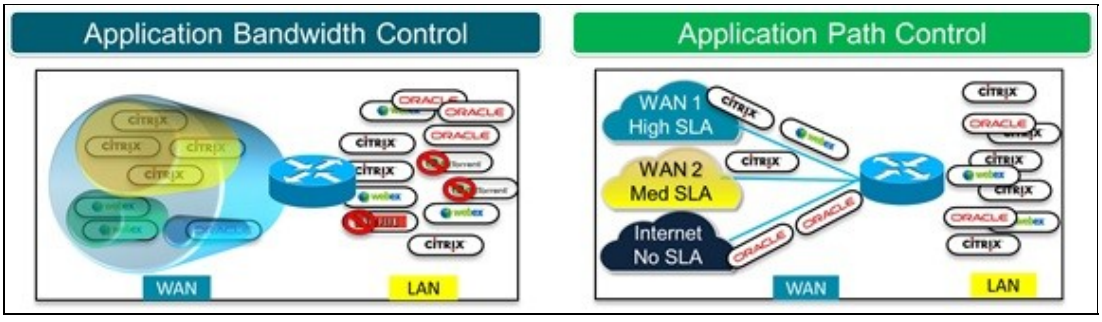

Figure 16. Control technologies used in AVC

QoS with NBAR2

By using **Cisco QoS** technology in conjunction with application identification provided by NBAR2, AVC can provide per-application bandwidth control such as guaranteeing bandwidth, limiting maximum

bandwidth, and prioritizing latency-sensitive application. QoS classification (class-map) has been enhanced to support classification based on NBAR2 application and attributes. These classification criteria can work in conjunction with existing QoS classification criteria such as ACL or DSCP. For more information on QoS, please visit http://www.cisco.com/go/qos

Performance Routing

AVC can also provide intelligent path selection through **Cisco Performance Routing (PfR)** technology. When there are multiple links, PfR can monitor the traffic path in real time and select the path which can satisfy the performance requirement for the application. For example, network administrator can define a policy for real time voice traffic with performance threshold such as delay or jitter, PfR will constantly monitor all the available paths and only send traffic over the paths which can meet the performance requirement.

For more information on PfR, please visit PfR Home Page

Conclusion

In today's environment, network has critical roles to deliver optimal application experience to the end users, and at the same time provide network admin visibility into the applications and their performance in the network. Cisco AVC addresses these challenges by providing the capabilities which are integrated into the network infrastructure to identify, monitor, and control applications. This integrated approach simplifies the operation, yet provides pervasive application visibility and control to address the increasing challenges of delivering applications with high quality of experiences.

For More Information

- Cisco AVC: http://www.cisco.com/go/avc
- Cisco AVC Knowledge Base Portal: http://www.cisco.com/go/avcportal
- Cisco Prime Infrastructure: http://www.cisco.com/go/ciscoprimeinfrastructure
- Cisco Developer Network (CDN) for AVC: http://developer.cisco.com/web/avc