Cisco Application Visibility and Control (AVC)

Q. What is Cisco Application Visibility and Control?

A. Cisco Application Visibility and Control (AVC) is a solution that uses multiple technologies and management tools that, when working together, provides a powerful and pervasive integrated solution for application visibility and control based on stateful deep packet inspection (DPI).

Q. How does AVC work?

A. With the Cisco AVC solution, Cisco wireless controllers can identify applications within the traffic flow using DPI technology and mark it with certain differentiated services code point (DSCP) value. It can collect various wireless performance metrics such as bandwidth use in terms of applications and clients. Then, using quality of service (QoS), routers/switches can reprioritize critical applications or deny an application's bandwidth use.

Q. What technology is used in the AVC solution?

A. Cisco AVC consists of the following technologies:

- Network-Based Application Recognition Version 2 (NBAR2), next-generation DPI technology that can identify more than 1000 applications and support application categorization, with the ability to update the protocol definition.
- NetFlow Version 9 export to select and export data of interest, allowing easy consumption of application performance statistics by Cisco and third-party applications.
- Reporting and management tools, such as Cisco Prime™ Infrastructure with Assurance module, an enterprise-grade infrastructure and service-monitoring tool for reporting of application and network performance that can provide up to 30 different reports for application visibility.
- QoS to facilitate the control of application performance.

Q. Why AVC is important in a wireless network?

A. A wireless network is a shared medium, which means that if a user downloads or uploads a huge amount of traffic over the wireless network, that user might consume a disproportionately large amount of the wireless network bandwidth, thereby adversely affecting the performance of other users. If that user happens to upload/download non-business-critical data while other users are trying to access business-critical applications, their productivity will be lost. In order to prioritize the enterprise's business-critical applications over the non-business-critical applications, AVC plays a primary role in recognizing, reporting, and controlling the applications that are accessed over the wireless network. It also helps with wireless network capacity planning and troubleshooting.

Q. Which wireless controllers support AVC?

A. AVC is currently supported on Cisco 2500, 5500, and 8500 Series Wireless Controllers; Cisco Flex 7500 Series Wireless Controllers; and Cisco Wireless Services Module 2 (WiSM2) when deployed in central mode (formerly local mode running AireOS Version 7.4 or greater).

Q. Do customers need a special license to use the AVC feature over a Cisco wireless network?

A. No.

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

Q. How many applications does AVC recognize?

A. AVC currently recognizes thousands of applications, including voice/video, email, file sharing, gaming, and peer-to-peer (P2P) applications.

Q. How easy is it for a customer to use AVC to prioritize real-time traffic such as voice and video?

A. AVC identifies more than 1000 applications, including several voice and video applications. In addition, AVC has a special category for "voice-video" applications, which customers can use in their QoS policies to mark with a higher DSCP value for prioritizing throughout the network.

Q. What applications/protocols are categorized under "voice-video"?

A. About 60 application protocols are currently classified under the "voice-video" category. To name a few, these include Cisco WebEx®, Cisco Jabber®, Microsoft Lync, Apple QuickTime, Apple FaceTime, Skype, YouTube, Netflix, RTSP, RTP, SIP, H.323, RTCP, and more. For a detailed list, refer to the 7.4 configuration guide.

Q. How easy is it for a customer use AVC to control P2P traffic?

A. AVC identifies more than 1000 applications, several among these being P2P applications. In addition, AVC has a special category for P2P applications, which customers can use in their QoS policies to filter on P2P.

Q. If I'm using AVC on my WLAN infrastructure, do I still need to use the medianet functionality on the wired infrastructure?

A. AVC complements medianet by providing visibility into and control over both application and media applications. AVC can coexist with the medianet passive monitoring capability called performance monitoring to monitor voice or video traffic. Network administrators can view performance metrics collected by medianet performance monitoring, such as jitter or loss, through the Cisco Prime Assurance voice/video dashboard.

Q. Can a customer slow down a particular scavenger-level application such as YouTube or BitTorrent at work?

A. Yes, AVC integration with QoS allows you to create a policy to mark traffic using a DSCP value based on application knowledge.

Q. Can a customer only use NetFlow v9 without using the associated NBAR2 for deep packet inspection?

A. No, a customer cannot deploy NetFlow v9 alone.

Q. Can the application be marked or dropped at WLAN, SSID, or BSSID level?

A. The QoS functionality uses Layer 3 and Layer 4 information so that applications can be marked or dropped at WLAN or SSID level. For example, no Netflix will be supported on enterprise SSID, but guests can run Netflix.

Q. Will there be any performance effects in terms of wireless controller throughput support by enabling AVC?

A. Most campus environments will not experience any discernable performance effect on the wireless controllers because of the additional deep packet inspection of NBAR2, QoS, and associated export with NetFlow v9. In a heavily loaded network with multiple SSIDs, full capacity of access points and clients, and a mix of applications with small packet sizes, some amount of performance effect can be expected.

Q. Is AVC IPv6 application aware?

A. No, AVC for IPv6 traffic is not supported.

Q. What management tools can we use with AVC?

A. AVC supports reporting using Cisco Prime Infrastructure with Assurance module.

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

Q. Is Cisco Prime infrastructure or Cisco Prime NAM mandatory for the AVC solution?

A. No, it is not a mandatory requirement for enabling and using the AVC solution. The Cisco wireless controller web GUI itself provides configuration menus and reporting charts for enabling AVC and monitoring the wireless network. However, Cisco Prime infrastructure is recommended because it can be used across wired devices such as Cisco ASR 1000, Cisco Integrated Services Routers (ISRs), and Cisco wireless networks.

Q. What additional benefits does Cisco Prime infrastructure provide when compared with the wireless controller web GUI?

A. First, Cisco Prime infrastructure has been supports AVC for Cisco wired devices (routers and switches) and Cisco wireless network. Second, Cisco Prime infrastructure enables customers to store historical information (daily/weekly/monthly) about wireless network devices and its clients' performance metrics such as throughput, QoS-related metrics, and location history of wireless clients that can be used for capacity planning and troubleshooting.

Q. Can AVC be used with third-party management tools?

A. The information exported by AVC is in the standard NetFlow Version 9 format and certainly lends itself to use with third-party tools. One example third-party tool that can create custom reports for Cisco AVC is Plixer Scrutinizer.

Q. What are the supported export formats?

A. AVC currently supports the NetFlow Version 9 export format. The following unique elements are included in the current version of the wireless AVC NetFlow record:

- applicationTag
- ipDiffServCodePoint
- octetDeltaCount
- packetDeltaCount
- postIpDiffServCodePoint
- staIPv4Address
- staMacAddress
- wlanSSID
- wtpMacAddress

Q. What is a protocol pack?

A. Starting version 7.5, Wireless LAN Controllers will support Protocol Packs. In version 7.4, protocols were embedded within the operating software and customers had to upgrade the image 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 upgrading the Cisco operating software.

Q. What is the release model for the protocol packs?

A. Model is based on alternating between major and minor updates.

Major protocol updates include support for new protocols, updates and bug fixes.

Minor protocol updates do not include support for new protocols.

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

Q. What Controller models support protocol packs?

A.

- Cisco 5508 Series Wireless LAN Controller
- Cisco Wireless Services Module 2 (WiSM2)
- Cisco 8510 Series Wireless Controller
- Cisco Flex 7510 Wireless Controller

Note: While the Cisco 2500 series wireless controller supports AVC, it does not support the capability to upgrade the protocol packs without upgrading software code.

Q. Where do customers get the protocol pack?

A. Customers can download protocol packs from CCO using the software type “NBAR2 Protocol Pack”.

Products > Cisco Products > Cisco Interfaces and Modules > Cisco Services Modules > **Cisco Wireless Services Module 2 (WiSM2)**
Products > Cisco Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 5500 Series Wireless Controllers > **Cisco 5508 Wireless Controller**
Products > Cisco Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 8500 Series Wireless Controllers > **Cisco 8510 Wireless Controller**
Products > Cisco Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco Flex 7500 Series Wireless Controllers > **Cisco Flex 7510 Wireless Controller**

Q. How can users load a protocol pack?

A. Using FTP or TFTP, users can download newer versions of protocol packs.

The command syntax is:

- Transfer download datatype avc-protocol-pack
- Transfer download start
- Default protocol-pack

Q. How can I show version of the existing AVC engine or protocol-pack?

A. The following command should be used:

- Show avc engine version
- AVC Engine Version: 13
- Show avc protocol-pack version
- AVC Protocol Pack Version: 4.0

Q. If I load incompatible protocol pack on my Wireless LAN Controller, what is the impact?

A. If a user tries to load incompatible protocol pack on controller, it will be rejected with an error message saying protocol pack is incompatible with underlying IOS NBAR software version.

The Previous protocol pack will remain active on device.

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

Q. What version of protocol packs can I download on the Wireless LAN Controller?

A. Protocol packs are released for specific NBAR engine versions

For example, rel 7.5 WLC has NBAR engine 13, so protocol packs for it are written for engine under the Wireless LAN Controller download section on CCO.

The name of the protocol pack file is as follows:

- pp-AIR-7.5-13-M.m.0.pack
  - PP stands for protocol pack
  - AIR stands for Aironet
  - AireOS Version is 7.5
  - The NBAR2 Engine version is 13
  - M stands for Major release
  - m stands for minor release

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

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

Printed in USA C67-722538-02 08/13

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