Configuring Application Visibility and Control

Application Visibility and Control

Application Visibility and Control (AVC) classifies applications using deep packet inspection techniques with the Network-Based Application Recognition (NBAR) engine, and provides application-level visibility and control (QoS) in wireless networks. After the applications are recognized, the AVC feature enables you to either drop, mark, or police the data traffic.

Using AVC, we can detect more than 1000 applications. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

Note You can view list of 30 applications in Top Applications in Monitor Summary section of the UI.

AVC DSCP marks only the DSCP of the original packet in the controller in both directions (upstream and downstream). It does not affect the outer CAPWAP DCSP. AVC DSCP is applicable only when the application is classified. For example, based on the AVC profile configuration, if an application is classified as ftp or http, the corresponding DSCP marking is applied irrespective of the WLAN QoS. For downstream, the DSCP value of outer CAPWAP header and inner packet's DSCP are taken from AVC DSCP. WLAN QoS is only applicable for all traffic from WLC to AP through CAPWAP. It does not change the DSCP of the original packet.

Using AVC rule, you can limit the bandwidth of a particular application for all the clients joined on the WLAN. These bandwidth contracts coexist with per-client downstream rate limiting with per client downstream rate limits that takes precedence over the per-application rate limits.

Note When you downgrade the controller from 8.0 to any earlier version, the AVC rate limit rules display the action as drop. This action is expected since the AVC rate limit rule is introduced in the controller version 8.0.

AVC is supported in central switching mode on the following controller platforms: Cisco 2504 WLCs, Cisco 5508 WLCs, Cisco Flex 7510 WLCs, Cisco 8510 WLCs, and Cisco Wireless Services Module 2 (WiSM2).

The number of concurrent flows supported for AVC classification on different controller platforms are noted in the following table.

Cisco WLC Platform	Flow
Cisco 2504 WLC	26,250
Cisco 5508 WLC	183,750
Cisco WiSM2	393,750
Cisco 8510 WLC	336,000
Cisco 5520 WLC	336,000
Cisco 8540 WLC	336,000

Application Visibility and Control Protocol Packs

Protocol packs are a means to distribute protocol updates outside the controller software release trains, and can be loaded on the controller without replacing the controller software.

The Application Visibility and Control Protocol Pack (AVC Protocol Pack) is a single compressed file that contains multiple Protocol Description Language (PDL) files and a manifest file. A set of required protocols can be loaded, which helps AVC to recognize additional protocols for classification on your network. The manifest file gives information about the protocol pack, such as the protocol pack name, version, and some information about the available PDLs in the protocol pack.

The AVC Protocol Packs are released to specific AVC engine versions. You can load a protocol pack if the engine version on the controller platform is the same or higher than the version required by the protocol pack.

AAA override for AVC profiles

The AAA attribute for client or user profile is configured on the AAA server using authentication from RADIUS server or Cisco ACS or ISE. The AAA attribute is processed during layer 2 or layer 3 authentication by the controller and the same is overridden by what is configured on the WLAN.

The AAA AVC profile is defined as a Cisco AV air. The string option is defined as **avc-profile-name** and this value has to be configured for any AVC profile available in the controller.

This section contains the following subsections:

Restrictions for Application Visibility and Control

- IPv6 packet classification is not supported.
- Layer 2 roaming is not supported across controllers.
- Multicast traffic is not supported.
- Controller GUI support is not present for the AVC Protocol Pack feature.
- Downloading the AVC Protocol Pack is not supported on the Cisco 2500 Series Wireless LAN Controllers.

- The number of applications that you can apply rate limit is 3.
- Only one rule can be configured per application. An application cannot have both a rate limit as well as a Mark rule.
- If the standby controller has a different protocol pack version installed before pairing, then the active and standby controllers will have different protocol packs versions after pairing, in a HA environment. In the standby controller, the transferred protocol pack takes the preference over default protocol pack.

  For example, the controller with the software release 8.0 contains Protocol Pack version 9.0 by default. Before pairing, if one of the controllers has a Protocol Pack version 11.0 installed, then after pairing one controller contains Protocol Pack version 9.0 and the other controller contains Protocol Pack 11.0 installed.
- AVC rate limiting is not supported on Cisco 2504 WLC.

Configuring Application Visibility and Control (GUI)

Step 1 Create and configure an AVC profile by following these steps:

a) Choose **Wireless** > **Application Visibility and Control** > **AVC Profiles**.
b) Click **New**.
c) Enter the AVC profile name.
d) Click **Apply**.
e) On the **AVC Profile Name** page, click the corresponding AVC profile name.

   The **AVC Profile > Edit** page is displayed.

f) Click **Add New Rule**.
g) Choose the application group and the application name from the respective drop-down lists.

   View the list of default AVC applications available by choosing **Wireless** > **Application Visibility and Control** > **AVC Applications**.

h) From the **Action** drop-down list, choose either of the following:

   - **Drop**—Drops the upstream and downstream packets that correspond to the chosen application.
   - **Mark**—Marks the upstream and downstream packets that correspond to the chosen application with the Differentiated Services Code Point (DSCP) value that you specify in the **DSCP (0 to 63)** drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.

     Note The default action is to give permission to all applications.

i) If you choose **Mark** from the **Action** drop-down list, choose a DSCP value from the **DSCP (0 to 63)** drop-down list.

   The DSCP value is a packet header code that is used to define QoS across the Internet. The DSCP values are mapped to the following QoS levels:

   - **Platinum (Voice)**—Assures a high QoS for Voice over Wireless.
   - **Gold (Video)**—Supports high-quality video applications.
   - **Silver (Best Effort)**—Supports normal bandwidth for clients.

- **Bronze (Background)**—Provides the lowest bandwidth for guest services.

You can also choose **Custom** and specify the DSCP value. The valid range is from 0 to 63.

j) Click **Apply**.
k) Click **Save Configuration**.

Step 2 Associate an AVC profile to a WLAN by following these steps:

a) Choose **WLANs** and click the corresponding WLAN ID.

The **WLANs > Edit** page is displayed.

b) Click the **QoS** tab.
c) Choose the AVC profile from the **AVC Profile** drop-down list.
d) Click **Apply**.
e) Click **Save Configuration**.

Configuring Application Visibility and Control (CLI)

- Create or delete an AVC profile by entering this command:

  config avc profile *avc-profile-name* {**create** | **delete**}
- Add a rule for an AVC profile by entering this command:

  config avc profile *avc-profile-name* **rule add application** *application-name* {**drop** | **mark** *dscp-value* | **ratelimit** *Average Ratelimit value Burst Ratelimit value*}
- Remove a rule for an AVC profile by entering this command:

  config avc profile *avc-profile-name* **rule remove application** *application-name*
- Configure an AVC profile to a WLAN by entering this command:

  config wlan avc *wlan-id* **profile** *avc-profile-name* {**enable** | **disable**}
- Configure application visibility for a WLAN by entering this command:

  config wlan avc *wlan-id* **visibility** {**enable** | **disable**}

  Note Application visibility is the subset of an AVC profile. Therefore, visibility is automatically enabled when you configure an AVC profile on the WLAN.
- Download an AVC Protocol Pack to the controller by entering these commands:

  1. **transfer download datatype avc-protocol-pack**
  2. **transfer download start**
- View information about all AVC profile or a particular AVC profile by entering this command:

  show avc profile {**summary** | **detailed** *avc-profile-name*}
- View information about AVC applications by entering these commands:

- **show avc applications** [*application-group*]—Displays all the supported AVC applications for the application group.
- **show avc statistics application** *application_name* **top-users** [**downstream wlan** | **upstream wlan** | **wlan**] [*wlan_id*] } —Displays AVC statistics for the top users of an application.
- **show avc statistics top-apps** [**upstream** | **downstream**]—Displays the AVC statistics for the most used application.
- **show avc statistics wlan** *wlan_id* {**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**] }—Displays the AVC statistics of a WLAN per application or top applications or top application groups.
- **show avc statistics client** *client_MAC* {**application** *application_name* | **top-apps** [**upstream** | **downstream**] }—Displays the client AVC statistics per application or top applications.

Note You can view list of 30 applications using the **show avc applications** and **show avc statistics** commands.

- View the protocol pack that is used on the controller by entering this command:

  show avc protocol-pack version
- View the AVC engine version information by entering this command:

  show avc engine version
- Configure troubleshooting for AVC events by entering this command:

  debug avc events {**enable** | **disable**}
- Configure troubleshooting for AVC errors by entering this command:

  debug avc error {**enable** | **disable**}

Configuring NetFlow

NetFlow

NetFlow is an embedded instrumentation within the controller software to characterize wireless network flows. NetFlow monitors each IP flow and exports the aggregated flow data to the external NetFlow collectors.

The NetFlow architecture consists of the following components:

- Collector—Entity that collects all the IP traffic information from various NetFlow exporters.
- Exporter—Network entity that exports the template with the IP traffic information. The controller acts as an exporter.

Note Controller does not support IPv6 address format when acting as an exporter for NetFlow.

Configuring NetFlow (GUI)

Step 1 Configure the Exporter by performing these steps:

a) Choose **Wireless** > **Netflow** > **Exporter.**
b) Click **New**.
c) Enter the Exporter name, IP address, and the port number.

The valid range for the port number is from 1 to 65535.

d) Click **Apply**.
e) Click **Save Configuration**.

Step 2 Configure the NetFlow Monitor by performing these steps:

a) Choose **Wireless** > **Netflow** > **Monitor.**
b) Click **New** and enter a Monitor name.
c) On the Monitor List window, click the Monitor name to open the **Netflow Monitor** > **Edit** window.
d) Choose the exporter name and the record name from the respective drop-down lists.

- Client App Record—Better Performance

e) Click **Apply**.
f) Click **Save Configuration**.

Step 3 Associate a NetFlow Monitor to a WLAN by performing these steps:

a) Choose **WLANs** and click a WLAN ID to open the **WLANs** > **Edit page.**
b) In the QoS tab, choose a NetFlow monitor from the **Netflow Monitor** drop-down list.
c) Click **Apply**.
d) Click **Save Configuration**.

Configuring NetFlow (CLI)

- Create an Exporter by entering this command:

  config flow create exporter *exporter-name ip-addr port-number*
- Create a NetFlow Monitor by entering this command:

  config flow create monitor *monitor-name*
- Associate or dissociate a NetFlow monitor with an exporter by entering this command:

  config flow {**add** | **delete**} **monitor** *monitor-name* **exporter** *exporter-name*
- Associate or dissociate a NetFlow monitor with a record by entering this command:

  config flow {**add** | **delete**} **monitor** *monitor-name* **record ipv4_client_app_flow_record**
- Associate or dissociate a NetFlow monitor with a WLAN by entering this command:

  config wlan flow *wlan-id* **monitor** *monitor-name* {**enable** | **disable**}
- View a summary of NetFlow monitors by entering this command:

  show flow monitor summary
- View information about the Exporter by entering this command:

show flow exporter {**summary** | **statistics**}

- Configure NetFlow debug by entering this command:

debug flow {**detail** | **error** | **info**} {**enable** | **disable**}