IOS XE Wireless LAN Controller AVC/QoS Design

At-A-Glance

Role in Wireless Campus Network

Cisco IOS XE wireless LAN controllers may be deployed in a centralized controller model or in a converged access model. In either deployment model, IOS XE controllers centrally manage QoS policies which - in turn - are enforced on wireless LAN access points, including:

- Application Visibility and Control (AVC)
- classification
- marking
- policing
- dropping
- DSCP-to-UP and UP-to-DSCP mapping

Enabling Application Visibility

There are four steps to enabling application visibility on IOS XE wireless LAN controllers:

1. Create a Flow Record
2. (Optional) Create a Flow Exporter
3. Create a Flow Monitor
4. Apply the Flow Monitor to the WLAN

Step 1: Create a Flow Record
The first step in enabling application visibility for IOS XE wireless controllers is to configure a flow record. A flow record specifies the details of a given flow that is to be tracked by matching one or more of the following parameters:

- IPv4 Source Address
- IPv4 Destination Address
- Transport Protocol Source-Port
- Transport Protocol Destination Port
- Flow Direction
- Application Name
- WLAN SSID

Once the match details are specified so as to identify a discrete flow, then the flow record also specifies the type of statistics and information that is to collected by the flow record, including:

- Bytes
- Packets
- Access Point (BSSID) MAC address
- Client MAC address

Step 2: (Optional) Create a Flow Exporter
An optional second step is to configure a flow exporter. The flow exporter defines the destination and transport parameters of the management station that the flow details are to be exported to via Flexible NetFlow (FNF). Application flow information is gathered by the NBAR2 engine on the access point and sent to the management station using NetFlow version 9 format.

Step 3: Create a Flow Monitor
The next step is to configure a flow monitor. A flow monitor associates a flow record with an optional flow exporter and can be applied to a WLAN.

Step 4: Apply the Flow Monitor to the WLAN
Once the flow monitor has been defined, then it can be applied to a given WLAN(s) and the direction of application can be specified.

Configuring AVC/QoS Policies

Application Visibility - by itself- only reports traffic statistics; however, the same deep packet inspection engine can be coupled with QoS policies to control these applications, via marking, policing or even outright dropping.

The steps to configure AVC/QoS policies on IOS XE wireless LAN controllers are:

1. Configure AVC-based class-maps
2. Configure a policy map to mark, police or drop applications
3. Apply the policy-map to the WLAN

Step 1: Configure AVC-based Class-Maps
The key command to enabling AVC within a standard Modular QoS Command-Line-Interface (MQC) class-map is **match protocol**. This command can be configured to match on:

- Individual applications:
  match protocol *application_name*
- Categories of applications:
  match protocol attribute category *category_name*
- Sub-categories of applications:
  match protocol attribute sub-category *sub_cat_name*
- Groups of applications:
  match protocol attribute application-group *app_group_name*

Step 2: Configure a Policy-Map
The policy map will specify the action to be performed on a given class of traffic. These actions may include:

- Marking via the **set** command
- Policing via the **police** command
- Dropping via the **drop** command

  Note: Only upstream dropping is supported

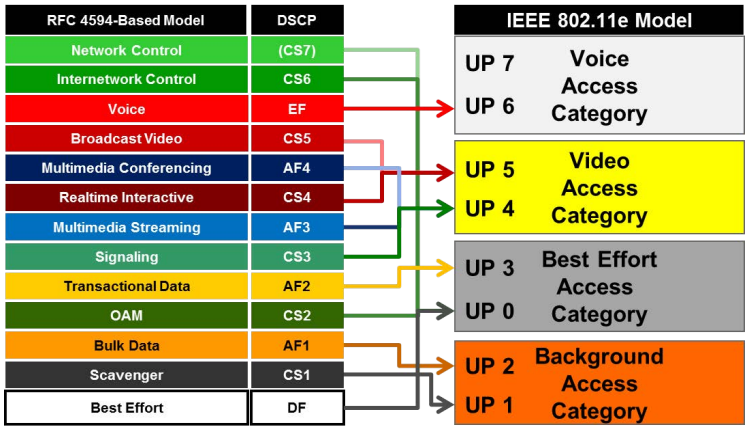
Step 3: Attach the Policy-Map to the WLAN
The policy map is attached to the desired WLAN(s) via a **service-policy** statement, which also specifies direction of application.

Configuring DSCP-to-UP Table Maps

There may be times when the default mappings between L2 User Priority and L3 DSCP may be sub-optimal for QoS. This can sometimes be the case because of marking recommendation discrepancies between the IEEE and IETF standards bodies.

The Cisco-recommended DSCP-to-UP mappings to reconcile IETF and IEEE markings are shown in Figure 1.

Figure 1 Cisco Recommended DSCP-to-UP Mappings



In the upstream direction, Cisco recommends trusting DSCP.

Note: The details behind Cisco's recommendations for IETF/IEEE QoS Mapping are documented in the Internet Draft:
https://tools.ietf.org/html/draft-szigeti-tsvwg-ieee-802-11e-00

Enabling Application Visibility

Step 1: Create a Flow Record

```
flow record AVC-FLOW-RECORD
 description BASIC-AVC-FLOW-RECORD
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match flow direction
 match application name
 match wireless ssid
 collect counter bytes long
 collect counter packets long
 collect wireless ap mac address
 collect wireless client mac address
```

Step 2: Create a Flow Exporter

```
flow exporter AVC-FLOW-EXPORTER
 destination 10.10.10.10
 transport udp 2055
 destination 10.20.20.20
 transport udp 9991
```

Note: Lancope collects Netflow on port 2055 and Cisco Prime Infrastructure collects Netflow on port 9991

Step 3: Create a Flow Monitor

```
flow monitor AVC-FLOW-MONITOR
 record AVC-FLOW-RECORD
 exporter AVC-FLOW-EXPORTER
```

Step 4: Apply the Flow Monitor to the WLAN

```
wlan EMPLOYEE-WLAN
 ip flow monitor AVC-FLOW-MONITOR input
 ip flow monitor AVC-FLOW-MONITOR output
```

Note: Highlighted commands are interface specific; otherwise these are global.

Configuring AVC/QoS Policies

Step 1: Configure AVC-based Class-Maps

```
class-map match-any VOICE
 match protocol cisco-phone
class-map match-any BROADCAST-VIDEO
 match protocol cisco-ip-camera
class-map match-any REAL-TIME-INTERACTIVE
 match protocol telepresence-media
class-map match-any CALL-SIGNALING
 match protocol skinny
 match protocol telepresence-control
class-map match-any TRANSACTIONAL-DATA
 match protocol citrix
 match protocol sap
class-map match-any BULK-DATA
 match protocol attribute category email
 match protocol attribute category file-sharing
 match protocol attribute sub-category backup-systems
class-map match-any SCAVENGER
 match protocol attribute category gaming
 match protocol attribute application-group skype-group
```

Step 2: Configure a Policy-Map

```
policy-map AVC-MARKING
 class VOICE
  set dscp ef
 class BROADCAST-VIDEO
  set dscp cs5
 class REAL-TIME-INTERACTIVE
  set dscp cs4
 class CALL-SIGNALING
  set dscp cs3
 class TRANSACTIONAL-DATA
  set dscp af21
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class class-default
  set dscp default
```

Step 3: Attach the Policy-Map to the WLAN

```
wlan EMPLOYEE-WLAN
service-policy client input AVC-MARKING
```

Configuring Downstream DSCP-to-UP Table Map (Upstream DSCP-Trust is enabled by default)

Step 1: Configure Cisco-Recommended Downstream DSCP-to-UP Table Map

```
table-map DSCP-to-UP
 map from 46 to 6
 map from 40 to 5
 map from 38 to 4
 map from 36 to 4
 map from 34 to 4
 map from 32 to 5
 map from 30 to 4
 map from 28 to 4
 map from 26 to 4
 map from 24 to 4
 map from 22 to 3
 map from 20 to 3
 map from 18 to 3
 map from 16 to 0
 map from 14 to 2
 map from 12 to 2
 map from 10 to 2
 map from 8 to 1
 default 0
```

Step 2: Reference this Table-Map within a Policy-Map

```
policy-map DSCP-TO-UP-POLICY
 class class-default
  set wlan user-priority
      dscp table DSCP-to-UP
```

Step 3: Attach the Policy-Map to WLAN

```
wlan EMPLOYEE-WLAN
 service-policy output
  DSCP-TO-UP-POLICY
```

For more details, see the AVC/QoS Design chapter of the BYOD CVD at:

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_AVC.html

And the Cisco Press book: **End-to-End QoS Network Design** (Second Edition)-Chapters 20 & 21