

Role in Wireless Campus Network

The Cisco AireOS wireless LAN controllers centrally manage QoS policies on wireless LAN access points, as well as perform advanced QoS operations, such as Application Visibility and Control classification, marking and policing.

QoS Design Steps

There are three main steps required to configure QoS on AireOS WLCs:

1. Select and tune the desired QoS Profile
2. Configure an AVC Profile
 - Apply the QoS and AVC Profiles on the WLAN and (optionally) enable Application Visibility

Step 1: Selecting and Tuning the QoS Profile

QoS Profiles are applied to both upstream and downstream flows on WLC egress. The WLAN QoS Profile defines (as shown in Figure 1):

- **Per-User Bandwidth Contracts—(Optional)** per-user limits for average and peak data and realtime traffic rates.
- **Per-SSID Bandwidth Contracts—(Optional)** per-SSID limits for average and peak data and realtime traffic rates.
- **WLAN Maximum Priority—**The highest DSCP marking value that may be used on the WLAN; this value can override AVC policies as well as DSCP-values received from the wired network. As such, in multiservice WLANs, **it is generally recommended to ensure that the Maximum Priority value be set to voice (i.e., platinum).**
- **Unicast and Multicast Default Priority—**The default DSCP marking value to be used on the WLAN for all traffic not explicitly classified by an overriding AVC Profile. **Typically these values are set as best effort (i.e., silver),** however there may be cases where this default value may be set to background (i.e., bronze), such as if applied to a guest WLAN.
- **Wired QoS Protocol—**Can be set to 802.1p and the maximum CoS value can be defined per WLAN

Figure 1 Design Recommendations for the Platinum QoS Profile for an Employee WLAN

Step 2: Configure an AVC Profile

AVC Profiles are applied to both upstream and downstream flows on WLC ingress. While this may simplify the QoS policy configuration on the WLC, it has design implications in upstream/downstream mapping.

Additionally, each WLAN can have only one AVC profile attached to it to control applications, however an AVC Profile can be attached to multiple WLANs. Also, an AVC Profile can contain a maximum of 32 application rules and a maximum of 16 AVC profiles can be created on a WLC. Also, only 3 AVC applications may be policed in a given profile.

As has been previously discussed, it also is important to note that each WLAN can have both a QoS Profile and an AVC Profile attached to it. The AVC Profile is applied when the packet *enters* the WLC and the QoS policy is applied when packet *exits* the WLC. QoS Profiles may define a Maximum Priority (DSCP value) for packet marking, which will override any AVC Profile marking policy. Thus care should be taken that QoS and AVC Profiles are correctly configured to complement-and not contradict-one another.

An example AVC Profile is shown in Figure 2.

Figure 2 Example AVC Profile for an Employee WLAN

The screenshot shows the Cisco WLC configuration page for the AVC Profile 'AVC-APPS'. The interface is divided into a left sidebar with navigation options and a main content area displaying a table of application rules. The table has columns for Application Name, Application Group Name, Action, and DSCP. A red box highlights the table content. To the right of the table, several application groups are listed with their corresponding DSCP values.

Application Name	Application Group Name	Action	DSCP
cisco-phone	voice-and-video	mark	46
cisco-labber-audio	voice-and-video	mark	46
cisco-labber-video	voice-and-video	mark	34
webex-meeting	voice-and-video	mark	34
telepresence-media	voice-and-video	mark	32
sip	voice-and-video	mark	24
sip-tls	voice-and-video	mark	24
h323	voice-and-video	mark	24
telepresence-control	voice-and-video	mark	24
cisco-labber-control	voice-and-video	mark	24
cisco-labber-im	instant-messaging	mark	18
citrix	business-and-productivity-to	mark	18
salesforce	business-and-productivity-to	mark	18
sap	business-and-productivity-to	mark	18
my-labber-ft	other	mark	10
ftp	file-sharing	mark	10
ftp-data	file-sharing	mark	10
ftps-data	file-sharing	mark	10
cifs	file-sharing	mark	10
exchange	email	mark	10
notes	email	mark	10
imap	email	mark	10
secure-imap	email	mark	10
facebook	browsing	mark	8
youtube	voice-and-video	mark	8
netflix	voice-and-video	mark	8
hulu	voice-and-video	mark	8
skype	voice-and-video	mark	8
msn-messenger-video	voice-and-video	mark	8
bittorrent	file-sharing	mark	8
itunes	file-sharing	mark	8
call-of-duty	other	mark	8

Summary of application groups and their DSCP values:

- Voice applications marked EF
- Multimedia Conferencing applications marked AF41
- TelePresence (Realtime Interactive) marked CS4
- Signaling protocols marked CS3
- Transactional Data applications marked AF21
- Bulk Data applications marked AF11
- Scavenger applications marked CS1

294188

Step 3: Apply the QoS and AVC Profiles on the WLAN and (optionally) enable Application Visibility

With the QoS and AVC Profiles defined, all that remains is to enable these on a given WLAN, as shown in Figure 3.

Additionally, by checking the box for AVC, Application Visibility can also be enabled on the WLAN.

Figure 3 Example AVC Profile for an Employee WLAN

The screenshot shows the Cisco WLC configuration page for the WLAN 'BYOD_Employee'. The 'QoS' tab is selected, and the 'Application Visibility' checkbox is checked. The 'AVC Profile' dropdown menu is open, showing 'AVC-APPS' selected. The 'Quality of Service (QoS)' dropdown is set to 'Platinum (voice)'.

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/or the Cisco Press book: End-to-End QoS Network Design (Second Edition)-Chapter 19