Application Considerations and License Requirements for BYOD

Revised: August 7, 2013

When implementing a BYOD solution, the applications that run on employee-owned devices need to be considered before selecting which of the particular BYOD use cases discussed above to deploy. The application requirements for these devices determine the level of network connectivity needed. The network connectivity requirements in turn influence the choice of the BYOD use case to apply.

Quality of Service

In addition to network connectivity, quality of service (QoS) is an important consideration for applications, especially those delivering real-time media. Device specific hardware, such as dedicated IP phones which send only voice traffic, allowed for the configuration of dedicated voice wireless networks. However, with the widespread use of smartphones and tablets which support collaboration software (such as Cisco's Jabber client), devices are capable of sending voice, video, and data traffic simultaneously. Hence, QoS is necessary to provide the necessary per-hop behavior as such traffic traverses the network infrastructure.

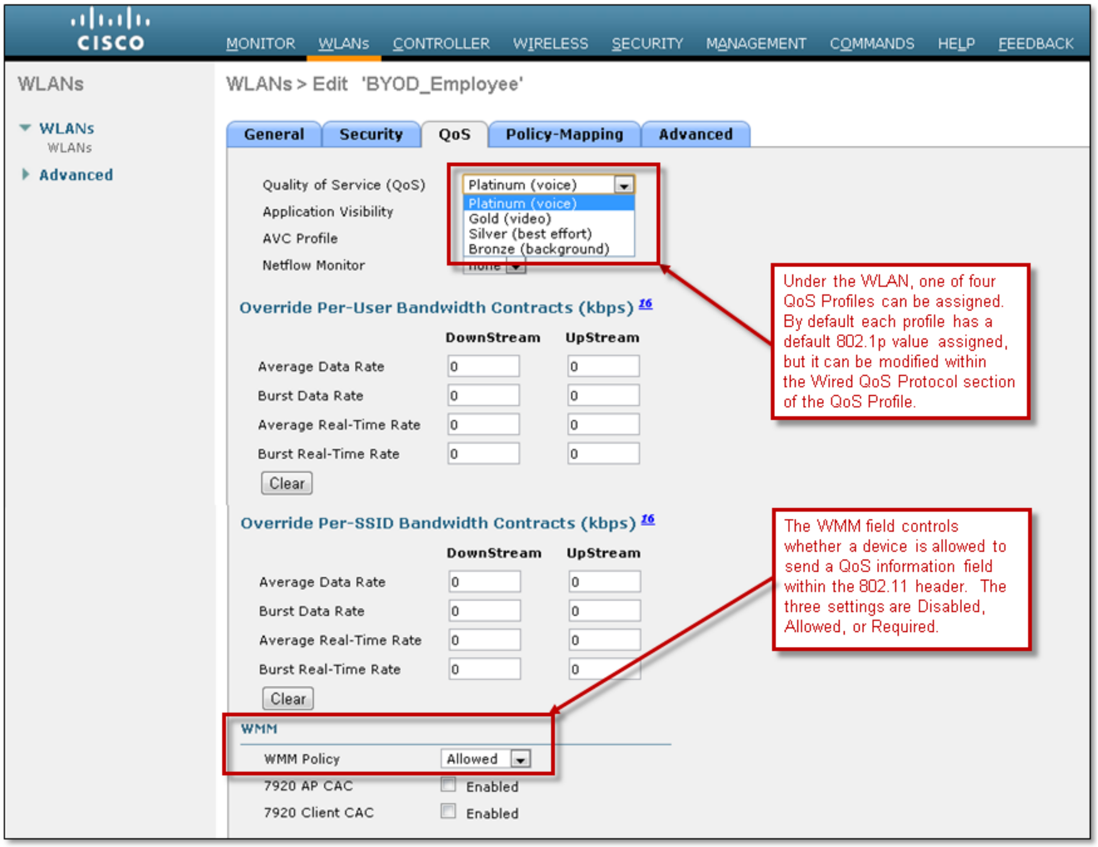
QoS can be categorized into the following broad functions:

- Classification and Marking-including Application Visibility and Control (AVC)
- Bandwidth Allocation/Rate Limiting (Shaping and/or Policing)
- Trust Boundary Establishment
- Queueing

For a discussion regarding implementing wired QoS, refer to Medianet Campus QoS Design 4.0 at: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html.

The following sections discuss various aspects of wireless QoS.

As of Cisco Unified Wireless Network (CUWN) software release 7.3 and above, wireless QoS is configured by applying one of four QoS Profiles—Platinum, Gold, Silver, or Bronze—to the WLAN to which a particular client device is associated. An example of the configuration is shown in Figure 7-1.



WLANs > Edit 'BYOD_Employee'

Quality of Service (QoS): Platinum (voice)
- Platinum (voice)
- Gold (video)
- Silver (best effort)
- Bronze (background)

Application Visibility

AVC Profile

Netflow Monitor: none

Override Per-User Bandwidth Contracts (kbps) 16

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Override Per-SSID Bandwidth Contracts (kbps) 16

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WMM

WMM Policy: Allowed

7920 AP CAC: □ Enabled

7920 Client CAC: □ Enabled

Under the WLAN, one of four QoS Profiles can be assigned. By default each profile has a default 802.1p value assigned, but it can be modified within the Wired QoS Protocol section of the QoS Profile.

The WMM field controls whether a device is allowed to send a QoS information field within the 802.11 header. The three settings are Disabled, Allowed, or Required.

Figure 7-1 Application of a QoS Profile to a WLAN

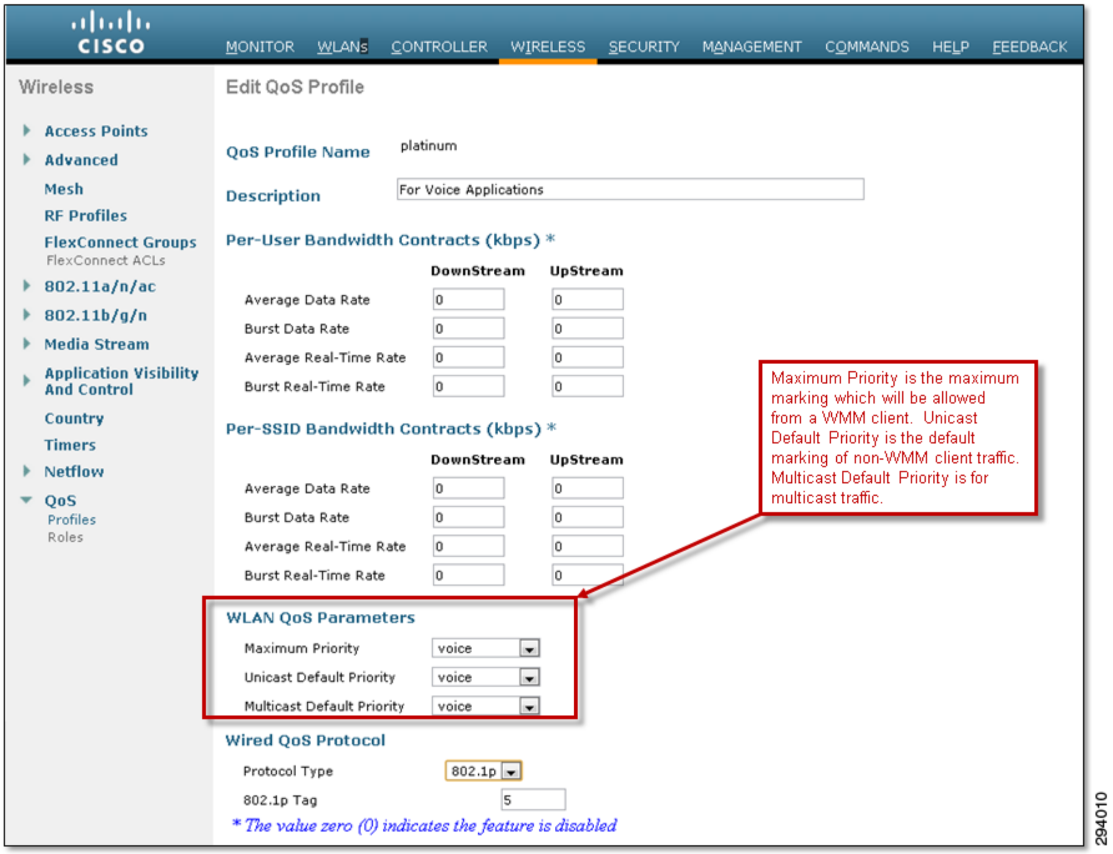
Note that the QoS settings for the profile can be overridden on a per-WLAN basis from within the QoS tab of the WLAN configuration.

The DSCP marking of client traffic, as it traverses the network within a CAPWAP tunnel, is controlled by three fields within the WLAN QoS Parameters field within the QoS Profile:

- Maximum Priority—This is the maximum 802.11 User Priority (UP) value of a packet sent by a Wi-Fi Multimedia (WMM)-enabled client which will be allowed by the access point. The User Priority maps to a DSCP value within the outer header of the CAPWAP tunnel as the packet traverses the network infrastructure. If the WMM-enabled client sends an 802.11 packet with a User Priority higher than allowed, the access point marks the packet down to the maximum allowed User Priority. This in turn maps to the DSCP value of the external CAPWAP header as the packet is sent over the network infrastructure.
- Unicast Default Priority—This is the default 802.11 User Priority (UP) to which a unicast packet sent by a non-WMM-enabled client is assigned. This User Priority also maps to the DSCP value within the outer header of the CAPWAP tunnel as the packet traverses the network infrastructure.
- Multicast Default Priority—This is the default 802.11 User Priority (UP) for multicast traffic. This User Priority maps to a DSCP value within the outer header of the CAPWAP tunnel as the packet traverses the network infrastructure.

An example of the configuration of the WLAN QoS Parameters is shown in Figure 7-2.

Figure 7-2 Controlling the Marking of Wireless Packets



Edit QoS Profile

QoS Profile Name platinum

Description For Voice Applications

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WLAN QoS Parameters

Maximum Priority voice
Unicast Default Priority voice
Multicast Default Priority voice

Wired QoS Protocol

Protocol Type 802.1p
802.1p Tag 5

* The value zero (0) indicates the feature is disabled

Maximum Priority is the maximum marking which will be allowed from a WMM client. Unicast Default Priority is the default marking of non-WMM client traffic. Multicast Default Priority is for multicast traffic.

It should be noted that these settings apply primarily to Local Mode (centralized wireless controller) designs and FlexConnect designs with central termination of traffic, since the WLAN QoS Parameters field results in the mapping of the 802.11 User Priority to the DSCP value within the outer header of the CAPWAP tunnel.

The original DSCP marking of the packet sent by the wireless client is always preserved and applied as the packet is placed onto the Ethernet segment, whether that is at the wireless controller for centralized wireless controller designs or at the access point for FlexConnect designs with local termination.

The wireless trust boundary is established via the configuration of the WMM Policy within the QoS tab of the WLAN configuration. An example was shown in Figure 7-1. The three possible settings for WMM Policy are:

- Disabled—The access point will not allow the use of QoS headers within 802.11 packets from WMM-enabled wireless clients on the WLAN.
- Allowed—The access point will allow the use of QoS headers within 802.11 packets from wireless clients on the WLAN. However the access point will still allow non-WMM wireless clients (which do not include QoS headers) to associate to the access point for that particular WLAN.
- Required—The access point requires the use of QoS headers within 802.11 packets from wireless clients on the WLAN. Hence, any non-WMM-enabled clients (which do not include QoS headers) will not be allowed to associate to the access point for that particular WLAN.

Note Where possible, it is advisable to configure WMM policy to Required. Some mobile devices may incorrectly mark traffic from collaboration applications when the WMM policy is set to Allowed versus Required. Note however that this requires all devices on the WLAN to support WMM before being allowed onto the WLAN. Before changing the WMM policy to Required, the network administrator should verify that all devices which utilize the WLAN are WMM-enabled. Otherwise, non-WMM-enabled devices will not be able to access the WLAN.

The configuration of the WMM Policy, along with the WLAN QoS Parameters, together create the wireless QoS trust boundary and determine the marking of wireless traffic within the CAPWAP tunnel as it traverses the network infrastructure.

Note The Cisco CT5760 wireless controller and the Catalyst 3850 Series switch both run IOS XE software. QoS configuration uses the Modular QoS based CLI (MQC) which is in alignment other platforms such as Catalyst 4500E Series switches. This version of the design guide does not address QoS on the Cisco CT5760 wireless controller and Catalyst 3850 Series switch. Future versions may address QoS on these platforms.

Rate Limiting

One additional option to prevent the wireless medium from becoming saturated, causing excessive latency and loss of traffic, is rate limiting. Rate limiting may be implemented per device or per SSID to prevent individual devices from using too much bandwidth and negatively impacting other devices and applications. Rate limiting is particularly useful for guest access implementations and is discussed in detail in Chapter 21, “BYOD Guest Wireless Access.”

Application Visibility and Control (AVC)

Beginning with Cisco Unified Wireless Network (CUWN) software release 7.4, the Application Visibility and Control set of features—already supported on Cisco routing platforms such as ASR 1000s and ISR G2s—became available on WLC platforms, including the Cisco 2500, 5500, 7500, 8500 WLCs, and WiSM2 controllers on Local and FlexConnect Modes (for WLANs configured for central switching only in 7.4 release).

The AVC feature set increases the efficiency, productivity, and manageability of the wireless network. Additionally, the support of AVC embedded within the WLAN infrastructure extends Cisco’s application-based QoS solutions end-to-end.

Business use-cases for AVC policies include:

- Guaranteeing voice quality from wireless applications meets enterprise VoIP requirements.
- Ensuring video applications—both interactive and streaming—are delivered to/from wireless devices with a high Quality of Experience, so that users can communicate and collaborate more efficiently and effectively-regardless of their location or device.
- Provisioning preferred services for business-critical applications running on wireless devices, such as Virtual Desktop applications, sales applications, customer relationship management (CRM) applications, and enterprise resource planning (ERP) applications, etc.

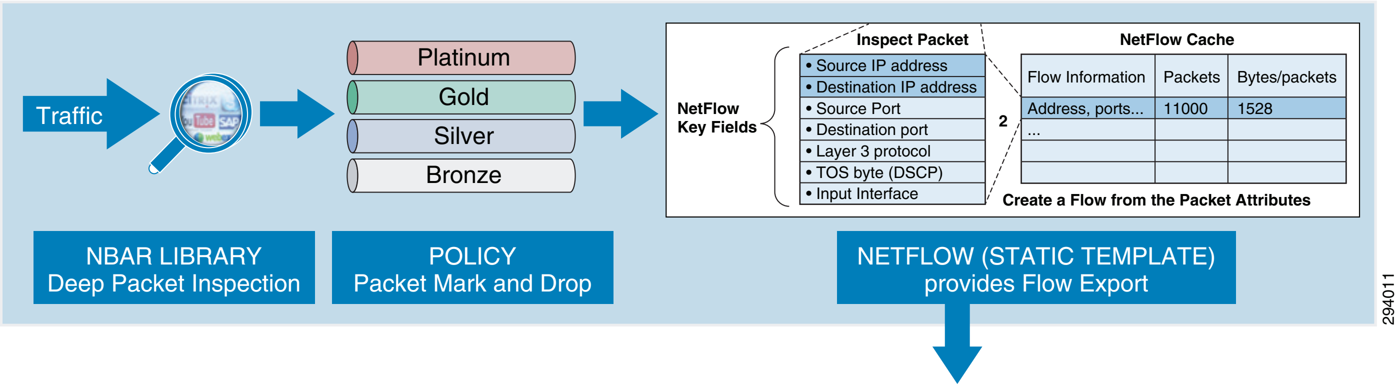
- De-prioritizing "background" application traffic (i.e., applications that send data to/from servers, rather than directly to other users and which do not directly impact user-productivity), such as email, file-transfers, content distribution, backup operations, software updates, etc.
- Identifying and de-prioritizing (or dropping) non-business applications, which can include social networking applications, peer-to-peer file-sharing applications, and type of entertainment and/or gaming applications so that network resources are always available for business-oriented applications.

AVC includes these components:

- Next-generation Deep Packet Inspection (DPI) technology called Network Based Application Recognition (NBAR2), which allows for identification and classification of applications. NBAR is a deep-packet inspection technology available on Cisco IOS based platforms, which includes support of stateful L4-L7 classification.
- QoS—Ability to remark applications using DiffServ, which can then be leveraged to prioritize or de-prioritize applications over both the wired and wireless networks.
- A template for Cisco NetFlow v9 to select and export data of interest to Cisco Prime or a third-party NetFlow collector to collect, analyze, and save reports for troubleshooting, capacity planning, and compliance purposes.

These AVC components are shown in Figure 7-3.

Figure 7-3 Cisco AVC Components



Flow Information	Packets	Bytes/packets
Address, ports...	11000	1528
...		

AVC on the WLC inherits NBAR2 from Cisco IOS that provides deep packet inspection technology to classify stateful L4-L7 application classification. This is critical technology for application management, as it is no longer a straightforward matter of configuring an access list based on the TCP or UDP port number(s) to positively identify an application. In fact, as applications have matured—particularly over the past decade—an ever increasing number of applications have become opaque to such identification. For example, HTTP protocol (TCP port 80) can carry thousands of potential applications within it and in today's networks seems to function more as a transport protocol rather than as the OSI application-layer protocol that it was originally designed as. Therefore to identify applications accurately, Deep Packet Inspection technologies—such as NBAR2—are critical.

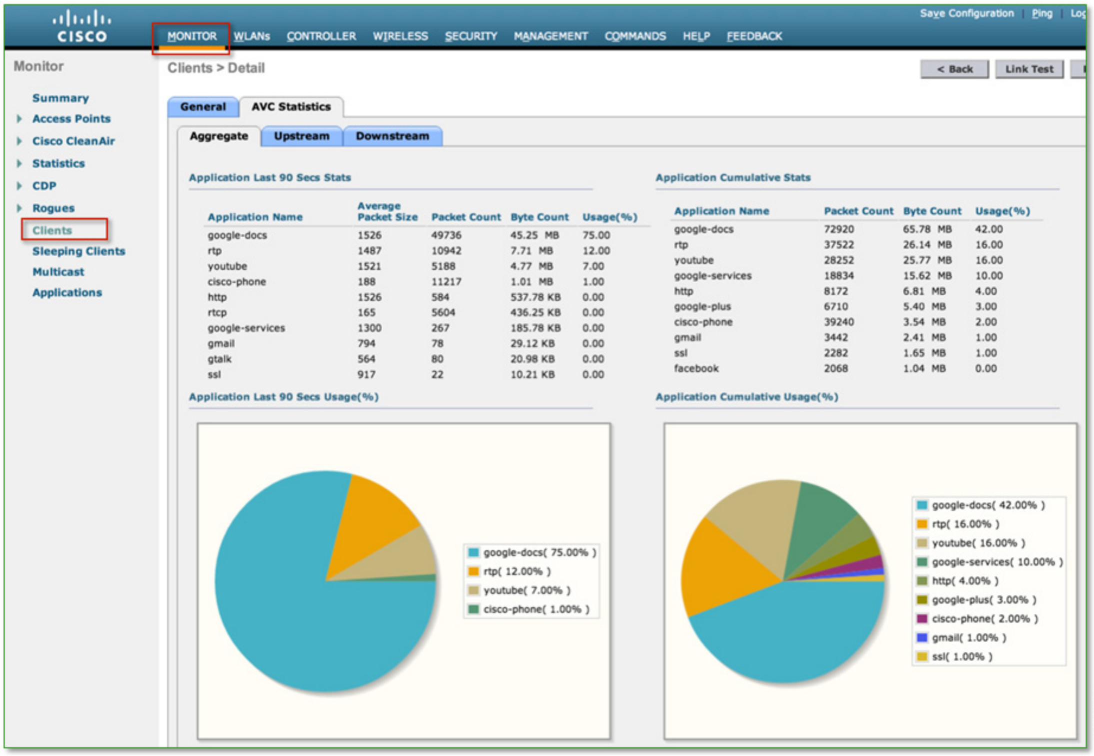
Once applications are recognized by the NBAR engine by their discrete protocol signatures, it registers this information in a Common Flow Table so that other WLC features can leverage this classification result. Such features include Quality of Service (QoS), NetFlow, and firewall features, all of which can take action based on this detailed classification.

Thus AVC provides:

- Application Visibility on the Cisco WLC by enabling Application Visibility for any WLAN configured. Once Application Visibility is turned on, the NBAR engine classifies applications on that particular WLAN. Application Visibility on the WLC can be viewed at an overall network level, per WLAN, or per client. An example of a per-client application visibility report is illustrated in Figure 7-4.
- Application Control on the Cisco WLC by creating an AVC profile (or policy) and attaching it to a WLAN. The AVC Profile supports QoS rules per application and provides the following actions to be taken on each classified application: Mark (with DSCP), Permit (and transmit unchanged), or Drop. An example of an AVC profile is shown in Figure 7-5, Figure 7-6, and Figure 7-7.

A client-based AVC report—such as shown in Figure 7-4—can show the top applications by device. AVC reports can also be compiled by WLAN or at the overall network level.

Figure 7-4 Cisco AVC Application Visibility Reports



Clients > Detail

Application Last 90 Secs Stats

Application Name	Average Packet Size	Packet Count	Byte Count	Usage(%)
google-docs	1526	49736	45.25 MB	75.00
rtp	1487	10942	7.71 MB	12.00
youtube	1521	5188	4.77 MB	7.00
cisco-phone	188	11217	1.01 MB	1.00
http	1526	584	537.78 KB	0.00
rtcp	165	5604	436.25 KB	0.00
google-services	1300	267	185.78 KB	0.00
gmail	794	78	29.12 KB	0.00
gtalk	564	80	20.98 KB	0.00
ssl	917	22	10.21 KB	0.00

Application Cumulative Stats

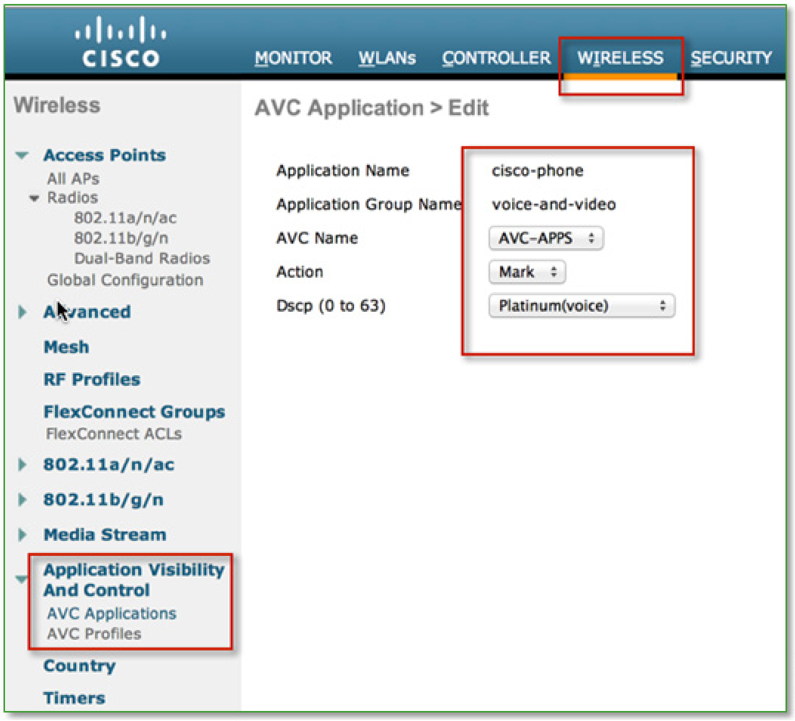
Application Name	Packet Count	Byte Count	Usage(%)
google-docs	72920	65.78 MB	42.00
rtp	37522	26.14 MB	16.00
youtube	28252	25.77 MB	16.00
google-services	18834	15.62 MB	10.00
http	8172	6.81 MB	4.00
google-plus	6710	5.40 MB	3.00
cisco-phone	39240	3.54 MB	2.00
gmail	3442	2.41 MB	1.00
ssl	2282	1.65 MB	1.00
facebook	2068	1.04 MB	0.00

Application Last 90 Secs Usage(%)

Application Cumulative Usage(%)

An AVC profile—a collection of individual application policy rules—can be configured via the WLC GUI or CLI. In Figure 7-5 an AVC application rule is being configured for voice traffic sourced-from or destined-to Cisco wireless devices. This traffic is identified via an NBAR2 signature named **cisco-phone** and is marked as DSCP 46 (EF) and assigned to the Platinum Wireless Multi-Media (WMM) access-category for the highest level of service over the air.

Figure 7-5 Cisco AVC Profile Example 1—Creating an AVC Policy Rule



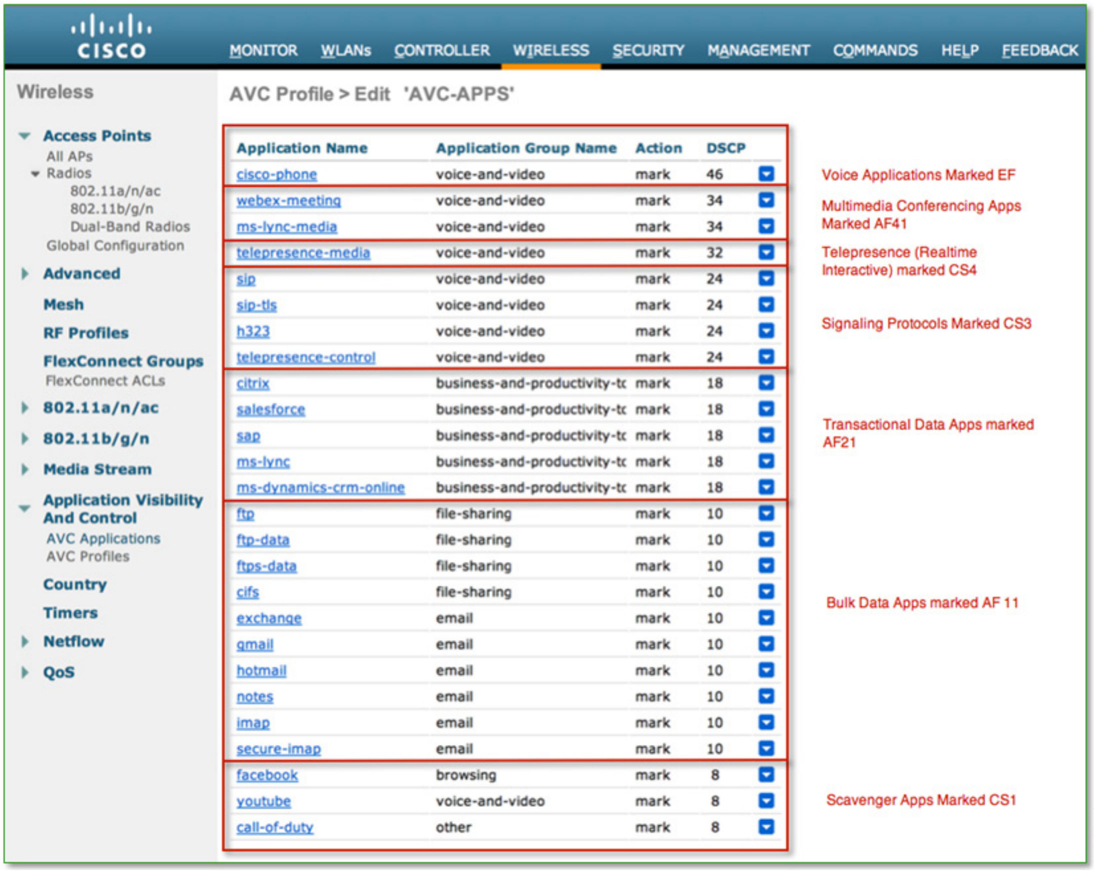
AVC Application > Edit

Application Name	cisco-phone
Application Group Name	voice-and-video
AVC Name	AVC-APPS
Action	Mark
Dscp (0 to 63)	Platinum(voice)

An AVC profile can contain up to 32 individual application rules, as is shown in Figure 7-6, containing recommended policies for the following classes of application traffic (as based on RFC 4594):

- Voice
- Video
- Multimedia Conferencing
- Multimedia Streaming
- Transactional Data
- Bulk Data
- Scavenger applications

Figure 7-6 Cisco AVC Profile Example 2—Displaying a Comprehensive AVC Policy



AVC Profile > Edit 'AVC-APPS'

Application Name	Application Group Name	Action	DSCP
cisco-phone	voice-and-video	mark	46
webex-meeting	voice-and-video	mark	34
ms-lync-media	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
citrix	business-and-productivity-tc	mark	18
salesforce	business-and-productivity-tc	mark	18
sap	business-and-productivity-tc	mark	18
ms-lync	business-and-productivity-tc	mark	18
ms-dynamics-crm-online	business-and-productivity-tc	mark	18
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
gmail	email	mark	10
hotmail	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
call-of-duty	other	mark	8

Voice Applications Marked EF

Multimedia Conferencing Apps Marked AF41

Telepresence (Realtime Interactive) marked CS4

Signaling Protocols Marked CS3

Transactional Data Apps marked AF21

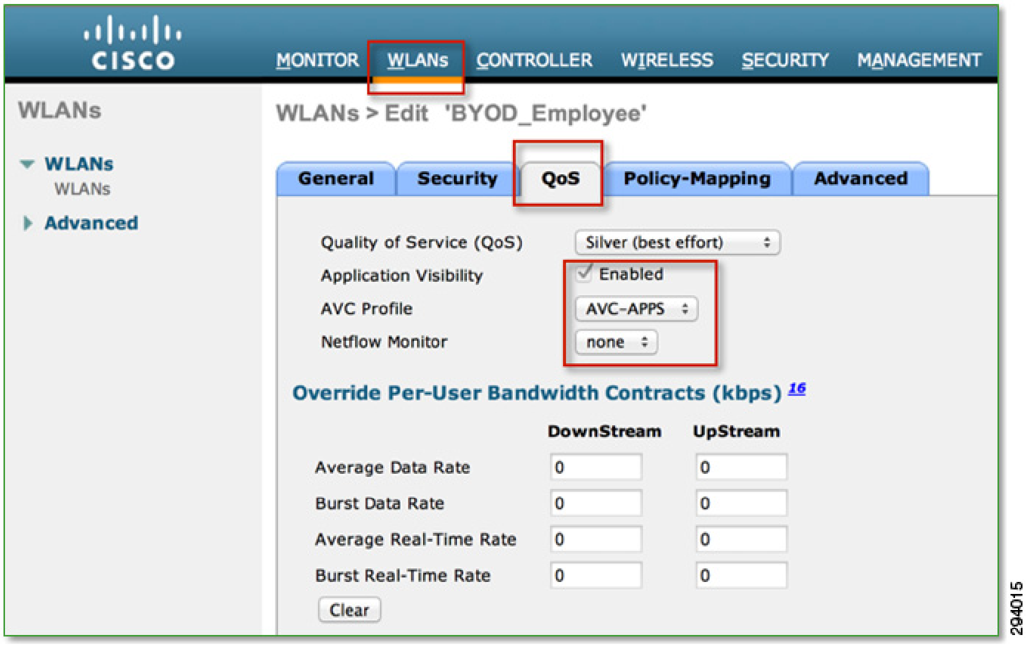
Bulk Data Apps marked AF 11

Scavenger Apps Marked CS1

294014

Once an AVC profile has been assembled, it can be applied to a WLAN(s), as shown in Figure 7-7. AVC policies are applied bi-directionally—that is, in the upstream and downstream directions simultaneously.

Figure 7-7 Cisco AVC Profile Example 3—Applying an AVC Profile to a WLAN



WLANs > Edit 'BYOD_Employee'

Quality of Service (QoS)	Silver (best effort)
Application Visibility	✓ Enabled
AVC Profile	AVC-APPS
Netflow Monitor	none

Override Per-User Bandwidth Contracts (kbps) 16

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

AVC supports over 1000 applications in its initial release for WLCs. Some of these applications-grouped by business case-are:

To ensure voice quality for wireless devices, the **cisco-phone** application would typically be assigned to the Platinum (Voice) WMM access category via AVC. However, additional VoIP applications may include:

- **aol-messenger-audio**
- **audio-over-http**
- **fring-voip**
- **gtalk-voip**
- **yahoo-voip-messenger**
- **yahoo-voip-over-sip**

Similarly, to protect video and multimedia applications, the following applications might be assigned to the Gold (Video) WMM access-category via AVC:

- **cisco-ip-camera**
- **telepresence-media**
- **webex-meeting**
- **ms-lync-media**
- **aol-messenger-video**
- **fring-video**
- **gtalk-video**
- **livemeeting**
- **msn-messenger-video**
- **rhapsody**

- **skype**
- **video-over-http**

Note It may be that some of these video conferencing applications may be considered non-business in nature (such as Skype and gtalk-video), in which case these may be provisioned into the Bronze (Background) WMM access category.

To deploy AVC policies to protect the signaling protocols relating to these voice and video applications, the following applications might be marked to the Call-Signaling marking of CS3 (DSCP 24) via AVC:

- **sip**
- **sip-tls**
- **skinny**
- **telepresence-control**
- **h323**
- **rtcp**

To deploy policies to protect business-critical applications, the following applications might be marked AF21 (DSCP 18) via AVC:

- **citrix**
- **ms-lync**
- **ms-dynamics-crm-online**
- **salesforce**
- **sap**
- **oraclenames**
- **perforce**
- **phonebook**
- **semantix**
- **synergy**

On the other hand, some business applications would be best serviced in the background by assigning these to the Bronze (Background) WMM access category via AVC:

- **ftp/ftp-data/ftps-data**
- **cifs**
- **exchange**
- **notes**
- **smtp**
- **imap/secure imap**
- **pop3/secure pop3**
- **gmail**
- **hotmail**
- **yahoo-mail**

And finally, many non-business applications can be controlled by either being assigned to the Bronze (Background) WMM access category or dropped via AVC policies:

- **youtube**
- **netflix**
- **facebook**
- **twitter**
- **bittorrent**
- **hulu**
- **itunes**
- **picasa**
- **call-of-duty**
- **doom**
- **directplay8**

Note It is important to note that these are only example applications and do not represent an exhaustive list of applications by class. With over a thousand applications to choose from, these lists are simplified for the sake of brevity and serve only to illustrate AVC policy options and concepts.

For comprehensive design guidance on using the AVC feature for WLCs, see: Chapter 24, "Mobile Traffic Engineering with Application Visibility and Control (AVC)."

Cisco Jabber

Cisco's Jabber clients are unified communications (UC) applications that are available for Android and Apple mobile devices as well as Microsoft Windows and Apple Mac computers. These client applications provide instant messaging (IM), presence, voice, video, and visual voicemail features. These features require that the employee-owned device is allowed to establish call signaling flows between the device itself and the corporate Cisco Unified Communications Manager (Unified CM) server, typically deployed within the campus data center. Note that the Basic Access use case discussed above terminates employee-owned devices on a DMZ segment off of the Internet Edge firewall. Cisco Jabber requires only Internet access to access WebEx cloud-based services like IM, meetings, and point-to-point voice and video calls. However, to deliver these same services with on-premise corporate assets such as Unified CM and other back-end UC applications, connectivity through the firewall is required for Jabber features to function. In addition to signaling, media flows also need to be allowed between the Jabber client and other IP voice and video endpoints, such as corporate IP phones deployed throughout the corporate network. This requires the network administrator to allow a range of addresses and ports inbound from the DMZ segment through the Internet Edge firewall. Given these connectivity considerations for real time communications and collaboration, the network administrator may instead decide to implement the Enhanced Access use case discussed above. With this BYOD model, the employee-owned devices are on-boarded (registered with the Cisco ISE server and provisioned with digital certificates) and terminated on the inside of the corporate network. This requires no modifications to the Internet Edge firewall, and potentially fewer security concerns.

Cisco Jabber Clients and the Cisco BYOD Infrastructure

Cisco Jabber, a Cisco mobile client application, provides core Unified Communications and collaboration capabilities, including voice, video, and instant messaging to users of mobile devices such as Android and Apple iOS smartphones and tablets. When a Cisco Jabber client device is attached to the corporate wireless LAN, the client can be deployed within the Cisco Bring Your Own Device (BYOD) infrastructure.

Because Cisco Jabber clients rely on enterprise wireless LAN connectivity or remote secure attachment through VPN, they can be deployed within the Cisco Unified Access network and can utilize the identification, security, and policy features and functions delivered by the BYOD infrastructure.

The Cisco BYOD infrastructure provides a range of access use cases or scenarios to address various device ownership and access requirements. The following high-level access use case models should be considered:

- Enhanced Access—This comprehensive use case provides network access for corporate, personal, and contractor/partner devices. It allows a business to build a policy that enables granular role-based application access and extends the security framework on and off-premises.
- Advanced Access —This use case introduces MDM integration with Enhanced Access.
- Limited Access—Enables access exclusively to corporate issued devices.
- Basic Access—This use case is an extension of traditional wireless guest access. It represents an alternative where the business policy is to not on-board/register employee wireless personal devices, but still provides Internet-only or partial access to the network.

Use Case Impact on Jabber

The Enhanced use case allows the simplest path for implementing a Cisco Jabber solution. Cisco Jabber clients, whether running on corporate or personal devices, require access to numerous back-end, on-premise enterprise application components for full functionality. The Enhanced Access use case will allow access from corporate devices with the option of allowing access from personal devices for Jabber back-end applications.

The Limited Access use case will allow Jabber use only from corporate devices.

Basic Access adds a significant layer of complexity for personal devices, requiring them to have access to back-end on-premise Jabber applications from the DMZ. Various signal, control, and media paths must be allowed through the firewall for full functionality.

In the case of cloud-based collaboration services, Cisco mobile clients and devices connect directly to the cloud through the Internet without the need for VPN or full enterprise network attachment. In these scenarios, user and mobile devices can be deployed using the Basic Access model because these use cases require only Internet access.

Other Jabber Design Considerations

When deploying Cisco Jabber clients within the Cisco BYOD infrastructure, consider the following high-level design and deployment guidelines:

- The network administrator should strongly consider allowing voice- and video-capable clients to attach to the enterprise network in the background (after initial provisioning), without user intervention, to ensure maximum use of the enterprises telephony infrastructure. Specifically, use of certificate-based identity and authentication helps facilitate an excellent user experience by minimizing network connection and authentication delay.
- In scenarios where Cisco Jabber clients are able to connect remotely to the enterprise network through a secure VPN:
  - The network administrator should weigh the corporate security policy against the need for seamless secure connectivity without user intervention to maximize utilization of the enterprise telephony infrastructure. The use of certificate-based authentication and enforcement of a device PIN lock policy provides seamless attachment without user intervention and functionality similar to two-factor authentication because the end user must possess the device and know the PIN lock to access the network. If two-factor authentication is mandated, then user intervention will be required in order for the device to attach remotely to the enterprise.
  - It is important for the infrastructure firewall configuration to allow all required client application network traffic to access the enterprise network. Failure to open access to appropriate ports and protocols at the corporate firewall could result in an inability of Cisco Jabber clients to register to on-premises Cisco call control for voice and video telephony services and/or the loss of other client features such as enterprise directory access or enterprise visual voicemail.
- When enterprise collaboration applications such as Cisco Jabber are installed on employee-owned mobile devices, if the enterprise security policy requires the device to be wiped or reset to factory default settings under certain conditions, device owners should be made aware of the policy and encouraged to backup personal data from their device regularly.
- When deploying Cisco Jabber, it is important for the underlying network infrastructure to support, end-to-end , the necessary QoS classes of service, including priority queuing for voice media and dedicated video and signaling bandwidth, to ensure the quality of client application voice and video calls and appropriate behavior of all features.

For further information regarding Cisco Jabber clients, see the product collateral and documentation at: http://www.cisco.com/go/jabber.

For further information regarding Cisco Mobile Unified Communications, see the Cisco Unified Communications System 9.X SRND at: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/9x/mobilapp.html.

Cisco Virtual Workspace (VXI) Smart Solution

The Cisco Virtual Workspace (VXI) Smart Solution provides an optimized end-to-end infrastructure for desktop virtualization deployments.

Cisco Virtual Workspace (VXI) Architecture

The Cisco Virtual Workspace (VXI) architecture consists of three fundamental building blocks: Cisco Virtualized Data Center, Virtualization-Aware Network, and Virtualized Collaborative Workspace.

Cisco's Virtualized Data Center provides the computing, switching, storage, and virtualization capabilities needed to support a hosted virtual desktop solution from Citrix.

Cisco's Virtualization-Aware Network connects data centers, enterprise campuses, branch offices, and remote workers to help ensure that traffic flowing between end users and their hosted desktops is transported securely, reliably, and efficiently. Virtualization-Aware Networks employ bandwidth optimization, load balancing, quality of service (QoS), security, and other technologies from Cisco's industry-leading portfolio.

Cisco's Virtualized Collaborative Workspace builds on the Cisco Collaboration architecture, extending the reach of the virtual desktop to a wide range of endpoints while supporting critical collaboration capabilities hosted in the data center. Endpoints can be zero clients, thin clients, mobile devices, or thick clients.

Cisco Virtual Workspace (VXI) Smart Solution also supports management tools for both Cisco and ecosystem partner products, as well as a rich services portfolio that helps enterprises make the most of their virtualization investments.

Cisco Virtual Workspace (VXI) Application Virtualization and Citrix

This Cisco Virtual Workspace (VXI) Smart Solution validated design is based on Citrix XenDesktop and XenApp virtualization solutions.

Citrix XenDesktop is a desktop virtualization solution that delivers Windows desktops as an on-demand service to users on any device, anytime, with a high definition user experience.

Citrix XenApp, which is included as part of the XenDesktop license, is an on-demand application delivery solution that enables Windows applications to be virtualized, centralized, and instantly delivered as a service to users anywhere on any device.

For more information about the Cisco Virtual Workspace with Citrix, refer to the Cisco Virtual Workspace (VXI) Smart Solution CVDs at:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns1100/landing_vxi.html.

License Requirements for BYOD Solution

Cisco ISE comes with several license options, such as Evaluation, Base, Advanced, and Wireless. For this design to be implemented, ISE requires the Advanced license option. To obtain more information on licensing, see:
http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html.