Microsoft Lync Client/Server in a Cisco Wireless LAN

Revised: September 9, 2016,

Microsoft Lync Client/Server in a Cisco Wireless LAN

Scope

Using Cisco Application Visibility and Control (AVC) technology, Cisco WLAN infrastructure and routers accurately classify and prioritize thousands of applications, including commonly deployed business applications such as Cisco Jabber, Cisco WebEx, Microsoft Office 365, Microsoft Lync 2013, and Skype. These business applications are supported with AVC protocol pack 6.4 and above, operating with next-generation Network-Based Application Recognition (NBAR2) engine 13 and above. With this capability, you can identify Lync version 2013 and also sub-classify how much of your traffic is data (desktop share), audio, video, and apply different policies on those. Cisco has also passed Microsoft's Lync certification testing for quality voice-over-wireless-LAN (VoWLAN) performance. This white paper provides Cisco network design considerations for Microsoft's Lync client and Lync server when functioning over a Cisco wireless LAN (WLAN) infrastructure. It also provides the steps for WLAN configuration and best practices for quality of service (QoS).

Background

Microsoft and Cisco have a history of collaboration in the development of Wi-Fi security and QoS. Cisco Unified Communications Manager (UCM) already supports Microsoft softphone clients and Microsoft call management servers. In continuation to this support, the Microsoft Lync client can register directly to UCM. The documents supporting overall network design, including security, QoS,

Session Initiation Protocol (SIP) Trunks, and collaboration services, are listed in the For More Information, on page 17 section. This document focuses on a Wi-Fi design that best provides high-quality calls for the users of the Microsoft Lync client with Lync server.

Figure 1: Cisco UC Integration for Microsoft Lync

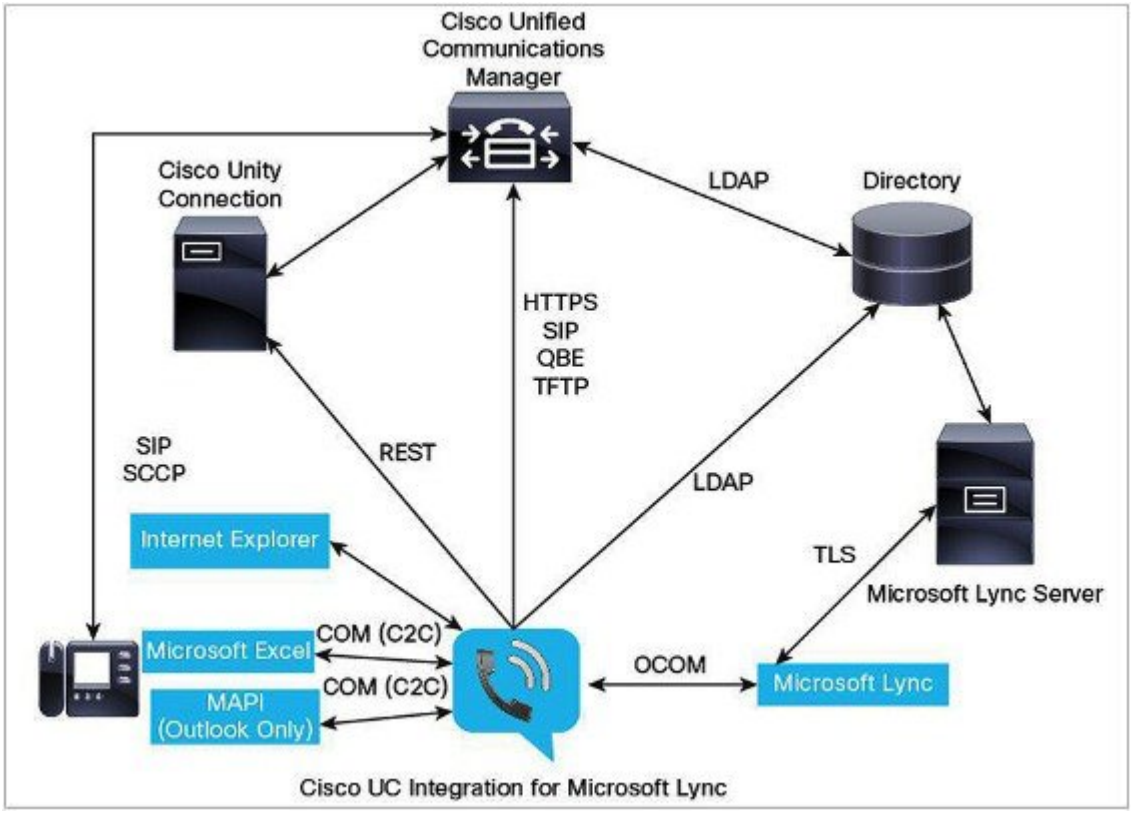


Figure 1: Cisco UC Integration for Microsoft Lync, on page 3 is included in the *Administration Guide for Cisco Unified Communications (UC) Integration for Microsoft Lync*. This is an example of an installation that includes both Cisco Unified Communications Manager and Microsoft Lync Call Manager. The Cisco Unified Wireless Network (UWN) WLAN technologies are compatible with this type of architecture or an architecture that is absent of the integration of the two call managers. UWN technology supports multiple communication managers and multiple wireless LAN controller (WLC) platforms in the same infrastructure. When operating in a large deployment with multiple controllers, the WLC-to-WLC connection options support Layer 2 and Layer 3 Wi-Fi client roaming without call disruption. WLC hardware options provide access point connections from five access points on a single branch office WLC to 6000 access points on a single large enterprise WLC.

Quality of Service Configuration

Wired and Wireless QoS

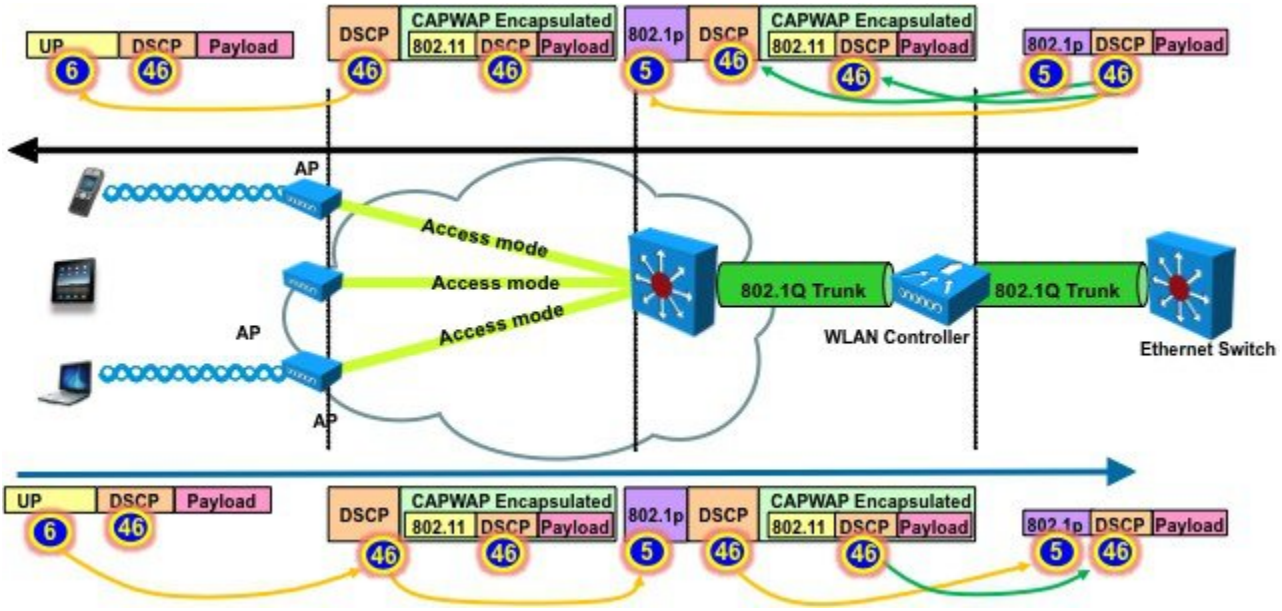
Ethernet and Wi-Fi share the concept of frame prioritization. Configuration options provide a means to maintain a packet's priority across the wireless network. Wireless Wi-Fi traffic is identified by a service set identifier (SSID). Wi-Fi traffic can also display a prioritization value, expressed through a User Priority (UP) tag present in the 802.11 header and defined by the 802.11e amendment in 2005. This tag can receive any value from 0 to 7. Traffic with higher UP receive a more expedited treatment. The Wi-Fi Alliance ensured compatibility between vendors applying 802.11 QoS marking and prioritization through the Wi-Fi Multimedia (WMM)

certification. The SSID configuration on the WLC defines the highest priority on which traffic will be forwarded and what VLAN will be mapped to what WLAN.

WLAN data in a unified wireless network is tunneled between the AP and the WLAN controller via CAPWAP . To maintain, over the wired network, the QoS classification that is applied to WLAN frames, a process of mapping classifications to and from wired QoS marking and Wi-Fi QoS marking is required.

For example, when prioritized traffic is sent by a WLAN client, it has an IEEE 802.11 User Priority marking in the header. The AP needs to translate this classification into a DSCP value for the wired CAPWAP packet carrying the frame to ensure that the packet is treated with the appropriate priority on its way to the WLC. A similar process needs to occur on the WLC for CAPWAP packets going to the AP.

Figure 2: Traffic Classification Flow for a WMM client, an AP, and a WLC



A mechanism to classify traffic from non-WMM clients is also required, so that their CAPWAP packets can also be given an appropriate QoS classification by the AP and the WLC.

Different vendors may use different translation mechanisms and values between Wi-Fi QoS marking and Wired QoS marking. For example, Microsoft does not differentiate between Wired and Wi-Fi networks, and uses a conversion map based on IP Precedence rather than DSCP. As a result, voice traffic is commonly affected DSCP 40 (IP Precedence 5) and 802.1p or 802.11e 5. In contrast, Cisco uses the DSCP values (and does not limit marking to IP Precedence), follows the IETF recommendations (for example RFC 3246) and the 802.11e mapping. As a result, Cisco recommends using DSCP 46 for voice traffic, which translates into 802.1p 5, but to 802.11e 6. The following table summarizes the applied marking for the main categories of traffic.

Table 1: QoS Layer 2 to Layer 3 Mapping Table

Cisco 802.1p User Priority Traffic Type	Cisco IP DSCP	IEEE 802.11e/WMM User Priority
Reserved (Network Control)	56 (CS7)	7 (unused)
Reserved (CAPWAP)	48 (CS6)	— (unused)
Voice	46 (EF)	6

Cisco 802.1p User Priority Traffic Type	Cisco IP DSCP	IEEE 802.11e/WMM User Priority
Video	34 (AF41)	5
Voice Control (Signaling)	24 (CS3)	4
Background (Transactional/Interactive Data)	18, 20, 22 (AF2x)	3
Background (Bulk Data)	10, 12, 14 (AF1x)	2
Best Effort	0 (BE)	0
Background	2, 4, 6	1
Unknown DSCP from Wired	D	D >> 3

WLAN QoS

WLAN QoS is the result of joint effort between Microsoft, Cisco, and IEEE to bring QoS to Wi-Fi channels. The IEEE ratified the Wi-Fi QoS specification, 802.11e, in 2005, which was updated in 2012. The Wi-Fi Alliance certifies access point and client QoS interoperability with a subset of the 802.11e specification known as Wi-Fi Multi-Media (WMM). WMM was also the result of the Microsoft QoS effort. All Wi-Fi data traffic with QoS capabilities has a WMM QoS priority field in the Wi-Fi packet header. Access points advertise their QoS capabilities in the same manner as they advertise their security capabilities, that is by Wi-Fi beacons and probe response frames. The QoS parameters for an SSID are contained in information elements of those frames. The QoS information elements are identified by the Microsoft OID value “00:50:F2”.

You can assign to each SSID a QoS profile. This profile determines the highest QoS level expected and allowed to transit to and from this SSID. The profile also determines what marking behavior should be used for incoming unmarked traffic, and for multicast traffic. When incoming traffic exceeds the maximum QoS value of the profile, the traffic is remarked to match the maximum QoS value assigned to the profile. The available profiles are Platinum, Gold, Silver, and Bronze.

Platinum is adapted to all traffic including real time Voice traffic. The maximum expected QoS level for this profile is DSCP 46, and UP 6.

Gold is adapted to all traffic including real time video traffic, but is not intended for real time voice traffic. The maximum expected QoS level for this profile is DSCP 34, and UP 5.

Silver is adapted to all transactional and data traffic, but is not intended for real time applications such as real time voice or real time video. The maximum expected QoS level for this profile is DSCP 18, and UP 3.

Bronze is adapted to background traffic. The maximum expected QoS level for this profile is DSCP 10, and UP 1.

Microsoft Lync includes services ranging from file transfer and application sharing to real audio and video communications. Real time audio communication traffic is very sensitive to delays and losses, and is typically assigned a higher priority than other traffic. As a result, the Wi-Fi WLAN QoS level recommended for Lync clients is a QoS level of Platinum. The Platinum QoS priority level allows forwarding of all prioritized traffic up to the Voice category.

The recommended WMM setting is **Required**. This keeps non-WMM clients from connecting to the SSID. WMM/802.11e was ratified in 2005. Legacy clients such as handheld data transaction computers and old laptop computers can be allowed, but use lower level QoS. Smartphones, tablets, and devices that are 802.11n/ac are WMM compliant. Their applications may not be marking DSCP, and the operating system may not allow WMM QoS marking. But, the devices still use the WMM/802.11e header format when transmitting or receiving Wi-Fi packets. Various policies on the WLC can be established to define the handling of QoS markings at the WLC.

Cisco recommends that WMM and DSCP marking be enabled on the Wi-Fi devices. The network hop from the Wi-Fi endpoint device to the access point is the most important hop in the network for maintaining a user-acceptable mean opinion score (MOS) value. Once the Wi-Fi client's transactions are received at the access point, the QoS policies on the WLC can control the marking or dropping of the packets. The requirement to set DSCP is by using group policy.

Cisco's 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 into Wi-Fi networks. After the applications are recognized, the AVC feature enables you to either drop, mark, or rate-limit (by direction) the data traffic. Even if DSCP is already set, there is a value of AVC providing visibility to the traffic that it classifies. Using AVC, the controller 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.

The QoS Behavior with AVC between AP, WLC, and Infrastructure

Upstream

1. A frame is transmitted with or without inner packet DSCP from a wireless side (wireless client).
2. On the AireOS solution, the receiving access point translates the 802.11e UP value in the frame header into a DSCP value using the Table 1: QoS Layer 2 to Layer 3 Mapping Table, on page 4, and capping the value to the QoS profile used for the SSID. CAPWAP is used to encapsulate the 802.11 frame. The CAPWAP encapsulated packet is transmitted to the WLC. The outer CAPWAP header contains the DSCP value translated from the 802.11e UP value (and capped if necessary). The inner encapsulated packet contains the original DSCP value applied by the wireless client.
3. The WLC removes the CAPWAP header.
4. The AVC module on the WLC, which is optional, can be used to overwrite the original DSCP value of the source packet to the configured value in the AVC profile. The WLC then reads the QoS profile associated to the SSID, and caps the 802.1p value to the maximum allowed by the QoS profile, while the DSCP value stays uncapped. The WLC then forwards the source packet with its remarked DSCP value to the destination address.

Downstream

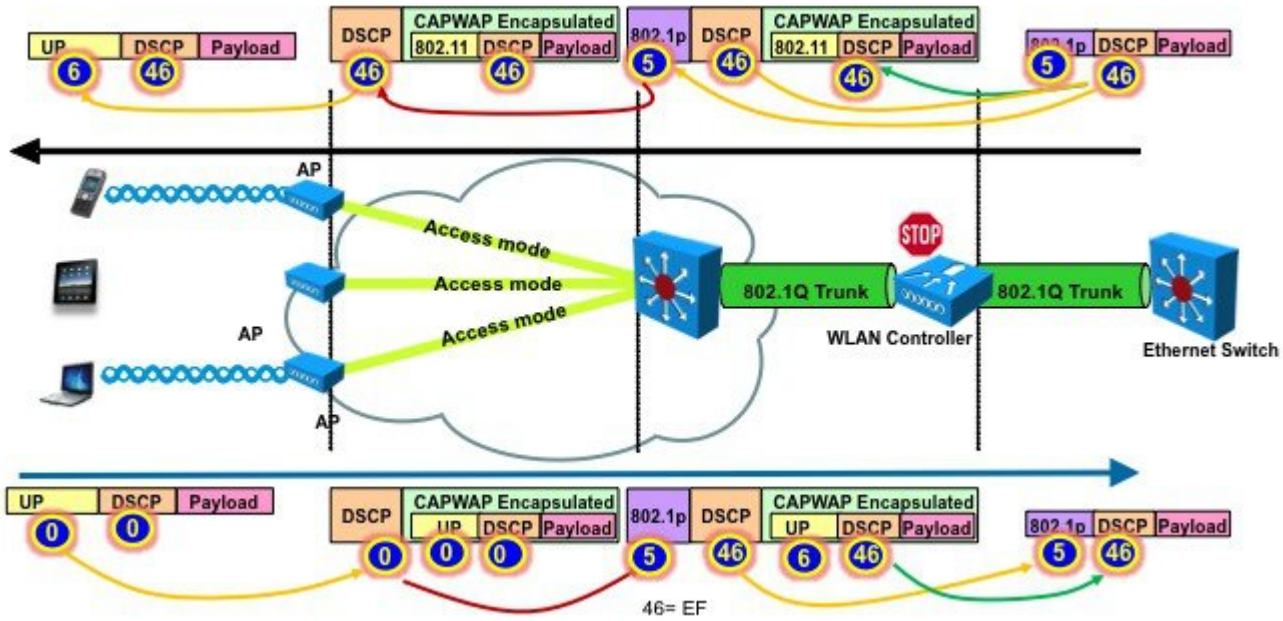
1. A packet comes from a switch with or without an inner-DSCP wired-side value.
2. The optional AVC module is used to overwrite the inner-DSCP value of the downstream source packet.
3. The WLC sends out the packet to the access point with QoS priority (CoS and DSCP) on the outer CAPWAP header. That value is no higher than the QoS priority configured on the WLAN.
4. The access point strips the CAPWAP header and sends the packet on air with a WMM UP value representative of the DSCP setting, or the WLAN configuration if the WLAN setting is lower. For more information, see the Table 1: QoS Layer 2 to Layer 3 Mapping Table, on page 4.

Note The WLAN QoS configuration sets the highest priority for which a packet in the WLAN may be forwarded. For example, a WLAN with a QoS priority of 'gold' will not forward audio packets at a voice priority. Those audio packets will be sent at a video packet priority.

AVC Classifying Lync Traffic

When Lync traffic reaches the wireless controller, the controller performs deep packet inspection to recognize the flow. If the flow is recognized as an application part of the AVC profile, the traffic is marked according to the AVC policy.

For example, when Lync voice traffic, which is unmarked reaches the wireless LAN controller, the NBAR engine on the WLC would recognize this traffic and mark the traffic according to the AVC profile. If the AVC profile was set to UP mark with DSCP value 46, the flows would be as in the following figure.



Cisco Switch Port Configuration for APs and WLCs

The QoS configuration of the switch port connecting the access point should trust the DSCP of the CAPWAP packets that are passed to it from the access point. There is no class-of-service (CoS) marking on the CAPWAP frames coming from the access point. The following is an example of the switchport configuration. Note that this configuration addresses only the classification and queuing commands that can be added depending on local QoS policy.

Note Check on the command requirement for various platforms, for example, MLS, MQC, and so on.

```
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
mls qos trust dscp
spanning-tree portfast
end
```

In trusting the access point DSCP values, the access switch trusts the policy set for that access point by the WLC. The maximum DSCP value assigned to client traffic is based on the QoS policy applied to the WLAN on that access point.

Recommended WLC Configuration for Lync Clients

Cisco recommends constant monitoring of Wi-Fi channel conditions to avoid interference, disruptions caused by rogue devices, and spectrum issues. The overall WLAN design should consider configuration of multicast direct as well as Wi-Fi call admission control for voice and video.

To provide an enterprise solution and a high-quality user experience for Lync users, Cisco recommends that the WLAN be created with the following options:

- WLAN QoS equal to platinum, which allows the clients to use any QoS tag/class:
  - Adding QoS service profiles when appropriate
  - Adding QoS service roles when appropriate
- WLAN band select to push clients to the 5 GHz band, where coverage design supports voice and VoWLAN
- WLAN 802.1x security:
  - Adding fast transition (11r) when appropriate to improve re-authentication roams
- 802.11k to provide access point neighbor lists based on client location for network-assisted roaming
- Disabled access point load balance
- Enabled channel scan at defaults
- Set WMM policy on the WLAN to **Allowed**. This permits a mix of QoS capable and non-QoS capable clients on the same WLAN

There are two methods of classifying and prioritizing MS Lync on the wireless network:

- Application Visibility and Control (AVC): AVC operates with NBAR2 engine and Deep Packet Inspection (DPI) to prioritize Lync traffic on a wireless network.
- Lync SDN API: This method requires a Lync SDN API running on a front end Lync server (On-Prem) to provide the WLC with Lync diagnostic data every time a Lync call is placed on the network. This method can be installed on Lync 2010 or Lync 2013 server.

Note The Lync SDN API takes precedence over AVC policies for QoS on the Cisco WLC.

Note Lync SDN feature not supported for Local switching scenario.

Feature	AVC	Lync SDN API
Classifying and prioritizing Lync audio and video flows independently	Yes	Yes
Classification of Lync desktop sharing and file transfer	No	Yes
Lync call quality records at the end of call	No	Yes
Advanced Lync troubleshooting with call statistics	No	Yes

Feature	AVC	Lync SDN API
Support for Office 365 (Lync Online)	Yes	No

Overview of the Suggested AVC Configuration for the Lync Application

Check the latest WLC configuration guide at http://www.cisco.com/c/en/us/support/wireless/5508-wireless-controller/model.html for commands on AVC configuration.

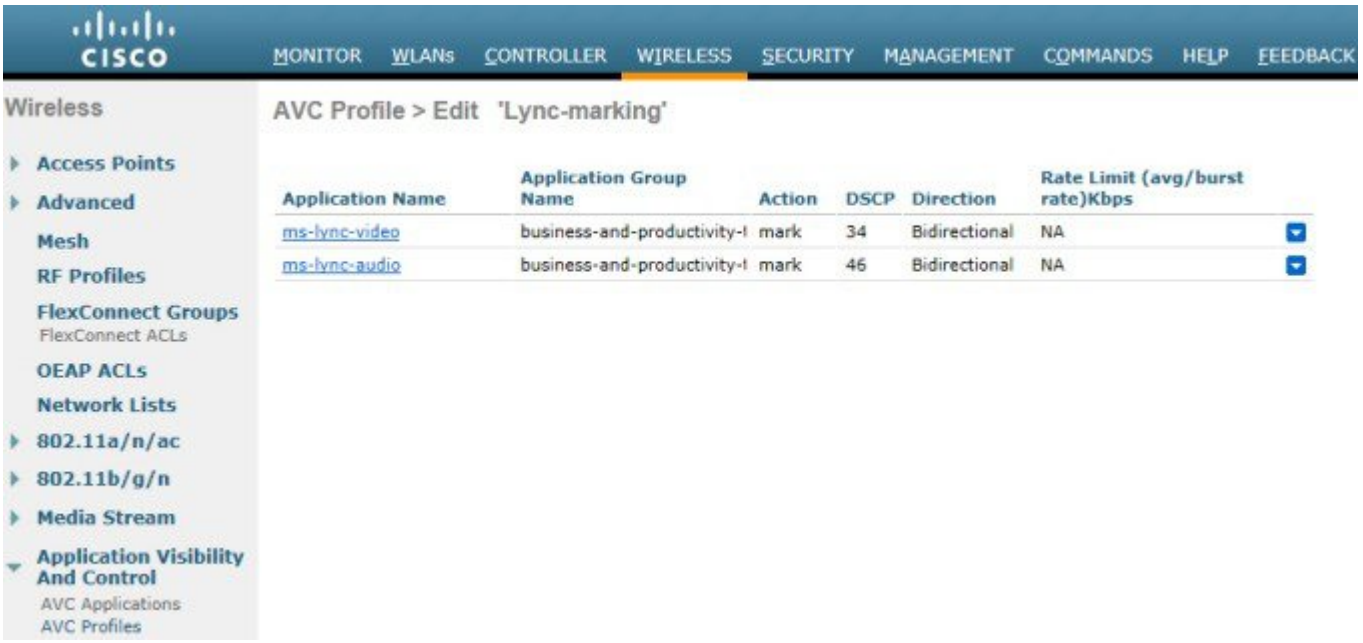
Recommended AVC Configuration for Lync Audio and Video

Microsoft Lync offers several types of services: File transfer, application sharing, SIP signaling, real time audio, and real time video communications. Microsoft commonly recommends DSCP 40 or 46 for real time voice, DSCP 34 for video, and 24 for the other services. This section focuses on configuring AVC for Lync audio and video. To configure AVC for Lync audio and video, perform the following steps:

Procedure

Step 1 Add a specific Lync application packet type for remarking the DSCP value for that packet type.

Step 2 Configure an AVC profile for use in a WLAN as shown in the following figure.



Step 3 The user created AVC profile name is **MS-Lync**.

Step 4 This sample profile uses three pre-defined application names (these are found in the AVC database) that fingerprint the secure Lync audio, video, and data packets.

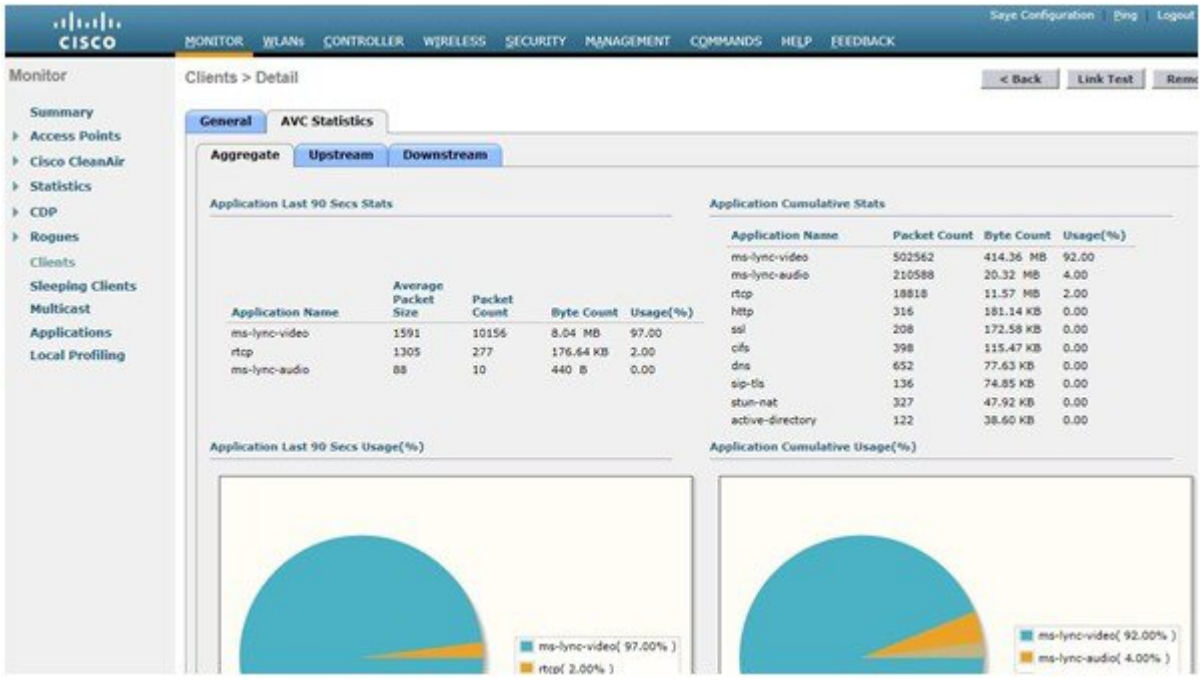
Step 5 Add as many applications as needed to the profile. This WLAN can also be used for Skype and the user would want those packets marked with a DSCP value of 20.

Step 6 In this sample profile AVC, remark the Lync audio packet to a DSCP value of 46, the video packets at 34, and the Lync data traffic at 0.

Step 7 The following figure shows that the user created WLAN is setup with Application Visibility **Enabled** and the AVC Profile of **MS-Lync** created in the previous step.

Step 8 Now the Lync traffic in this WLAN has its traffic remarked to the values in the profile.

Step 9 The following figure shows traffic of one Lync video call between two Wi-Fi endpoints.



Other Lync data types can also be included in a profile and then have their QoS priorities managed in a similar fashion as the examples for audio and video.

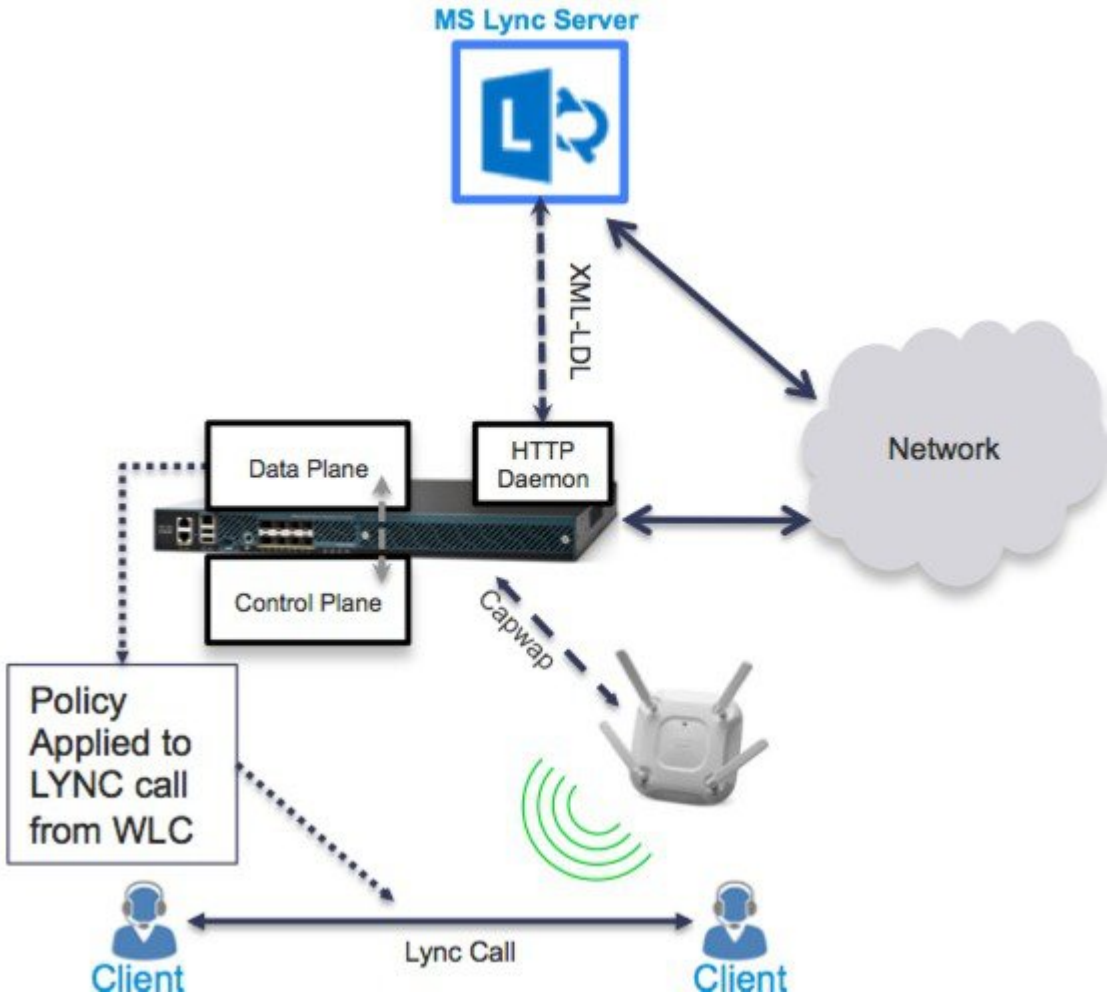
Lync SDN Introduction

The Lync SDN (Software-Defined Networking) API allows developers to build applications and services that can monitor, isolate, and correct issues on the network that affect Lync quality of experience. The installer application also provides customers with the ability to interface with the qualified third party applications (for example, Cisco wireless LAN controller) built on the Lync SDN API.

The Lync SDN API solution enables the following:

- Classify, manage, and report Lync traffic (including encrypted traffic) such as voice, video, desktop sharing, and file transfer.
- Automate QoS policy to control any given Lync call.

Lync SDN API solution



Lync SDN Configuration

You can configure Lync SDN API using both GUI and CLI. It is recommended to use the GUI wherever applicable, with CLI to supplement as reference.

Cisco WLC is compatible with Lync SDN API 2.0 only. The Lync SDN API software can be downloaded at: http://www.microsoft.com/en-us/download/details.aspx?id=39714.

For Microsft Lync SDN API documentation, including setup of Lync SDN Manager, Lync Dialog Listener, refer to the following documentation on Microsoft web page:

http://msdn.microsoft.com/en-us/library/office/dn439303(v=office.15).aspx
For integrating the Lync SDN API 2.0 with the Cisco WLC, the backward compatibility flag must be set to “true". You can do this by modifying the `SDNManager.exe.config` file as follows and restarting the SDN manager service.

```
   ...
   <errors switchValue="All" name="Logging Errors &amp; Warnings">
      <listeners>
        <add name="LNEAppLog"/>
      </listeners>
   </errors>
 </specialSources>
</loggingConfiguration>
<appSettings>
  <add key="submituri" value="http://WLC-ip:port"/>
  <add key="backwardcompatibility" value="true"/>
  ...
```

Procedure

Step 1 Configure Global Lync:

a) From WLC main menu, go to **WIRELESS > Lync Server**.

b) Check the **Lync Server** check box to enable it.

c) Assign a port number (15790) and protocol (http).

d) Click **Apply**.

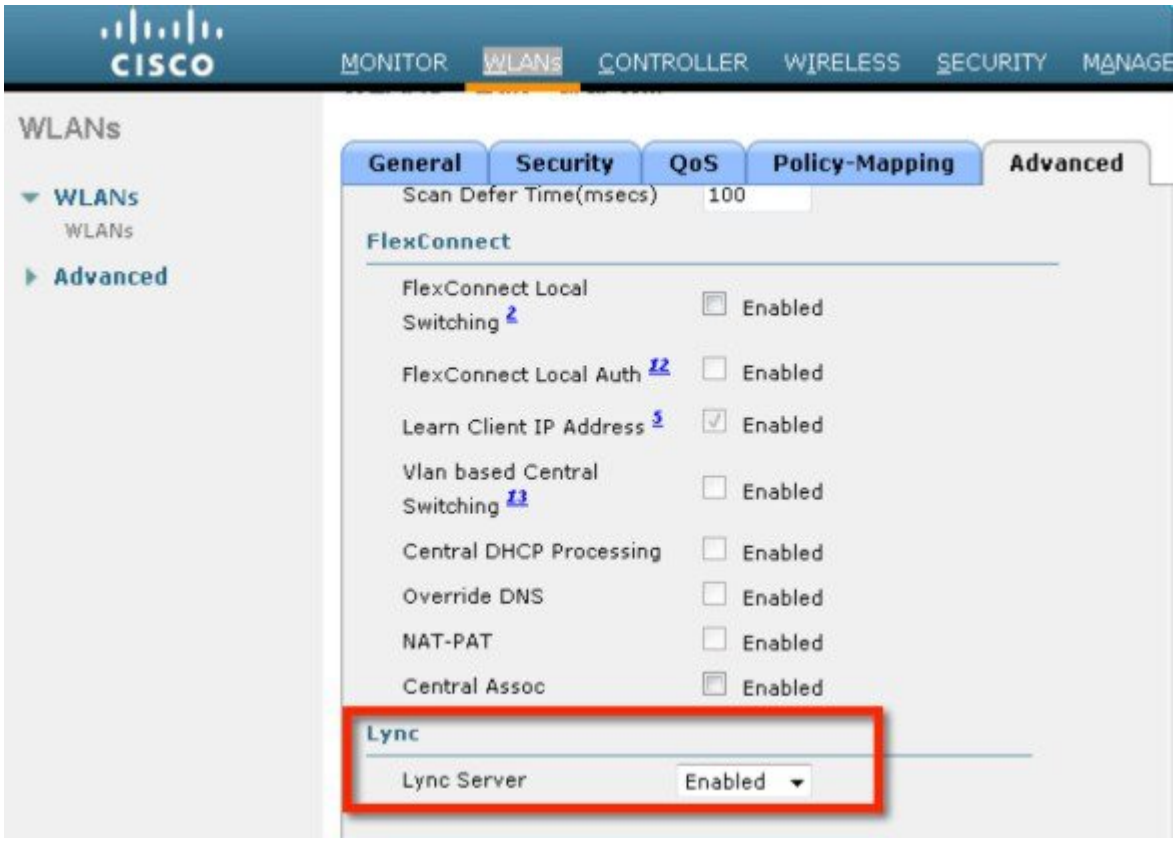
Note Port 15790 is arbitrary, but commonly used, just make sure that the Lync SDN server is also configured for use with the same port.

The reason for using HTTP is to simplify testing. HTTPS is also supported. For more information on this setup, refer to the following Microsoft web page: http://msdn.microsoft.com/en-us/library/office/dn439302(v=office.15).aspx

Step 2 Configure Lync WLAN:

a) Navigate to the **WLANs** and select the WLAN on which you want to have Lync service enabled.

b) Under the **Advanced** tab, in the **Lync** area, from the **Lync Server** drop-down list, choose **Enabled**.

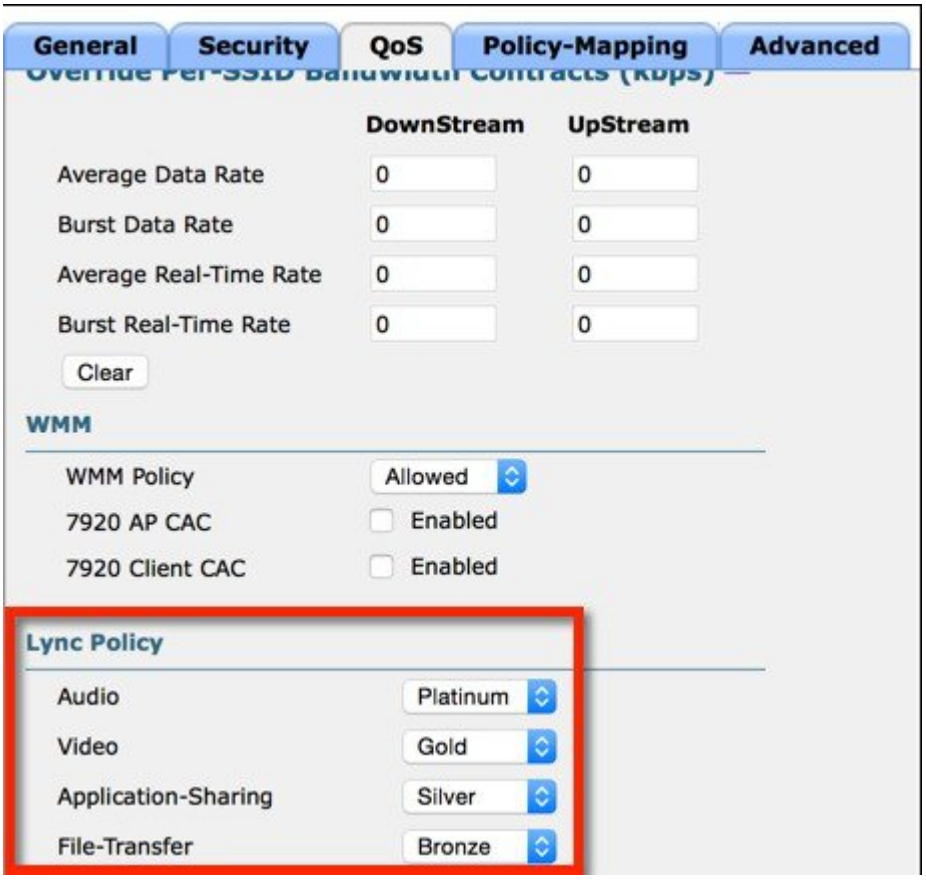


Step 3 Configure WLAN QoS:

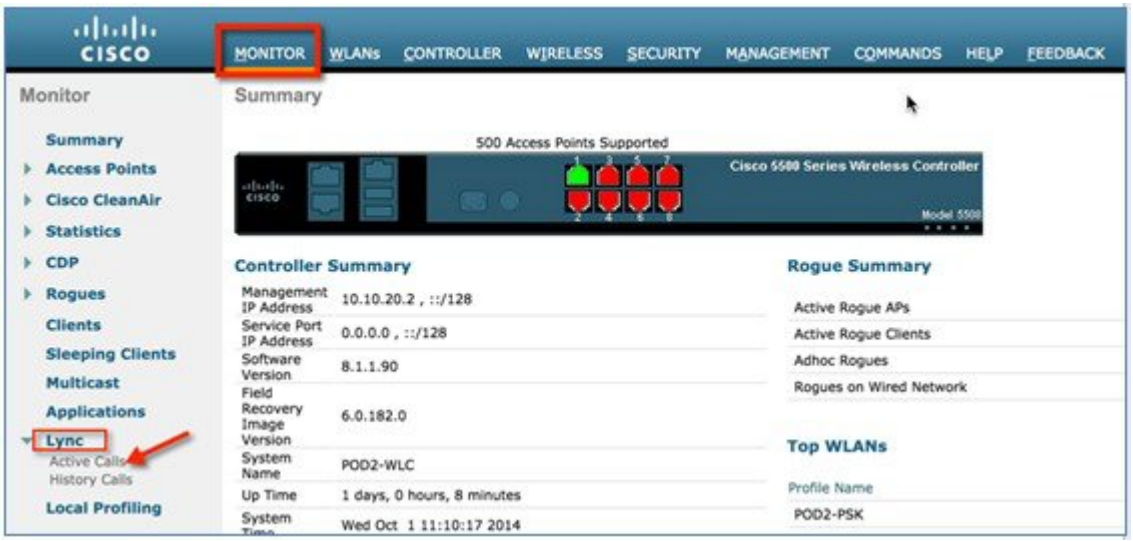
a) On the same WLAN, click the **QoS** tab, and enable **Application Visibility**.

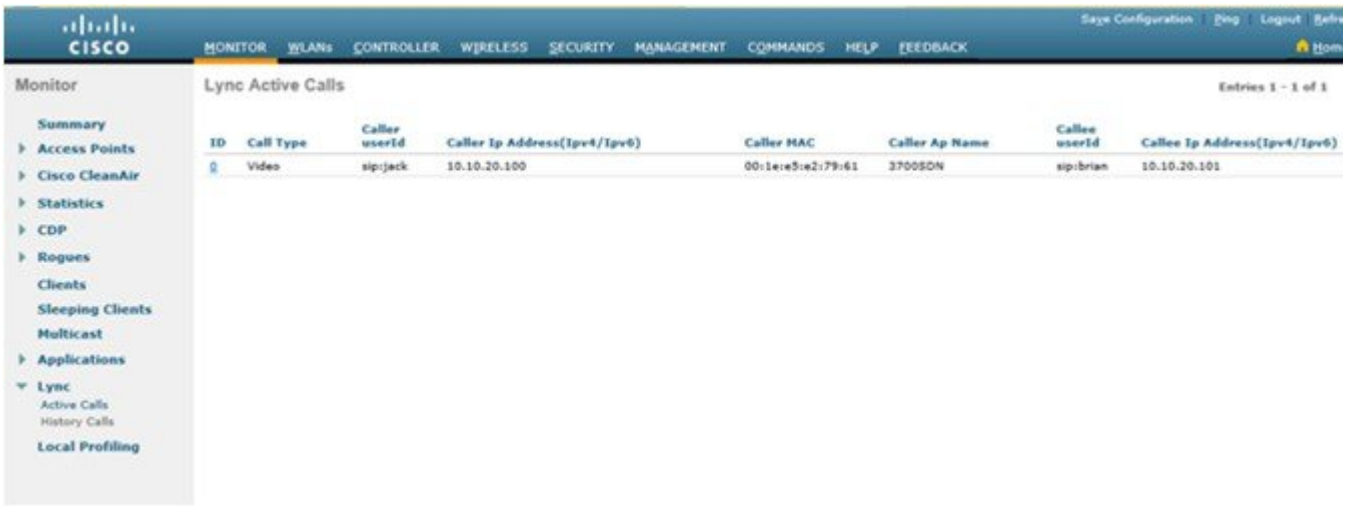
Note Enabling Application Visibility is not mandatory, but is recommended to see if the Lync calls are getting classified and recognized).

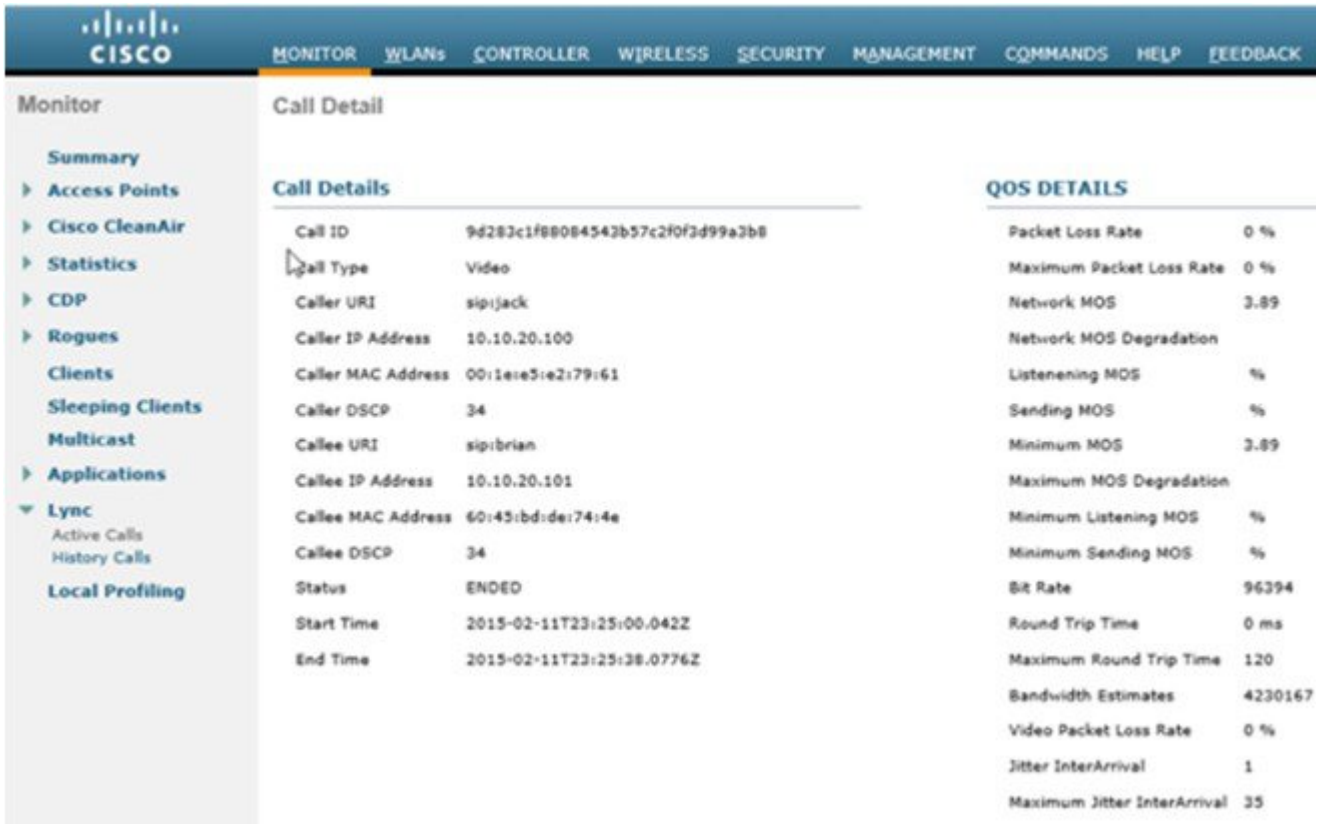
b) Scroll down to the **Lync Policy** area, and define the following parameters: **Audio = Platinum, Video = Gold, Application-Sharing = Silver, File-Transfer = Bronze**.



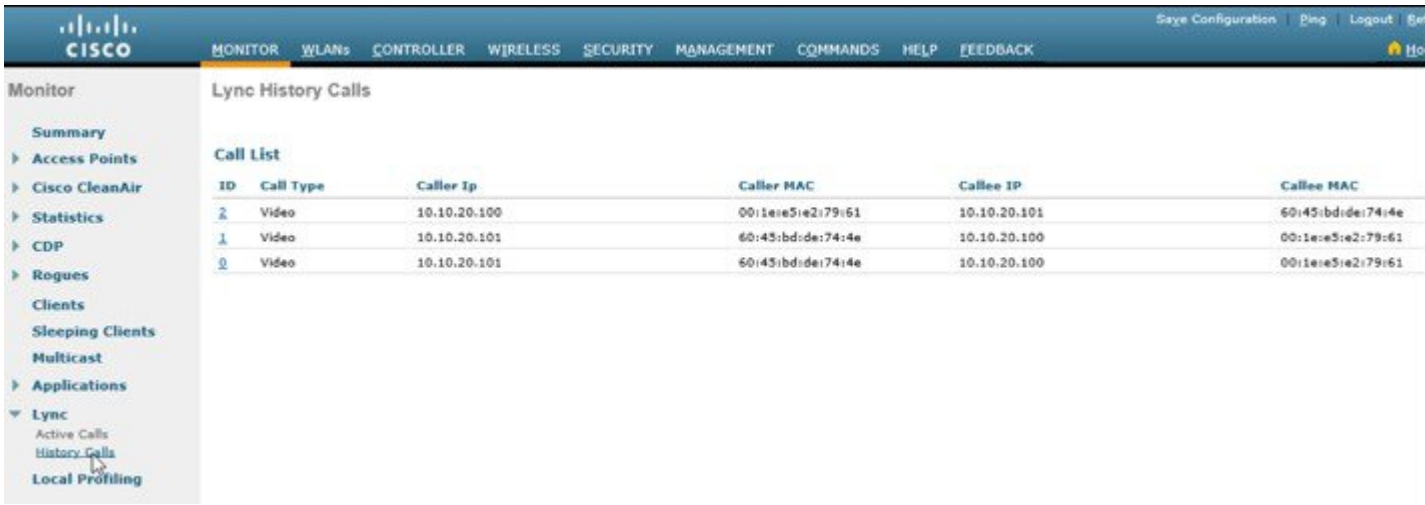
Step 4 To monitor the call, navigate to **MONITOR > Lync SDN > Active Calls**. You can view the lync-call status.


MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Lync
Active Calls
History Calls
Local Profiling
Summary
500 Access Points Supported
Cisco 5500 Series Wireless Controller
Controller Summary
Management IP Address
10.10.20.2 , ::/128
Service Port IP Address
0.0.0.0 , ::/128
Software Version
8.1.1.90
Field Recovery Image Version
6.0.182.0
System Name
POD2-WLC
Up Time
1 days, 0 hours, 8 minutes
Rogue Summary
Active Rogue APs
Active Rogue Clients
Adhoc Rogues
Rogues on Wired Network
Top WLANs
Profile Name
POD2-PSK


MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Lync
Active Calls
History Calls
Local Profiling
Lync Active Calls
ID
Call Type
Caller userId
Caller Ip Address(Ipv4/Ipv6)
Caller MAC
Caller Ap Name
Callee userId
Callee Ip Address(Ipv4/Ipv6)
0
Video
sip:jack
10.10.20.100
00:1e:e5:e2:79:61
3700SDN
sip:brian
10.10.20.101



Step 5 Once the call is complete, you can view the call stats such as MOS value and jitter under **MONITOR > Lync > History Calls**.



Summary

Wireless is the primary mode for access-layer deployment and customers expect to complete support of collaboration applications over WLAN. The best practice for WLANs continues to be to deploy highly-available WLCs, in conjunction with high-density of access points to promote always-available WLAN infrastructure.

In addition, technologies such as Cisco CleanAir, ClientLink, and radio resource management (RRM) allow you to optimize your network performance while simultaneously reducing coverage holes and bypassing interference.

Finally, this white paper shows you how Cisco AVC / Lync SDN API classify Lync 2013 and allow customers to prioritize audio and video using the appropriate QoS treatments. The Microsoft Lync certification is the proof-point that Cisco WLAN provides industry-leading support for collaboration and business applications.

For More Information

Refer to the following Cisco and Microsoft online references for more information:

Cisco Validated Designs and Solution Reference Network Design (SRND)

- The Cisco Design Zone website contains the primary library of solution guides for Collaboration, Enterprise Networks, Mobility, and technologies.

  http://www.cisco.com/c/en/us/solutions/enterprise/unified-communication-system/index.html

  - The Cisco Real-Time over Wireless LAN Design Guide is listed under Collaboration.
  - The Overall Mobility Design is listed under Design Zone for Mobility.

- Cisco Collaboration 9.x SRND

  - This document provides design considerations and guidelines for deploying Cisco Unified Communications and Collaboration solutions, including: Cisco Unified Communications Manager 9.x (offers design for integration with Microsoft Lync.

    http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab09/clb09.html

    http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab09/clb09/collabor.html

AVC – Application Visibility and Control

- Cisco Application Visibility and Control (AVC) Q&A

  http://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/qa_c67-722538.html

- Configuring Application Visibility and Control (WLC 7.6 or later)

  http://www.cisco.com/c/en/us/support/wireless/5508-wireless-controller/model.html

Microsoft Lync

- Deploying Lync Clients: Lync Tech Center
  http://technet.microsoft.com/en-us/lync/fp123621.aspx
- Lync Online Wiki Portal
  http://community.office365.com/en-us/wikis/lync/default.aspx

Cisco Unified Communications

- Support forum: Cisco Support Community for IP Telephony, Voice, and Video Collaboration
  https://supportforums.cisco.com/community/netpro/collaboration-voice-video/ip-telephony
- Cisco Communities: Unified Communications
  https://communities.cisco.com/community/technology/collaboration/uc

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands