White Paper

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. The recently introduced AVC protocol pack 6.3 operates with next-generation Network-Based Application Recognition (NBAR2) engine 13 to provide you this. With this capability you can identify Lync version 2013 and also sub-classify how much of your traffic is data (desktop share), audio, and 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 also 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 reference section. This document will focus on a Wi-Fi design that best provides high-quality calls for the users of the Lync Client with Microsoft Lync server.

Figure 1 outlines a deployment example.

Figure 1. Deployment Architecture of a Typical Cisco Unified Communications Integration for Microsoft Lync Deployment

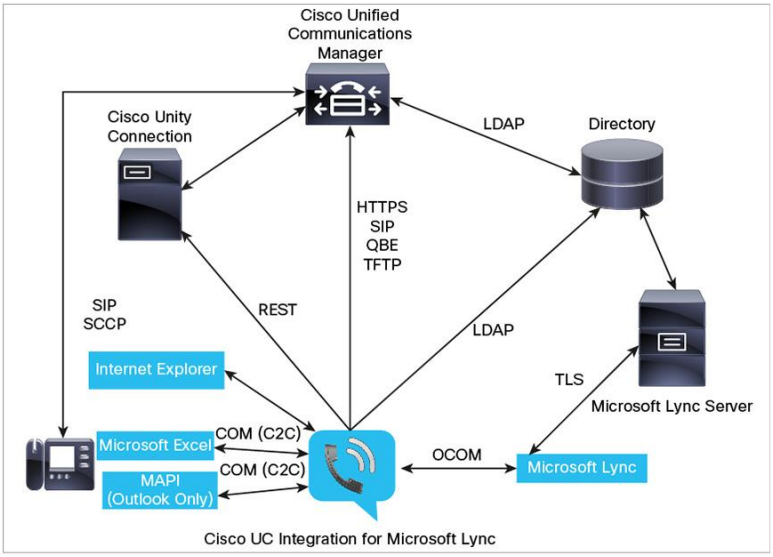


Figure 1 is included in the Administration Guide for Cisco Unified Communications (UC) Integration for Microsoft Lync. This is an example of an installation that includes both a Cisco Unified Communications Manager and a Microsoft Lync Call Manager. The Cisco Unified Wireless Network (UWN) WLAN technologies 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 user priority. 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). Within the definition of a particular SSID there is a range of Wi-Fi multimedia (WMM) user priority classes (0-7) that nearly match the class-of-service priorities in 802.1Q (see Figure 2). 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. The Cisco 802.1p value table differs somewhat from Microsoft's. If there is a mixture of vendor switch and routers, then service-policy mapping for cos-dscp may be a design requirement.

Figure 2. Wi-Fi Multimedia User Priority Class and 802.1Q Class-of-Service Priorities Comparison Table

Cisco 802.1p User Priority based Traffic Type	Cisco 802.1p CoS	Cisco IP DSCP	IEEE IP DSCP	IEEE 802.11e/ WMM User Priority
Reserved (Network Control)	7	56	56	7
Reserved	6	48		
Voice	5	46 (EF)	48	6
Video	4	34 (AF41)	40	5
Voice Control	3	26 (AF31)	32	4
Background (Gold)	2	18 (AF21)	16	3
Background (Gold)	2	20 (AF22)	16	3
Background (Gold)	2	22 (AF23)	16	3
Background (Silver)	1	10 (AF11)	8	2
Background (Silver)	1	12 (AF12)	8	2
Background (Silver)	1	14 (AF13)	8	2
Best Effort	0	0 (BE)	0.24	0
Background	0	2	8	1
Background	0	4	8	1
Background	0	6	8	1
Unknown DSCP from wired	Access port	D	Don't care	D >> 3

WLAN QoS

WLAN QoS is the result of a joint effort between Microsoft, Cisco, and the IEEE to bring QoS to Wi-Fi channels. The IEEE ratified the Wi-Fi QoS specification in 2005. The specification is 802.11e. 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 (WWM). WWM 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 fashion 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”.

The Wi-Fi WLAN QoS level recommended for Lync clients is a QoS level of platinum. The platinum QoS level is for voice priority traffic. It is a configuration option on the WLC that is part of the SSID definition. This allows audio traffic to be sent at the IEEE 802.11e user priority value of 6 (voice), which would most likely carry a 802.3 header value for differentiated services code point (DSCP) of 46 (expedited forwarding). The recommended WMM setting is required. This keeps non-WMM clients from connecting to the SSID. WMM/802.11e was ratified in 2005. Only legacy clients like handheld data transaction computers and old laptop computers would be kept from joining the WLAN. Smartphones and tablets are WMM-capable and enabled. 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.

Cisco AVC classifies applications using deep packet inspection techniques with the NBAR engine, and provides application-level visibility and control into Wi-Fi networks. After the applications are recognized, the AVC feature can enable you to either drop or mark the data traffic. Using AVC, the controller can detect more than 1000 applications. AVC helps you to perform real-time analysis and to create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

The QoS Behavior with AVC Between the Access Point, the WLC, and the infrastructure Upstream

1. A packet is transmitted with or without inner DSCP from a wireless side (wireless client).
2. An access point will forward that packet on the Ethernet inside a Control and Provisioning of Wireless Access Points protocol (CAPWAP) packet with the header having the destination address of the WLC.
3. The WLC will remove the CAPWAP header.
4. The AVC module on the WLC will overwrite the original DSCP value of the source packet to the configured value in the AVC profile. The WLC will then forward 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. AVC module logic will overwrite the inner-DSCP value of the downstream source packet.
3. A controller will compare the WLAN QoS configuration (as per 802.1p value that is actually 802.11e) with the inner-DSCP value that NBAR had overwritten. The WLC will choose the lesser value and put it into CAPWAP header for DSCP.
4. The WLC will send out the packet to the access point with a QoS user priority on the outer CAPWAP header. That value is no higher than the QoS priority configured on the WLAN.
5. 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.

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.

Switch Port Configuration for Access Points 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. Below is an example of this switchport configuration. Note that this configuration addresses only the classification and queuing commands that can be added depending on local QoS policy.

```
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.

QoS CAPWAP Packets over WAN Connections

The QoS classification decision at the WLC-connected switch is slightly more complicated than at the access point-connected switch because the choice can be to either trust the DSCP or the CoS of traffic coming from the WLC. When making this decision, consider that:

- Traffic leaving the WLC can be either upstream (to the WLC or network) or downstream (to the access point and WLAN client). The downstream traffic is CAPWAP-encapsulated, and the upstream traffic is either CAPWAP-encapsulated or un-encapsulated WLAN client traffic leaving the WLC.
- DSCP values of CAPWAP packets are controlled by the QoS policies on the WLC; the DSCP values set on the WLAN client traffic (encapsulated by the CAPWAP tunnel header) have not been altered from those set by the WLAN client.
- CoS values of frames leaving the WLC are set by the WLC QoS policies, regardless of whether they are upstream, downstream, encapsulated, or un-encapsulated.

QoS LAN Switch Port Configuration Example for a WLC

The following example chooses to trust the CoS settings of the WLC because this allows a central location for the management of WLAN QoS rather than having to manage the WLC configuration and an additional policy at the WLC switch connection.

```
interface GigabitEthernet1/0/13
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 11-13,60,61
switchport mode trunk
mls qos trust cos
end
```

Recommended WLC configuration for Lync clients

There are many Wi-Fi configuration options on the Cisco WLCs. For an overall view of design options of the WLC, visit the Cisco Validated Design Program webpage at http://www.cisco.com/go/cvd and review the Enterprise Mobility Design Guide and Real-Time Traffic over Wireless LAN.

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 the 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:

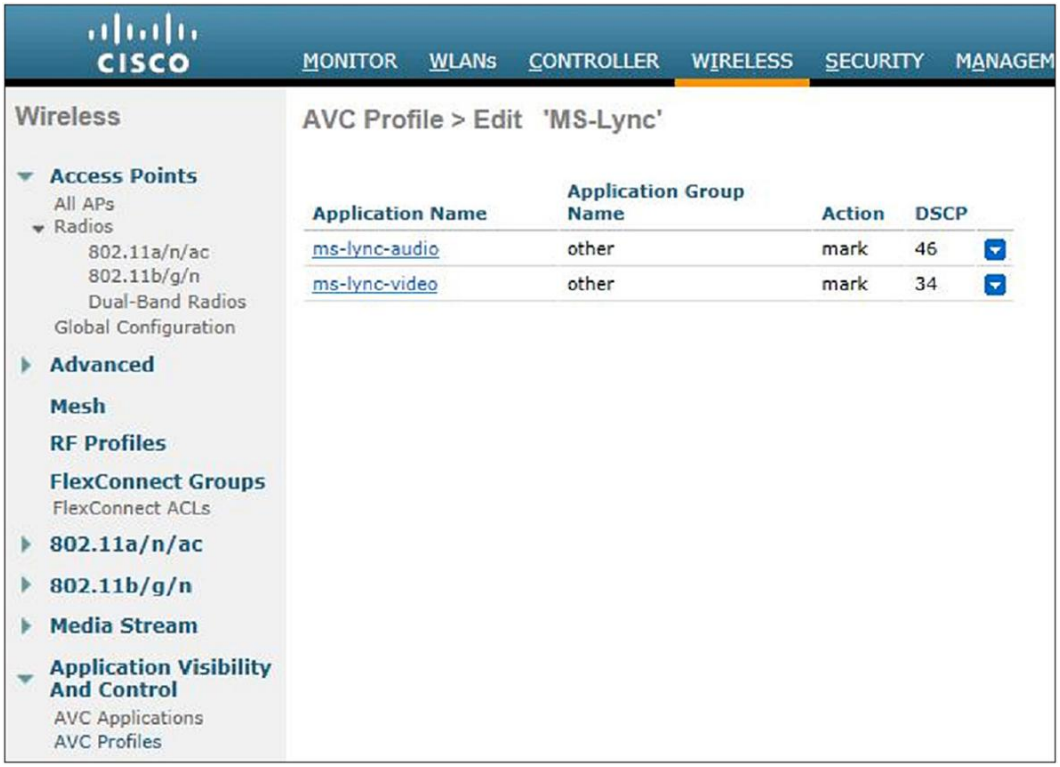
1. WLAN QoS equal to platinum
   a. Adding QoS service profiles when appropriate
   b. Adding QoS service roles when appropriate
2. WLAN band select to push clients to the 5-GHz band, where coverage design supports VoWLAN
3. WLAN 802.1x security
   a. Adding fast transition (11r) when appropriate to improve re-authentication roams
4. 802.11k to provide access point neighbor lists based on client location for network-assisted roaming
5. **Disabled** access point load balance
6. **Enabled** channel scan at defaults
7. **Enabled** AVC for all Lync Application packet types at desired DSCP values
   a. Add AVC profiles for other applications as best-suited for the WLAN or VLAN

Overview of the Suggested AVC Configuration for the Lync Application

Visit the WLC 7.6 configuration guide to AVC configuration at http://www.cisco.com/c/en/us/support/wireless/5508-wireless-controller/model.html#ConfigurationGuides.

More GUI Illustrations of Recommended AVC Configuration for Lync audio and Video

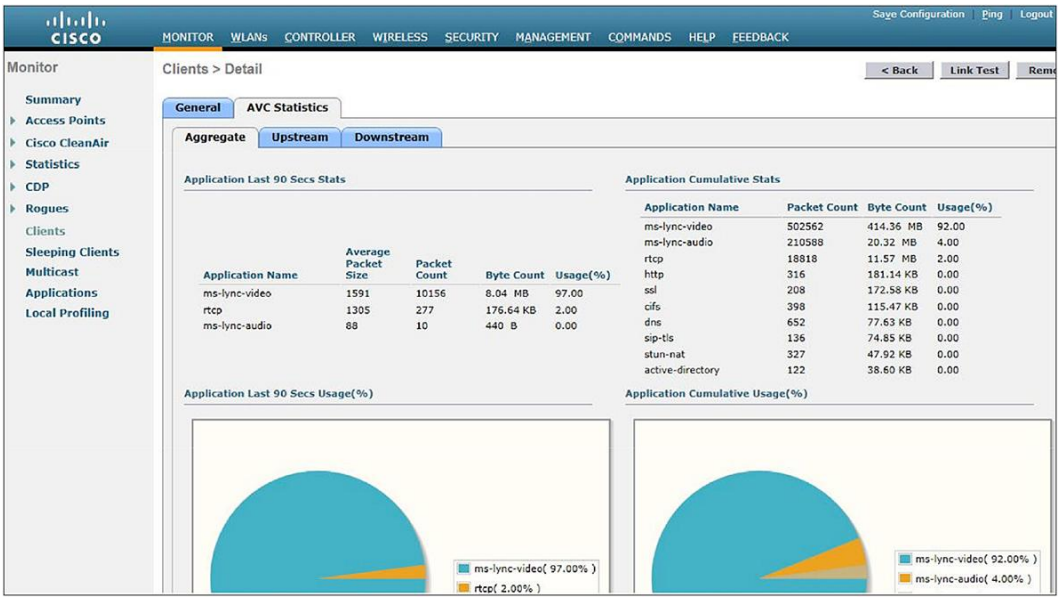
1. Add a specific Lync application packet type for remarking the DSCP value for that packet type.
2. This graphic shows how to configure an AVC profile for use in a WLAN.



3. The user-created AVC profile name is ‘MS-Lync’.
4. This sample profile will use two pre-defined application names (these are found in the AVC database) that fingerprint the secure Lync audio and video packets.
5. The user then adds to the profile as many applications as needed. This WLAN may also be used for Skype; the user could want those packets marked with a DSCP value of 20.
6. In this sample profile AVC, remark the Lync audio packet to a DSCP value of 46 and the video packets at 34.

7. The user-created WLAN is set up with ‘Application Visibility’ **enabled** and the ‘AVC Profile’ of **MS-Lync** created in the previous.

8. Now the Lync traffic in this WLAN will have its traffic remarked to the values in the profile.



9. This shows traffic of one Lync video call between two Wi-Fi endpoints.

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

Summary

Wireless is the primary mode for access-layer deployment and customers expect 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 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 classifies Lync 2013 and allows 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 Cisco and Microsoft online references below for more information.

Cisco Validated Designs and Solution Reference Network Design (SRND)

- **Note:** The Cisco Design Zone website contains our primary library of solution guides for Collaboration, Enterprise Networks, Mobility, and Medianet technologies
  - The “Cisco Real-Time over Wireless LAN Design Guide” is listed under Collaboration
  - Our ‘Overall Mobility Design’ is under Design Zone for Mobility

- Cisco Collaboration 9.x SRND - August 23, 2013
  - This document provides design considerations and guidelines for deploying Cisco Unified Communications and Collaboration solutions, including Cisco Unified Communications Manager 9.*x* (offers design considerations for integration with Microsoft Lync)
  - http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/collab09/clb09.html
  - http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/collab09/collabor.html#wp1286569

AVC - Application Visibility and Control

- Cisco Application Visibility and Control (AVC) Q&A
  http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps12722/qa_c67-722538_ps10315_Products_Q_and_A_Item.html
- Configuring Application Visibility and Control (WLC 7.6)
  http://www.cisco.com/c/en/us/support/wireless/5508-wireless-controller/model.html#ConfigurationGuides

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

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-730674-01 04/14