DEPLOYMENT GUIDE

DEPLOYING MOBILITY CONTROLLERS FOR MICROSOFT LYNC USING CLASSIFY MEDIA, ARUBA'S HEURISTIC-BASED LYNC TRAFFIC CLASSIFICATION

INTRODUCTION

The adoption of enterprise unified communication (UC) applications like Microsoft Lync is growing with incredible speed. The combination of mobile UC clients and a UC-enabled Wi-Fi enables companies to improve collaboration, communication and mobility throughout the enterprise.

Mobile devices running UC applications also create an excellent opportunity to rightsize networks and forgo investments in expensive switching infrastructure, backup power refresh and desk phones.

One of the biggest obstacles for mobile UC over a WLAN has been the wireless infrastructure's limited ability to provide a high-quality user experience.

This document describes the configuration of Aruba Mobility Controllers to detect Lync traffic based on heuristic detection. Heuristics detection of Lync 2010 and 2013 traffic has been available since ArubaOS™ 6.0. Using heuristic detection Lync traffic can be automatically prioritized for voice and video.

This document assumes the existence of a tested Lync installation and a fully functioning Aruba WLAN. It is advisable to confirm the functionality of all components prior to configuration.

This guide additionally references best-practices settings. Please refer to the ArubaOS user guide as well as the Aruba campus WLAN validated reference design guide for additional detailed configuration steps needed to ensure proper WLAN configuration.

SOLUTION COMPONENTS

Lync 2010/2013/Lync online system

These Lync systems handle processing and management. The heuristics engine can detect Lync traffic for systems running Lync 2010, 2013 and Lync online solution (as part of Office 365).

Lync 2010 and 2013 clients

Lync clients provide a single interface for the user to communicate via instant messaging, voice messaging, calling to outside phones, video conferencing, web conferencing and file sharing. Clients are available for nearly all operating systems, including Windows, Mac OS, Android, iOS, Windows Mobile and BlackBerry.

Aruba Mobility Controllers

Mobility Controllers offer centralized network services to Aruba APs and come in different capacities and form factors that fit into any size network. To take advantage of Lync heuristic detection, Mobility Controllers must be running ArubaOS 6.0 or later.

Aruba APs

Aruba APs come in a variety of different configurations, which gives customers a wide range of options for speed – 802.11ac, 802.11n and 802.11a/b/g – as well as capacity and RF coverage. Any AP that is compatible with a Mobility Controller can be used with the Lync integration.

SOLUTION DESCRIPTION

The Lync client and server send call control signals through the Mobility Controller via TCP port 5061 or TCP 443, which initiates a Lync call. This information is used to identify clients in the call and prioritize RTP streams.

Configuration guidelines for Lync over Wi-Fi

The following best practices are a required for a successful wireless Lync solution. Please refer to the ArubaOS user guide and Aruba campus WLAN validated reference design guide for details on making these settings.

NOTE: Please review wmm dscp mapping values in show wlan ssid-profile <ssid name> output and verify it matches QoS settings on the server and wired infrastructure as appropriate. Refer to "Configuring DSCP-WMM section" in this document for more details on DSCP-WMM configuration.What is DLNA?

DLRF RECOMMENDATIONS

- 100% coverage in all areas of Lync use
- Capacity-based RF design:
- Distance between two APs should not exceed more than 50 feet
- Min and max AP power difference no greater than two steps
- AP Power setting to low to moderate power
- Disable lower data rates
- Set supported beacon rate to higher rate
- Minimum RF signal (RSSI) levels of -65 dBm
- Minimum signal-to-noise ratio (SNR) of 25 dB
- Local probe request threshold to 18
- Cell size reduction to 15 dB for dense deployment with AP-225s, and 10 dB for dense deployment with AP-135s

CONTROLLER SETTINGS

- Broadcast filter ARP – enabled on the virtual AP profile
- Enable fair-access station shaping policy in the traffic management profile
- On the SSID profile
- Set max-retries to eight
- Configure QoS settings (DSCP-WMM mapping) to be the same as the wired network and as per the tagging in the client devices if configured
- In the ARM profile
- Enable voice/video aware scan
- ClientMatch™ - enabled
- In case of 802.1X authentication in the dot1X profile
- Enable Opportunistic Key Caching (OKC)
- Enable validate-pmkid
- Enable EAPOL rate optimization

NETWORK PERFORMANCE

- End-to-end QoS - Make sure the same QoS configured and matched across all the wired switches/routers and in wireless infrastructure end-to-end. Ensure that APs are included in QOS trust to enable upstream markings.
- Round trip delay of less than 100 ms between clients
- Jitter of less than 10 ms
- Packet loss <5%
- QoS trust on all voice ports
- When using mobile clients for Lync, Aruba recommends choosing clients that are WMM® certified to ensure Lync traffic is prioritized appropriately

  NOTE: WMM certification for clients does not mean that the client traffic will be automatically prioritized in the air as per the WMM standards. For the upstream Lync traffic, from the client device, to benefit from WMM, the device's operating system needs to pass the classification from the application to the WLAN interface. This may be automatically supported on purpose built Wi-Fi Lync devices. However, on general purposed platforms like PCs, mobile phones and tablets, application traffic classification support on the OS must be implemented before the WMM features can be leveraged. Please refer to you device vendors OS recommendations to enable application traffic classification on the respective devices.

  NOTE: Beginning in Aruba OS 6.3.1 Lync can be integrated to ArubaOS via the Microsoft SDN API. The SDN API provides improved visibility and troubleshooting capabilities for Lync. Heuristic and SDN integration are mutually exclusive in Aruba OS 6.3.x and cannot be configured together. But in Aruba OS 6.4, heuristics and SDN API can be configured together. Refer to "What's New in AOS v6.4" section below for more details.

Configuring the Aruba Mobility Controller to detect Lync traffic for Lync 2010/2013

The Mobility Controller can detect Lync traffic through packet inspection via an ACL configured in a user role. Inspection of this traffic is made possible through the use of the classify media option in the ACL.

The classify media option tells the controller to watch the call control ports and then sample UDP traffic to detect a Lync call. To ensure optimal performance only a few packets are sampled. Once a call is detected the Mobility Controller will prioritize the stream on the AP.

- It is recommended to set up a netdestination alias for the Lync front end servers

```
netdestination lync-servers
        host 192.168.10.10
        host 192.168.20.10
!
```

- Create an ACL to monitor the Lync call setup traffic: laptop clients will communicate on 5061 and mobile on 443.

  NOTE: You must also ensure that the Lync clients can communicate with other Lync clients via standard RTP ports (UDP 1024 -65,535) or to the RTP ports as configured on the Lync server. Please refer to this tech net doc for more info http://technet.microsoft.com/en-us/library/jj204760.aspx

```
ip access-list session lync-control
        any alias lync-servers svc-
        sips permit classify-media
        any alias lync-servers 443
        permit classify-media
!
ip access-list session lync-rtp
        any any udp 1024 65535 permit
!
```

- Apply the ACL to the user role used for Lync traffic

```
user-role lync-user
        access-list session lync-
        control
        access-list session lync-rtp
```

  NOTE: Administrator must configure an ACL to allow TCP based non-RTP Lync traffic such as desktop-sharing and file transfer. This traffic will not be prioritized by heuristics, but ACL will ensure the traffic is not blocked.

Configuring the Aruba Mobility Controller to detect Lync traffic for Lync Online

Clients that connect to Microsoft Lync Online for Lync use Port 443 to send call control to the Lync servers. Since only a small number of packets are inspected applying this ACL should have minimal impact on the controller even though all https sessions will be inspected.

- Create an ACL to monitor the Lync call setup traffic

```
ip access-list session lync-365-control
    any any tcp 443 permit classify-media

!

ip access-list session lync-rtp
    any any udp 1024 65535 permit

!
```

- Apply the ACL to the user role used for Lync traffic

```
user-role lync-user

    access-list session lync-365-control

    access-list session lync-rtp
```

Verifying operation of heuristics detection of Lync traffic

Once heuristics detection is configured on the Mobility Controller and users are assigned the role with the Lync detection ACL, the Mobility Controller will begin to identify and prioritize the Lync traffic.

NOTE: Beginning in ArubaOS 6.3 additional commands to monitor Lync traffic via the SDN API were introduced. When using heuristics these commands will not display Lync call or client information.

To verify the operation of the heuristics detection start a Lync call between two clients and then log into the Mobility Controller via the command line. Run the following commands to verify heuristic detection.

```
show datapath session table <IP-of-Lync-Client>
```

Ensure that the traffic between the two clients has the V flag set.

```
show voice call-cdrs
```

Ensure call data is recorded for each call (note there will be one call per device)

Voice Client(s) CDRs									
CDR ID Value	Client IP Call Type	Client Name	ALG	Dir	Called to	Status	Dur(sec)	Original time	R-
29	10.79.225.6	Client	lync	NA	NA	SUCC	32	Oct 9 13:51:34	NA
NA									
28	10.79.225.6	Client	lync	NA	NA	SUCC	24	Oct 9 13:43:02	NA
NA									
27	10.79.225.8	Client	lync	NA	NA	SUCC	70	Oct 9 13:39:08	NA
NA									
26	10.79.225.6	Client	lync	NA	NA	SUCC	92	Oct 9 13:38:46	NA
NA									
25	10:79.225.8	Client	lync	NA	NA	SUCC	36	Oct 9 13:37:50	NA
NA									

Configuring DSCP-WMM mapping on the Aruba Mobility Controller

DSCP-WMM mapping for Lync voice/video traffic can be configured on the controller. In addition, DSCP-WMM mapping for best-effort and background traffic can be configured as well as part of this configuration.

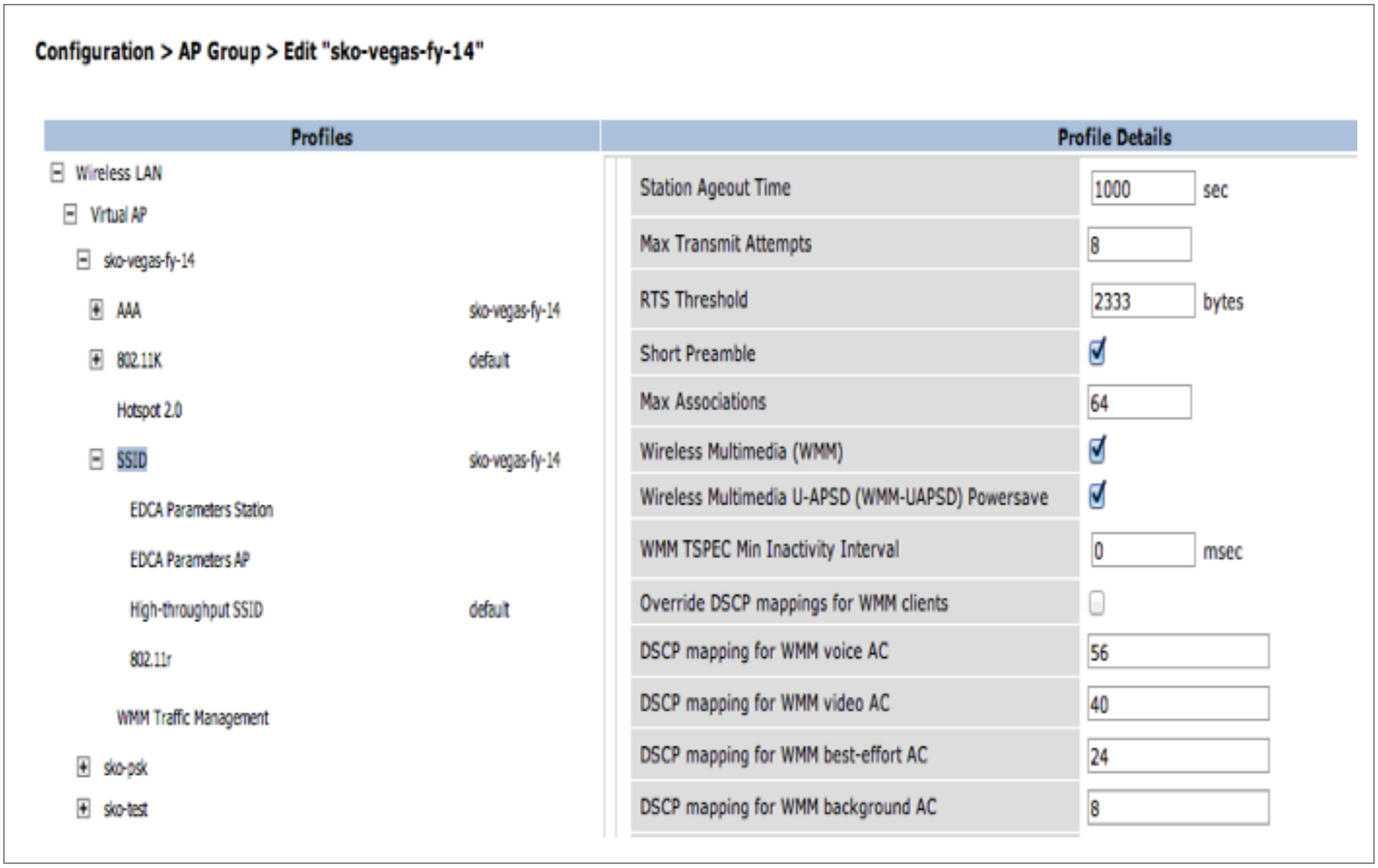
I. Web UI configuration of DSCP-WMM mapping

a. Configure traffic control prioritization profile: In configuration page, go to **“AP Group->Virtual AP->SSID Profile -> Advanced”**

III. Default DSCP-WMM mapping

If no DSCP value is configured on the controller, Lync VO/VI traffic will be marked with default DSCP Tags. The default DSCP tag for Lync heuristics is as follows -

Traffic Type	Default DSCP	Default WMM
Voice	48	WMM-AC-VO
Video	40	WMM-AC-VI
Best Effort	24	WMM-AC-BE
Background	8	WMM-AC-BK



Configuration > AP Group > Edit "sko-vegas-fy-14"

Station Ageout Time	1000 sec
Max Transmit Attempts	8
RTS Threshold	2333 bytes
Short Preamble	☑
Max Associations	64
Wireless Multimedia (WMM)	☑
Wireless Multimedia U-APSD (WMM-UAPSD) Powersave	☑
WMM TSPEC Min Inactivity Interval	0 msec
Override DSCP mappings for WMM clients	□
DSCP mapping for WMM voice AC	56
DSCP mapping for WMM video AC	40
DSCP mapping for WMM best-effort AC	24
DSCP mapping for WMM background AC	8

II. CLI Configuration

```
# configure terminal
 (config) # wlan ssid-profile “test”
 (SSID Profile “test”) #wmm
 (SSID Profile “test”) #wmm-vo-dscp 56
 (SSID Profile “test”) #wmm-vi-dscp 40
 (SSID Profile “test”) #wmm-be-dscp 24
 (SSID Profile “test”) #wmm-bk-dscp 8
```

WHAT'S NEW IN ARUBA OS 6.4

Simultaneous enablement of SDN API and Lync heuristics

In 6.4, both Lync SDN API and heuristics based classification/ prioritization can be enabled simultaneously. In the case, where both methods are enabled SDN API based Lync classification will take priority.

Dynamic opening of ports for Lync voice/video Traffic

Prior to 6.4, UDP ports are needed be explicitly configured to allow Lync voice/video traffic as below:

```
ip access-list session lync-acl
   any any udp 1025-65535 permit
```

In 6.4, firewall sessions will be dynamically opened up in datapath for Lync Voice and Video calls. For this, UDP port 3478 needs to be permitted in Lync ACL to allow STUN messages. Lync clients initiate STUN connectivity check prior to media transmission. Once STUN connectivity check is succeeded, media transmission happens.

Dynamic opening of ports is not done for Lync desktop-sharing and file transfer calls. Administrator needs to open up TCP ports used by these applications.

CAVEATS IN AOS 6.4

- Real time call quality UCC score is NOT available for Lync voice/video calls using heuristics
- Real time call quality UCC score is NOT available for Lync voice/video calls using Lync Online (Office 365)

APPENDIX A: MICROSOFT LYNC 2013/2013 CERTIFICATION TEST RESULTS

Test results

Microsoft designed three scenarios in their Wi-Fi test plan to mirror real-world conditions of end-users with Microsoft Lync: Data only, fixed and mobility. A series of tests was performed against each of these scenarios to test the infrastructure's ability to handle the QoS, connectivity and scalability requirements of the three test scenarios. A brief description of the three environments tested under the qualification program is as follows:

Lync data-only over Wi-Fi

The Lync Data-Only over Wi-Fi (data-only) category supports environments in which data applications predominate and the density of Wi-Fi clients is modest. While Lync can support a number of modalities; IM, presence, web conferencing and calendaring are predominantly data based modalities that are bursty in nature. Most devices, applications and networks can correctly handle data over Wi-Fi when user and client density is low to moderate.

Lync fixed real-time (RT)-multimedia over Wi-Fi

The Lync Fixed RT-Multimedia over Wi-Fi (Fixed) category is a superset of Lync data-only over Wi-Fi with the added capabilities of voice mail, video conferencing, telephony and audio conferencing over Wi-Fi. The key added functionality in this category is that real-time media is supported over Wi-Fi in a fixed setting.

Lync mobility RT-multimedia over Wi-Fi

The Lync mobility RT-multimedia over Wi-Fi (mobility) category is the superset under which both the data-only and fixed categories coexist. It encompasses all features of the other categories and also includes originating, consuming and terminating Lync services, including RT-multimedia, while mobile, e.g., a user who has a Lync portable device who uses various Lync workloads, including RT-multimedia, while mobile. Lync sessions can be originated when fixed or mobile.

Lync Data-Only over Wi-Fi							
Section	Test Case #	Test Case Description	Result	Lync QoE Results (If multiple calls are being measured, the metrics will be document- ed for each call)			
				Jitter (ms)	Delay (ms)	Packet Loss (%)	NMOS Degrada-tion
4.2		**802.11a Certification**					
	4.2.1	Access Point is 802.11a certified	Pass				
	4.2.2	Access Point support 802.11a operation	Pass	2	6	0.12	0.09
4.3		**802.11G Wi-Fi Certified**					
	4.3.1	Access Point is 802.11g certified	Pass				
	4.3.2	Access point supports 802.11g operation	Pass	1	7	0.03	0.04
4.4		**802.11N Wi-Fi certified**					
	4.4.1	Access Point is 802.11n certified	Pass				
	4.4.2	Access point supports 802.11n operation (2.4GHz)	Pass	2	10	0.25	0.11
	4.4.3	Access point supports 802.11n operation (5GHz)	Pass	2	8	0.1	0.09
4.5		**WPA2 Support**					
	4.5.1	Access point is certified for WPA2 enterprise	Pass				
	4.5.2	Access Point authenticates Lync End Point using WPA2 PSK	Pass	0.06	9	0.17	0.06

	4.5.3	Access Point authenticates Lync End Point using WPA2 Enterprise	Pass	2	8	0.05	0.08
	4.5.4	AP supports PMK for roaming	Pass	2	18	0.63	0.44
4.6		**Wide Channel Operation**					
	4.6.1	AP connectivity with both 20MHz and 40MHz support on 5GHz band	Pass	2	8	0.1	0.09
4.7		**Power Over Gigabit Ethernet**					
	4.7.1	AP can be powered using a Power over Gigabit Ethernet inter-face	Pass				
4.8		**IPv6 Support**					
	4.8.1	AP supports IPv6 in either hardware or software	Pass				
	4.8.2	AP can handle calls when both IPv4 and IPv6 are enabled	Pass	2	10	0.25	0.12
4.9		**Band Steering**					
	4.9.1	AP can steer dual band clients to 5GHz when Band Steering is enabled	Pass	2.5	8	0.13	0.1
4.10		**Spectrum Analysis**					
	4.10.1	AP can detect and display the source of interference on a channel	Pass	1	34	0	0.02
	4.10.2	AP can determine the category of interference in English terms	Pass	1	34	0	0.02
4.11		**Logging**					
	4.11.1	AP generates session logs with session details	NA	2	6	0.56	0.13
4.12		**RF Coverage**					
	4.12.1	WLAN solution can identify the client's location (AP it is connected to) and past roaming history archives the movements of the client	Pass	4	9	0.47	0.38
	4.12.2	WLAN solution displays RF coverage heat maps in 2.4 GHz	Pass				
	4.12.3	WLAN solution displays RF coverage heat maps in 5 GHz	Pass				
4.13		Ability to distinguish between voice/video/data sessions					
	4.13.1	Video session is specified as such in the logs	NA	3	6	0.1	0.04
	4.13.2	Access Point should be able to distinguish between voice and video data traffic	NA	3	6	0.1	0.04
4.14		**Fair distribution of airtime among clients with different speeds**					
	4.14.1	All 11n clients	Pass	ATF disabled: 3 ATF enabled: 1	ATF disabled: 19 ATF enabled: 10	ATF disabled: 1.14 ATF enabled: 0.73	ATF disabled: 0.30 ATF enabled: 0.22

4.14		**Fair distribution of airtime among clients with different speeds**					
	4.14.1	All 11n clients	Pass	ATF disabled: 3 ATF enabled: 1	ATF disabled: 19 ATF enabled: 10	ATF disabled: 1.14 ATF enabled: 0.73	ATF disabled: 0.30 ATF enabled: 0.22
	4.14.2	802.11n capable endpoints have better throughput in a mixed 11n/11g environment when ATF is enabled with fair-access	Pass	ATF disabled: 3 ATF enabled: 2	ATF disabled: 21 ATF enabled: 15	ATF disabled: 16.35 ATF enabled: 0.48	ATF disabled: 1.69 ATF enabled: 0.08
	4.14.3	802.11n capable endpoints have better throughput in a mixed 11n/11a environment when ATF is enabled with fair-access	Pass	ATF disabled: 3 ATF enabled: 4	ATF disabled: 14 ATF enabled: 18	ATF disabled: 36.81 ATF enabled: 0.09	ATF disabled: 2.16 ATF enabled: 0.09
	4.14.4	802.11n clients have better performance in terms of throughput and MOS in a mixed 11n/11a environment when ATF is enabled with preferred access	Pass	ATF disabled: 3 ATF enabled: 9	ATF disabled: 14 ATF enabled: 11	ATF disabled: 36.81 ATF enabled: 0	ATF disabled: 2.16 ATF enabled: 0.02
4.15		**Balancing Client across Access Points**					
	4.15.1	AP responds with busy signal when it has reached maximum allowable users		2	67	0.06	0.07
	4.15.2	WLAN load balances across APs		4	6	0.11	0.11
4.16		**Traffic Classification on a per flow basis**					
	4.16.1	Access Point classifies untagged network inbound video traffic from Lync Server and tags it on the wireless interface to the client	Pass	1	6	0.06	0.13
	4.16.2	Access Point classifies untagged network inbound voice only traffic from Lync Server and tags it on the wireless interface to the client	Pass	5	5	0.13	0.02
	4.16.3	Access Point classifies untagged wireless inbound video traffic from Lync End Point and tags it on the wired interface to Lync Server	Pass	1	4	0.02	0.04
	4.16.4	Access Point classifies untagged wireless inbound voice only traffic from Lync End Point and tags it on the wired interface to Lync Server	Pass	5	5	0.13	0.02
4.17		**Mapping Priority Tags**					
	4.17.1	Access Point remaps incorrect 802.1p and DSCP tags from the network inbound voice traffic to WMM and DSCP tags on wireless outbound interface	Pass	1	5	0.31	0.09

	4.17.2	Access Point remaps incorrect WMM and DSCP tags from wire- less inbound video traffic to 802.1p and DSCP tags on network outbound interface	Pass	4	6	0	0.07
	4.17.3	Access Point remaps incorrect WMM and DSCP tags on wire- less inbound voice traffic to 802.1p and DSCP tags on network outbound interface	Pass	1	5	0	0.03
	4.17.4	Access Point/controller has the ability to retag incorrectly tagged voice only traffic from the wired interface with the correct voice tags on the wired (DSCP tags) and wireless (WMM tags) interfaces	Pass	1	5	0	0.03
4.18		**Shaping Data Traffic**					
	4.18.1	Video call quality is not affected with data traffic shaping enabled	Pass	2	8	0.19	0.1
	4.18.2	Voice call quality is not affected with data traffic shaping enabled	Pass	4	35	0.46	0.17
4.19		**Prioritizing SIP-TLS**					
	4.19.1	Access Point prioritizes untagged SIP TLS traffic from the network over any other traffic type under full congestion	Pass	1	10	0.37	0.15
	4.19.2	Access Point prioritizes untagged SIP TLS traffic from the WLAN over any other traffic type under full congestion	Pass	1	10	0.37	0.15
4.20		**Encryption Support**					
	4.20.1	AP supports WPA2-AES encryption	Pass	6	19	0.25	0.08
	4.20.2	AP supports WPA2-TKIP encryption	Pass	1	38	0	0.01
	4.20.3	AP supports WPA-AES encryption	Pass	1	11	0.13	0.04
	4.20.4	AP supports WPA-TKIP encryption	Pass	3	10	0.05	0.04
4.21		**FIPS Accreditation**					
	4.21.1	140-2 accredited for government applications	Pass				
4.22		**HIPAA Compliance**					
	4.22.1	HIPAA Compliance for healthcare solutions	Pass				
4.23		**PCI Compliance**					
	4.23.1	PCI compliance for applications requiring financial transactions	Pass				
4.24		**ICSA Certified Firewall**					
	4.24.1	Aruba has built-in ICSA certified firewall	Pass				
4.25		**Quarantining Misbehaving Clients**					
	4.25.1	WLAN can detect and quarantine clients that are spoofing IP addresses	Pass				
	4.25.2	WLAN system can detect and quarantine clients that have multiple authentication failures and clients that try to access restricted network	Pass				
	4.25.3	WLAN system detects and quarantines clients generating de-auth attacks	Pass	1	9	0.08	0.04

	4.25.4	WLAN system can detects and prohibits client from associating to ad-hoc networks	Pass	1	9	0.08	0.04
4.26		**Quarantining Misbehaving Clients**					
	4.26.1	Access Point performs rogue Access Point detection while servicing voice call	Pass	2	9	0.15	0.06

Lync fixed real time (RT)-multimedia over Wi-Fi							
Section	**Test Case #**	**Test Case Description**	**Result**	**Lync QoE Results (If multiple calls are being measured, the metrics will be document- ed for each call)**			
				Jitter (ms)	**Delay (ms)**	**Packet Loss (%)**	**NMOS Degradation**
5.2		**WMM Certification**					
	5.2.1	AP is certified for WMM	Pass				
5.3		**Spatial Streams**					
	5.3.1	AP must disclose number of supported spatial streams	Pass				
	5.3.2	AP has at least two transmit antennas	Pass				
	5.3.3	AP has at least two receive antennas	Pass				
5.4		**Dual Band Operation**					
	5.4.1	AP can handle calls in the 2.4 GHz band	Pass	1	7	0.03	0.04
	5.4.2	AP can handle calls in the 5 GHz band	Pass	2	6	0.12	0.09
	5.4.3	AP can handle simultaneous voice calls between users in 2.4GHz and between users in 5GHz	Pass	EP1- EP3 0 EP2- EP4 1 EP1- EP4 2 EP2- EP3 1	EP1- EP3 10 EP2- EP4 10 EP1- EP4 9 EP2- EP3 8	EP1- EP3 0.18 EP2- EP4 0.08 EP1- EP4 0.1 EP2- EP3 0	EP1- EP3 0.07 EP2- EP4 0.06 EP1- EP4 0.02 EP2- EP3 0.02
5.5		**Dynamic RF Power Management**					
	5.5.1	AP supports RF power management in a voice enabled network	Pass				
5.6		**Dynamic Channel Selection**					
	5.6.1	AP supports dynamic channel selection in a voice enabled network	Pass				
5.7		**Defer Intrusion Detection and Scanning while processing Real-Time Traffic**					
	5.7.1	WLAN does not cause jitter of more than 50ms while doing Intrusion Detection (Rogue AP detection)	Pass	2	9	0.15	0.06
	5.7.2	WLAN does not cause more than 1% packet loss while doing Intrusion Detection (Rogue AP detection)	Pass	2	9	0.15	0.06
	5.7.3	WLAN does not cause more than 3 consecutive lost packets while doing Intrusion Detection (Rogue Access Point)	Pass	2	9	0.15	0.06

	5.7.4	Intrusion detection is performed without increasing the RTP delay by more than 50ms (Rogue Access Point)	Pass	2	9	0.15	0.06
	5.7.5	WLAN does not cause degradation of call quality while doing Intrusion Prevention (Rogue Access Point)	Pass	2	9	0.15	0.06
5.8		**WMM Tag Mapping**					
	5.8.1	AP maps WMM priority tag for video traffic to 802.1p priority tag for video traffic on the network side	Pass	2	6	0.27	0.07
	5.8.2	Access Point maps 802.11e (WMM) priority tag for voice traffic to 802.1p priority tag for voice traffic on the network side	Pass	2	6	0.27	0.07
5.9		**Prioritizing Traffic**					
	5.9.1	AP can prioritize voice over video and video over data traffic with WMM and 802.1p tagging disabled on end-points and Lync server respectively	Pass	2	6	0.27	0.07
	5.9.2	AP can prioritize voice over video and video over data traffic with WMM and 802.1p tagging enabled on end-points and Lync server respectively	Pass	2	6	0.27	0.07
	5.9.3	AP can prioritize voice over video and video over data traffic with WMM disabled and 802.1p tagging enabled on end-points and Lync server respectively	Pass	2	6	0.27	0.07
	5.9.4	AP can prioritize voice over video and video over data traffic with WMM enabled and 802.1p tagging disabled on end-points and Lync server respectively	Pass	2	6	0.27	0.07
5.10		**Protecting Existing Call Quality**					
	5.10.1	Existing call quality is not affected when a new call is made through a fully loaded Access Point	Pass	2	6	0.27	0.07
5.11		**Priority Tag Mapping to Tunnel Priority**					
	5.11.1	AP that tunnels all client traffic to controller maps WMM tags to					
	5.11.1	AP that tunnels all client traffic to controller maps WMM tags to DSCP tunnel priority tags	Pass	1	6	0.16	0.02
	5.11.2	AP that tunnels all client traffic to controller maps DSCP tags to DSCP tunnel priority tags	Pass	1	6	0.16	0.02
5.12		**Scalability of Wide Band Codec Voice Calls without Back- ground Traffic**					
	5.12.1	AP must be able to handle at least five Lync video calls (10 clients) with no background traffic	Pass	3.1	9.3	0.12	0.15
5.13		**Scalability of Video VGA Calls without Background Traffic**					
	5.13.1	AP must be able to handle at least one video call with no back- ground traffic	Pass	3.8	17	0.84	0.22
5.14		**Scalability of Wide Band Voice Calls with 100% UDP Down- stream Background Traffic**					

	5.14.1	AP must be able to handle at least one wide-band codec voice call with 100% UDP downstream background traffic	Pass	3.8	17	0.84	0.22
5.15		**Scalability of Wide Band Codec Voice Calls with 100% UDP Upstream Background Traffic**					
	5.15.1	AP must be able to handle at least one wide-band codec voice call with 100% UDP upstream background traffic	Pass	4	10	0.88	0.34
5.16		**Scalability of Video VGA calls with 100% UDP Downstream Background Traffic**					
	5.16.1	AP must be able to handle at least one wide-band codec voice call with 100% UDP downstream background traffic	Pass	3.8	17	0.84	0.22
5.17		**Scalability of Video VGA calls with 100% UDP Upstream Background Traffic**					
	5.17.1	AP must be able to handle at least one wide-band codec voice call with 100% UDP upstream background traffic	Pass	4	10	0.88	0.34
5.18		**Scalability of Wide Band Voice Calls with 100% TCP Down- stream Background Traffic**					
	5.18.1	AP must be able to handle at least one wide-band codec voice call with TCP downstream background traffic	Pass	8.2	26	0.45	0.38
5.19		**Scalability of Wide Band Codec Voice Calls with 100% TCP Upstream Background Traffic**					
	5.19.1	AP must be able to handle at least one wide-band codec voice call with 100% TCP upstream background traffic	Pass	8	23	0.24	0.35
5.20		**Scalability of Video VGA calls with 100% TCP Downstream Background Traffic**					
	5.20.1	AP must be able to handle at least one wide-band codec voice call with 100% TCP downstream background traffic	Pass	8.2	26	0.45	0.38
5.21		**Scalability of Video VGA calls with 100% TCP Upstream Background Traffic**					
	5.21.1	AP must be able to handle at least one wide-band codec voice call with 100% TCP upstream background traffic	Pass	8	23	0.24	0.35

Lync mobility RT-multimedia over Wi-Fi							
Section	Test Case #	Test Case Description	Result	Lync QoE Results (If multiple calls are being measured, the metrics will be document- ed for each call)			
				Jitter (ms)	Delay (ms)	Packet Loss (%)	NMOS Degradation
6		Mobility					
6.2		OKC/PMK Caching					
6.3		Fast Roaming					
	6.3.1	AP ensures fast roaming between APs without affecting call quality when encryption used is 802.1x	Pass	3	11	0.44	0.15
	6.3.2	AP ensures fast roaming between APs without affecting call quality when encryption used is PSK	Pass	2	11	0.59	0.22
	6.3.3	AP ensures fast roaming without affecting call quality when roaming between controller/APs in different subnets	Pass	3	9	0.09	0.07
6.4		Efficient Roaming with AP-assisted Handoff					
	6.4.1	AP supports efficient roaming with AP-assisted handoff					
6.5		Jitter During Roaming					
	6.5.1	AP causes no more than 50ms jitter while roaming between APs	Pass	2	11	0.59	0.22
6.6		Delay During Roaming					
	6.6.1	AP causes no more than 50ms delay when roaming between APs	Pass	2	11	0.59	0.22
	6.6.2	AP causes no more than 100ms delay when roaming between APs under maximum load	Pass	2	11	0.15	0.3
6.7		Packet Loss During Roaming					
	6.7.1	AP causes no more than 1% packet loss while roaming be- tween APs	Pass	2	11	0.59	0.22
	6.7.2	AP causes no more than 3 consecutive lost packets while roaming between APs	Pass	2	11	0.59	0.22
6.8		Broadcast Load Indications using 802.11v QBSS Transition Mgmt. Frames					
	6.8.1	Access Point broadcasts channel load information in beacon and probe response frames when QBSS is enabled	Pass	5	11	1.34	0.34
6.9		UCI Forum UC Mobility Certified					
	6.9.1	AP is UCI Forum UC Mobility Certified	Pass				
6.10		WFA Voice Enterprise (V-E) Certified					
	6.10.1	AP is WFA Voice Enterprise (V-E) Certified	Pass				

APPENDIX B: MICROSOFT LYNC 2010/2013 CERTIFICATION TESTING CONFIGURATION

Relevant configuration settings used for this test

The following configuration settings were used during these tests

```
ip access-list session lync
  any any tcp 5061  permit classify-media queue high
!
user-role lync
 access-list session lync
 access-list session allowall
!
rf arm-profile “lync”
   assignment disable
   max-tx-power 21
   min-tx-power 3
   voip-aware-scan
   ps-aware-scan
!
rf dot11a-radio-profile “slb-a”
   channel 157+
   tx-power 20.5
   slb-update-interval 1
   arm-profile “lync”
!
rf dot11g-radio-profile “slb-g”
   no radio-enable
   channel 6
   tx-power 20.5
   slb-update-interval 1
   arm-profile “lync”
!
wlan wmm-traffic-management-profile “lync”
   enable-shaping
   voice 38
   video 60
   best-effort 1
   background 1
!
wlan ssid-profile “lync”
   essid “lync1”
   opmode wpa2-aes
   wmm
   wpa-passphrase 467a8594684544e217b-
8873deac82124cf5515e58938c724
   qbss-load-enable
!
```

```
wlan virtual-ap “lync”
   aaa-profile “lync”
   ssid-profile “lync”
   vlan 3
   blacklist-time 120
   auth-failure-blacklist-time 180
   vlan-mobility
   wmm-traffic-management-profile “lync”
!

wlan traffic-management-profile “lync”
   bw-alloc virtual-ap “lync” share 100
   shaping-policy fair-access
!
ap-group “lync”
   virtual-ap “lync”
   dot11a-radio-profile “slb-a”
   dot11g-radio-profile “slb-g”
   dot11a-traffic-mgmt-profile “lync”
   dot11g-traffic-mgmt-profile “lync”
```

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com