



**Deploying Microsoft Lync Server 2010:**

Best Practices to achieve optimal voice and video quality with Microsoft Lync Server 2010 on Aruba Wireless LAN infrastructure

**April 2011**

---

## Table of Contents

Introduction	3
Unified Communications and the Mobile Workforce	3
Solution Components	3
Aruba Wireless LAN	3
Microsoft Lync Server 2010 (Standard & Enterprise)	4
Wireless LAN Best Practices for Microsoft Unified Communications	5
Pervasive Wireless Coverage	5
Managing RF Interference	6
Applying Correct Priority to Mixed Voice, Video, and Data Clients	6
Performance Assurance for Encrypted Microsoft Lync Traffic	6
Call Admission Control	6
Microsoft Lync Server 2010 Qualification	6
Test Goals	7
Network Topology	7
Hardware, Tools and Versions	7
Test Methodology	8
Summary Test Results	9
Conclusion	10
References	10
Appendix A: Detailed Test Results	11
Appendix B: Aruba WLAN QoS Configuration	12
Appendix C: Aruba Mobility Controller Configuration	13

---

## Introduction

Workforces are growing increasingly mobile as companies deploy resources closer to customers, and station them in the most cost-efficient locations. The “office” of today is a transitory state defined by wherever a worker happens to be at that moment. No longer tethered to Ethernet cables in assigned offices, mobile workers can be found at home, on the road, in branch offices, and using hoteling suites. To keep such a workforce connected, networks must now be delivered to the worker instead of bringing the worker to the network. The difference is not just semantic – it has profound implications on the enforcement of security policies, the breadth of connectivity options, and the tools through which LANs, wireless LANs, and mobile devices must be managed.

Communication is also no longer restricted to a stand-alone service like voice. Today it must be integrated into business processes and include video, chat, and presence. A static device that makes only voice calls does not meet the needs of users who are accustomed to smartphones, tablets, and other communication devices.

### Unified Communications and the Mobile Workforce

Microsoft Lync Server 2010 ushers in a new connected user experience in which every communication is transformed into a more collaborative, engaging interaction. With its software based approach, Microsoft Lync Server 2010 provides a highly secure system that functions reliably from anywhere a user works or roams, on top of existing networking. Lync is easy to manage, less expensive to deploy and operate, and uses a single interface to unite voice communications, IM, and audio, video, and Web conferencing into a rich, context-sensitive offering.

To work effectively, Microsoft Lync needs to ride on top of a reliable, high performance, and secure networking infrastructure. One that is capable of deciphering the types of communications in motion, and then conditioning the network to securely deliver them using Quality of Service mechanisms to ensure an optimal user experience. Aruba’s 802.11n Wi-Fi solutions accomplish this task by offering connection speeds greater than 100BaseT Ethernet, enterprise-grade security, and multi-media Quality of Service (QoS). The combination of Microsoft Lync Server 2010 with Aruba’s wireless LAN (WLAN) offers significant benefits, both for employees and the corporate IT. Correctly implemented, it delivers communications wherever user’s need network access inside and outside the enterprise.

## Solution Components

### Aruba Wireless LAN

Secure and reliable mobility is the responsibility of the enterprise network, which must support a wide range of converged clients over wireless, wired, and remote access networks. Laptops and smartphones are capable of simultaneously running voice, data, and now video applications, an operating model that breaks traditional dedicated VLAN and SSID architectures. Delivering the quality of service (QoS), bandwidth, and management tools necessary to accommodate these devices on a grand scale – within a campus environment, to users on the road, and in branch offices – requires a specially tailored system design.

Microsoft Lync Server 2010 uses an encrypted signaling protocol that is highly secure but renders useless the traditional snooping mechanisms of identifying SIP signaling or the consequent real-time traffic. Thus real-time traffic is forced to be treated and processed in the same way as competing best-effort traffic, i.e., with lowest priority. The problem is exacerbated when multiple real-time and non-real-time applications run on the same client devices, like laptops and smart phones, because of the challenges of isolating and prioritizing just the real-time traffic.

Aruba’s unique fingerprinting technology can identify Lync streams in session. In addition to snooping on the SIP exchange, application fingerprinting observes the packets as they flow through the WLAN, detecting patterns that match the behavior of Lync voice and video traffic. Once identified, the packets are tagged as media traffic (Class of Service [CoS] and Type of Service [ToS] tags). The QoS tags are translated by the access point to WMM-Voice and WMM-Video to ensure that they receive appropriate over-the-air QoS.

---

Application and device fingerprinting enable the system to detect the types of traffic flows, and the devices from which they originate. The network can then be dynamically conditioned to deliver QoS – on an application-by-application, device-by-device basis – as needed to ensure highly reliable application delivery. Aruba’s integrated policy enforcement firewall isolates applications from one another to essentially create multiple dedicated virtual networks, and then allocates the necessary bandwidth for each user and application.

To ensure reliable application delivery in changing RF environments, Aruba’s Adaptive Radio Management (ARM) technology forces client devices to shift away from the noisy 2.4GHz band to the quieter 5GHz band, adjusts radio power levels to blanket coverage areas, load balance by shifting clients between access points, and even allocates airtime based on the capabilities of each client device. The result is a superb user experience without any user involvement.

These services are complemented by security systems that ensure the integrity of the network. Rogue detection, wireless intrusion and prevention, access control, remote site VPN, content security scanning, end-to-end data encryption, and other services protect the network and users at all times.

Aruba’s extensive portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to unified communications applications and services – regardless of the user’s device, location, or network. This dramatically improves productivity, lowering capital and operational costs while providing a superior uninterrupted user experience.

### **Microsoft Lync Server 2010 (Standard & Enterprise)**

Microsoft Lync 2010 enhances virtual meetings with a suite of productivity-enhancing features:

- Audio and Video Web conferencing
- Enterprise-grade voice over IP
- One-click communications
- Group chat
- Easy integration with leading PBX solutions

The Lync architecture is centered around the concept of “sites,” each of which contains Lync Server 2010 components. A typical site consists of computers running Lync software and connected together by one or more high performance, low-latency local area networks. A “central site” includes at least one Front End pool or Standard Edition server. A “branch site” is associated with a single central site whose servers deliver the Lync functionality used at the branch sites.

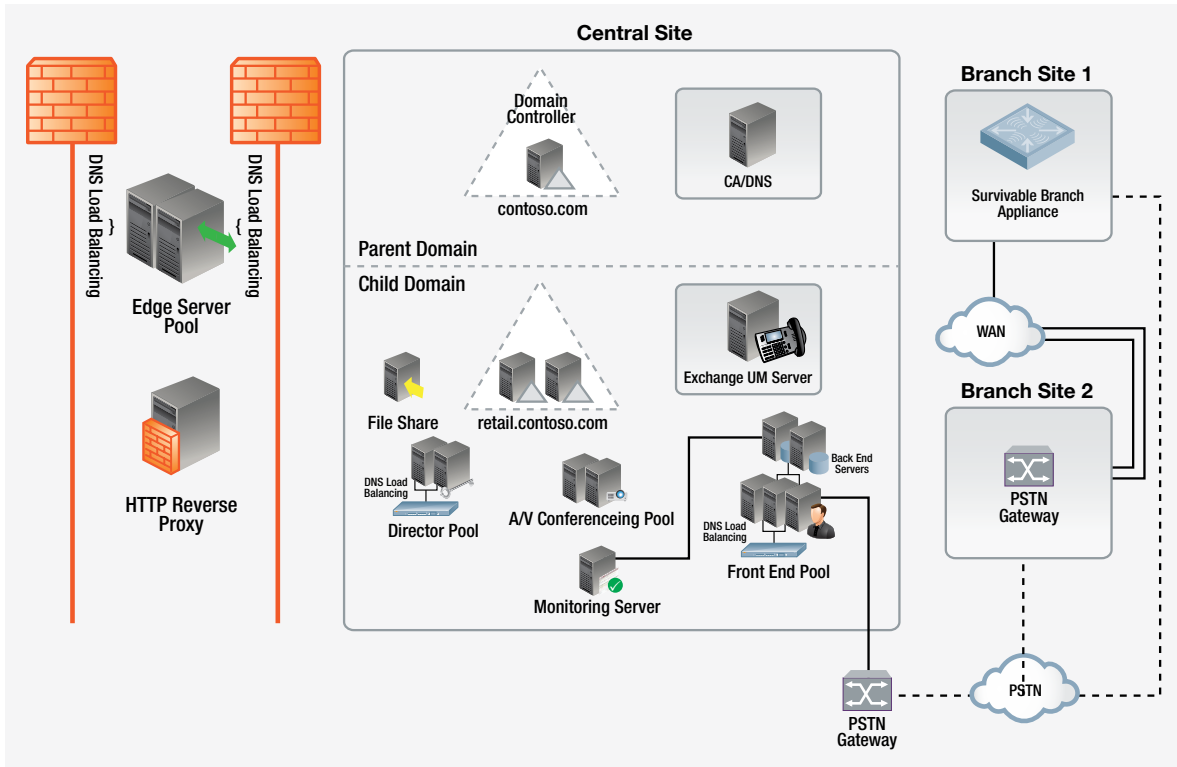
Each branch site contains either (1) an industry-standard blade server running a PSTN gateway and a Microsoft Lync Server 2010 Registrar and Mediation Server running on Windows Server 2008 R2, known as a “Survivable Branch Appliance;” (2) a server connected to either a PSTN gateway or a SIP trunk to a telephone service provider and running Windows Server and Lync Server 2010 Registrar and Mediation Server software – known as a Survivable Branch Server; or (3) a PSTN gateway and an optional Mediation Server for use in branch office with a resilient wide area network connection link to a central site.

Every deployment must include at least one central site. If branch sites are deployed then each is affiliated with one central site, which delivers to the branch those Lync services that are not otherwise available at the branch site, i.e., presence and conferencing.

Every server running Microsoft Lync Server 2010 runs one or more server roles including: Front End Server and Back End Server running basic functions and the system database; A/V Conferencing Server delivering A/V functionality; Edge Server to enable users to communicate and collaborate with user’s outside the firewall; Mediation Server for implementing voice and dial-in conferencing; Monitoring Server for collecting statistics and performance data;

Archiving Server to archive instant messages and meeting content; and Director to authenticate user requests and provide presence and conferencing services. Pools of servers running the same role can be deployed for high availability, with a load balancer used to spread traffic as necessary.

The figure below shows a typical reference topology with limited high availability. Please refer to Microsoft’s Lync documentation (<http://technet.microsoft.com/en-us/lync>) for a library of other deployment scenarios.



Source: Microsoft <http://technet.microsoft.com/en-us/library/gg425939.aspx>

## Wireless LAN Best Practices for Microsoft Unified Communications

Mobility presents a number of unique challenges for Unified Communications that are not experienced with wired networks. These challenges must be overcome to ensure an uninterrupted mobile unified communications user experience. These challenges, together with Aruba best practices solutions, are summarized below.

### Pervasive Wireless Coverage

Real-time services like voice and video are intolerant of poor RF conditions. They demand high signal levels with good signal-to-noise ratios. To support multimedia services, it is important to ensure that WLAN coverage extends pervasively to all parts of the building, with uniformly good signal levels. RF channels must be selected to avoid the interference sources that are present in every modern enterprise.

Aruba’s ARM technology continually optimizes RF coverage based on measurements of signal strength and interference reported by WLAN access points, ensuring that client devices always enjoy the high signal levels required for good voice and video performance. ARM maximizes coverage and network capacity, while avoiding interference. It is the sum of these features that optimizes voice and video quality.

---

## Managing RF Interference

Wireless interference is time varying and can arise unexpectedly. In most cases an Aruba wireless LAN will automatically adapt and mitigate the effects of interference, but sometimes that's not possible. In these cases the network needs to open a window of visibility into the RF environment, without the expense of a truck roll, to help network engineers understand what's happening. Aruba's 802.1n access points incorporate spectrum analyzers that provide on-demand monitoring, logging, and characterization of the RF environment. This feature can be enabled remotely so that a distant network engineer can assess how best to mitigate issues like continuous high level fixed frequency transmitters that can't otherwise be addressed automatically by ARM.

Wi-Fi is a broadcast medium in which over-the-air packet collisions are a fact of life. These collisions can result in dropped packets or consume bandwidth by forcing packet retransmission, both of which have detrimental effects on real-time like voice and video traffic.

ARM mitigates these issues by using band steering to redirect 5GHz-capable clients away from the congested 2.4GHz band and up to the quieter, higher capacity 5GHz band. This feature is particularly well suited for PC users running Lync since all current laptops support 5GHz operation.

## Applying Correct Priority to Mixed Voice, Video, and Data Clients

The traditional approach to enterprise VoIP has been to use a separate voice VLAN to segregate and prioritize voice traffic. This model breaks down when a Lync enabled PC or mobile device transmits both voice and data traffic. The device can belong to only a single VLAN – which should it be, voice or data?

Aruba's application-aware architecture can identify and police individual sessions from a device, dynamically prioritizing them by traffic type without need to relegate them to different VLANs. With this network intelligence, a single WLAN SSID, matched with a single VLAN, can offer full voice control and prioritization in presence of lower priority data traffic. The end result is a better user experience and less IT overhead managing VLANs.

## Performance Assurance for Encrypted Microsoft Lync Traffic

The signaling channel for Microsoft Lync is encrypted, and as a call setup and teardown cannot be easily monitored. And yet, without visibility to this information, it is difficult if not impossible to identify and prioritize real-time traffic.

Aruba's heuristics-based application fingerprinting continuously inspects UDP sessions set up over the WLAN to identify those that are RTP and carry voice or other multimedia traffic. When such streams are identified, they are automatically tagged with the correct voice priority.

## Call Admission Control

With restricted bandwidth available on the WLAN, it is important that the quality of calls in progress is not degraded as new calls and video sessions are initiated. When the call count on an access point reaches a threshold on an Aruba WLAN, Microsoft Lync clients and other voice-capable devices are automatically load-balanced with adjacent access points. While it is not possible to intercept call set-up messages because signaling is encrypted end-to-end, load-balancing can still be a very effective mechanism for holding back additional calls.

## Microsoft Lync Server 2010 Qualification

This section describes the test configuration and test cases used to test interoperability between Aruba Networks WLAN solution and Microsoft Lync Server 2010.

## Test Goals

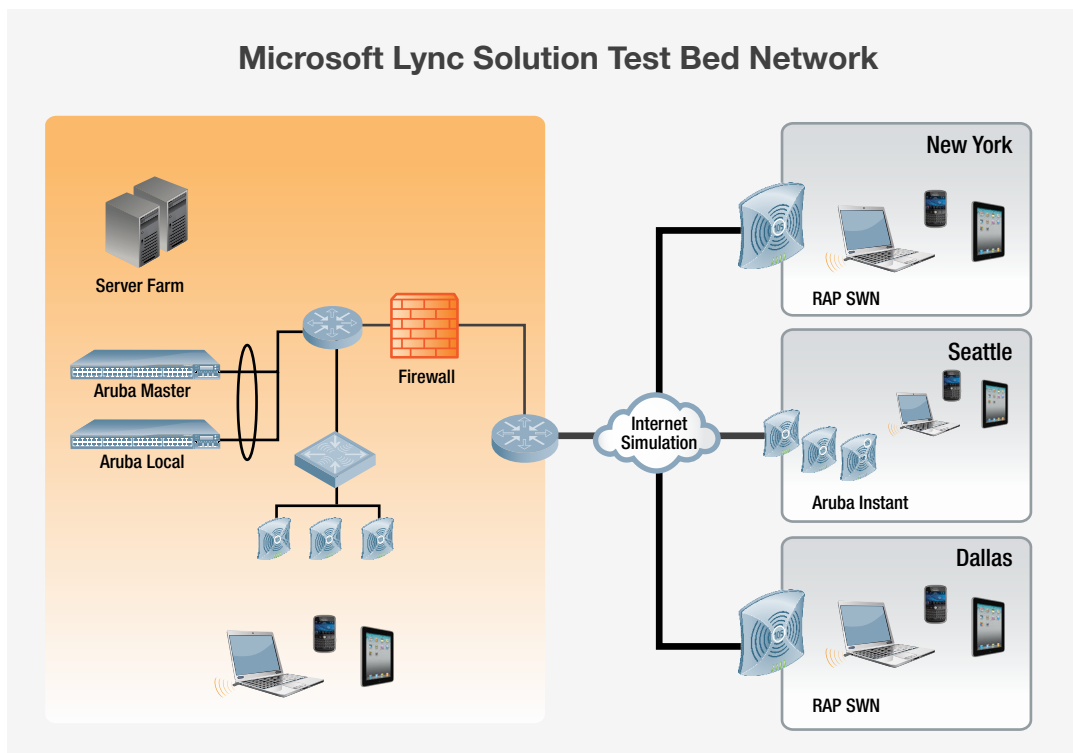
Validate the performance of typical multi-site, multimedia communications on Microsoft Lync Server 2010 operating over Aruba's wireless LAN and secure remote access platform.

## Network Topology

The topology consisted of a Main Site (Seattle), and three Branch Sites (Austin, San Francisco and New York). The sites were differentiated by the amount of delay, jitter, and packet loss introduced by the simulated Internet.

All of the servers were in a server pool and could be reached from all four sites. The branch office sites showcased the Aruba Instant and RAP-5WN solutions from Aruba. Quality and MoS scores were measured using Microsoft's Monitoring server role. The figure below illustrates the wireless network topology used to support verification testing of the Microsoft Lync solution.

## Hardware, Tools and Versions



*Microsoft Lync Solution Test Bed Network Diagram*

<p><b>Main Site</b> Seattle</p>	<p><b>Microsoft Set-up</b> Lync Server(front-end server) Lync Monitoring Server Active Directory SQL Server</p> <p><b>Aruba Set-up</b> 3600 Master Controller, AOS 6.0.1 3200 Local Controller, AOS 6.0.1 AP-105 and AP-125 Access Points connected over an L3 network AirWave Wireless Management Suite</p> <p><b>Clients</b> Polycom CX600 Desk Phones Wireless Laptops</p>
<p><b>Branch Site 1</b> New York</p>	<p><b>Aruba Set-up</b> RAP-5WN Remote Access Point</p> <p><b>Clients</b> Polycom CX600 Desk Phones Wireless Laptops</p>
<p><b>Branch Site 2</b> Austin</p>	<p><b>Aruba Set-up</b> Aruba Instant</p> <p><b>Clients</b> Polycom CX600 Desk Phones Wireless Laptops</p>
<p><b>Branch Site 3</b> San Francisco</p>	<p><b>Aruba Set-up</b> RAP-5WN Remote Access Point</p> <p><b>Clients</b> Polycom CX600 Desk Phones Wireless Laptops</p>

## Test Methodology

The three branch office links were flooded to 80% of their capacity with background data traffic to simulate an actual networking environment. A generic network simulator was used between the sites to introduce different delay and packet loss scenarios.

The interoperability tests involved simulating various network connection scenarios and testing the quality of the Lync call over the Aruba infrastructure. A Microsoft Lync Monitoring Server was used to measure call quality, the metrics including average delay, average jitter, average packet loss, and average loss. These metrics together with a manual voice quality assessment determined if the quality was acceptable or not. A call was considered acceptable if the call was clear with no feedbacks, echo, breaks, or long pauses. The quality of both voice and video calls was tested.

Two types of clients were used to generate the calls: a Polycom CX600 wired phone, and soft clients running wirelessly on Lync certified laptops.

The following call types were tested for the given scenarios:

**Call Type**

- Wireless soft client to wireless soft client – video
- Wireless soft client to wireless soft client – voice only
- Wireless soft client to wired phone – voice only
- Wired phone to wired phone – voice only
- Multi-party conference calls

**Network Scenarios**

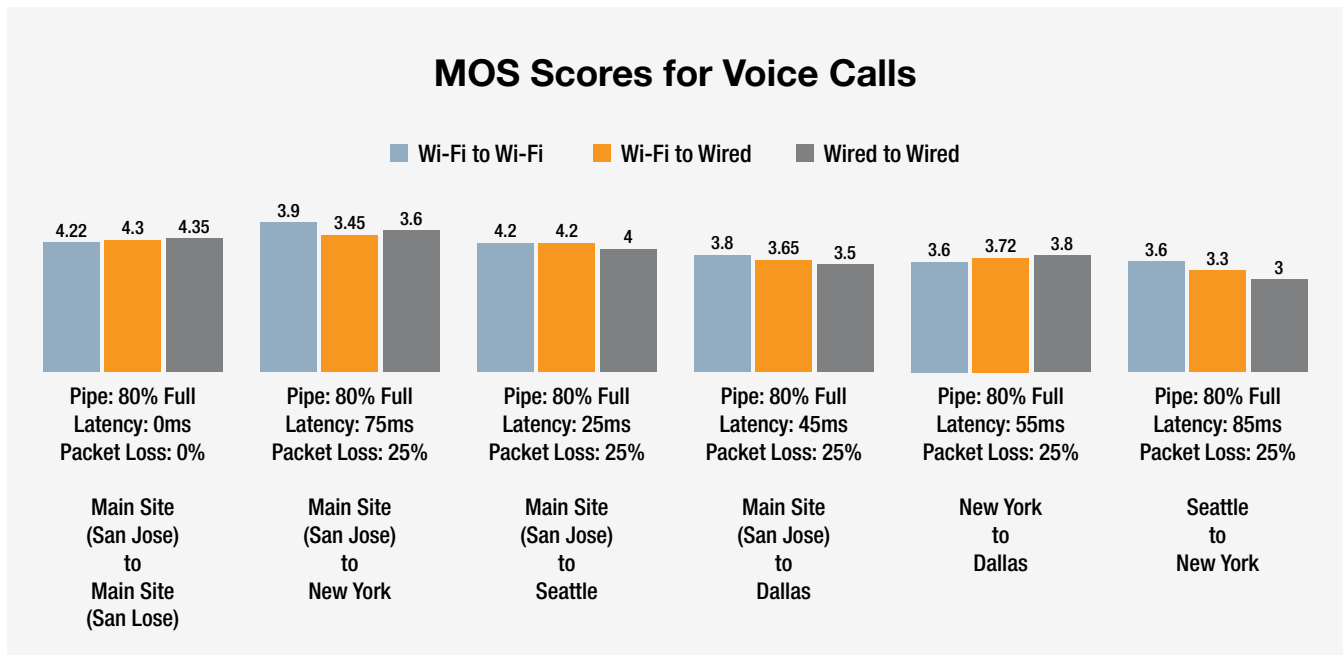
- Calls originating and terminating in the Main Site (Seattle)
- Calls origination from the Main Site (Seattle) and terminating at each of the Branch Sites
- Calls originating at a Branch Site and terminating at a Branch Site

**Summary Test Results**

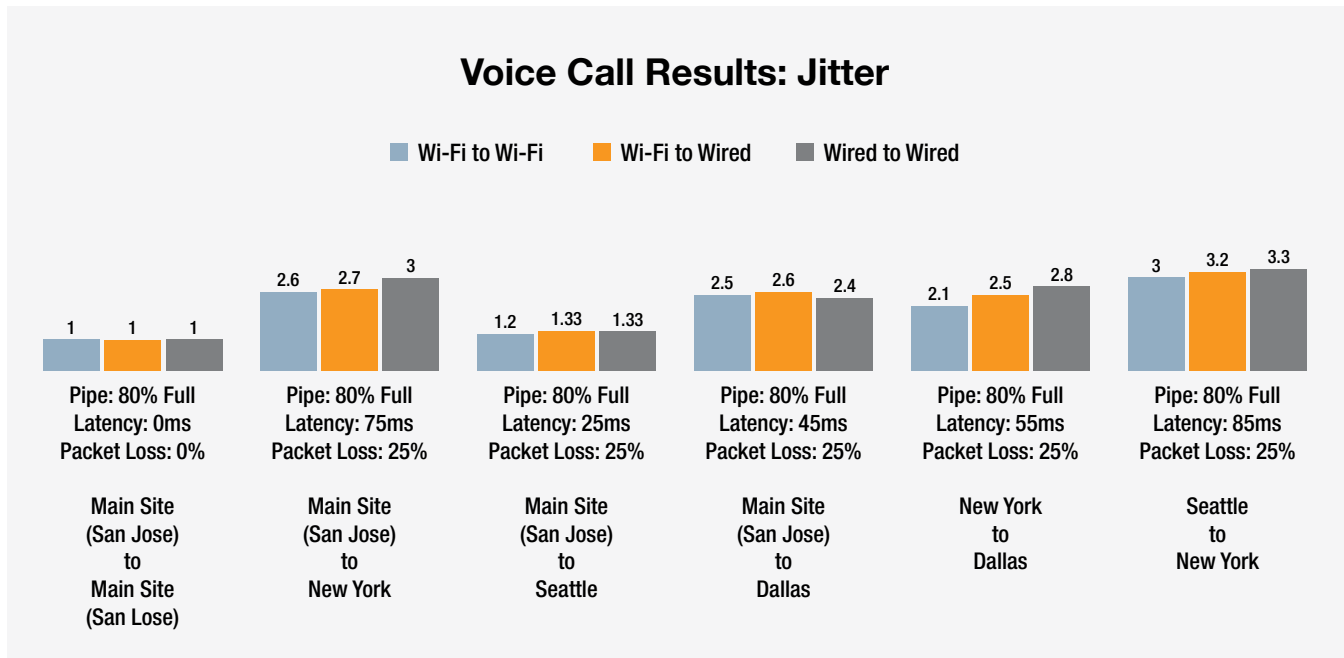
The tests of Lync on Aruba’s wireless LAN infrastructure were deemed successful by the Microsoft and Aruba verification teams. Following the recommendations in this solution guide, customers and partners are ensured a successful deployment of Microsoft Lync.

The key metric used to determine the success of the test cases is the Mean Opinion Scores (MOS) score as reported by the Lync Monitoring Server, and the manual call quality tests conducted by the verification team. A MOS score is measured on the scale of 1 to 5 with 1 being bad and 5 being excellent. For acceptable voice quality, the MOS score must be higher than 3 at all times.

The performance tests as captured in the charts below clearly show the quality of the calls to be very good even when a symmetrical delay of 85 milliseconds was introduced into the network in both directions of the link.



Similarly, jitter measurements for the same test cases are also in the acceptable range. A lower jitter number equates to better performance, and the Wi-Fi clients consistently outperform their wired counterparts.



See Appendix A for detailed test results.

## Conclusion

As the migration continues towards mobile computing and smartphones, and away from wired desk connections, a wirelessly-connected Microsoft Lync Server platform is an ideal platform through which users can stay connected with the enterprise and one another. Aruba’s wireless infrastructure is the ideal host platform for Lync: application fingerprinting identifies and prioritizes sessions without network configuration, enabling the Microsoft Lync Server to be deployed anywhere within the enterprise WLAN with service assurance.

The combination of Microsoft Lync Server and Aruba’s wireless LAN allows mobile employees to communicate more reliably, securely, and effectively over voice, video, IM, or conferencing than was ever before possible.

## References

- Aruba OS 6.0 User’s Guide
- Aruba Checklist for Planning a Voice Over Wi-Fi Network: Quality of Service
- <http://airheads.arubanetworks.com/article/checklist-planning-voice-over-wi-fi-network-quality-service>
- Microsoft Lync Getting Started Guide – <http://lync.microsoft.com/en-us/Pages/default.aspx>
- Microsoft Lync Planning Guide – <http://lync.microsoft.com/en-us/Pages/default.aspx>

## Appendix A: Detailed Test Results

	Branch	Network Condition	Scenarios	Average Jitter	Average NMOS
AUDIO	Main site (San Jose) to Main Site (San Jose)	80% pipe full 0ms latency 0% packet loss	Soft client to soft client	1	4.22
			Soft client to IP phone client	1	4.3
			IP phone client to IP phone client	1	4.35
	Main site (San Jose) to New York	80% pipe full 75ms latency 25% packet loss	Soft client to soft client	2.6	3.9
			Soft client to IP phone client	2.7	3.45
			IP phone client to IP phone client	3	3.6
	Main Site (San Jose)-Seattle	80% pipe full 25ms latency each way 25% packet loss	Soft client to soft client	1.2	4.2
			Soft client to IP phone client	1.33	4.2
			IP phone client to IP phone client	1.33	4
	Main Site (San Jose) - Dallas	80% pipe full 45ms latency each way 25% packet loss	Soft client to soft client	2.5	3.8
			Soft client to IP phone client	2.6	3.65
			IP phone client to IP phone client	2.4	3.5
	Seattle - New York	80% pipe full 85ms latency each way 25% packet loss	Soft client to Soft client	3	3.6
			Soft client to IP phone client	3.2	3.3
			IP phone client to IP phone client	3.3	3
New York - Dallas	80% pipe full 55ms latency each way 25% packet loss	Soft client to soft client	2.1	3.6	
		Soft client to IP phone client	2.5	3.72	
		IP phone client to IP phone client	2.8	3.8	
VIDEO	Main site (San Jose) - Seattle	80% pipe full 75ms latency each way 5% packet loss	VGA video quality	6.3	3.2
	Seattle - New York	80% pipe full 85ms latency each way 5% packet loss	VGA video quality	5.8	3.1

Wireless tests – wireless clients to wireless clients.

---

## Appendix B: Aruba WLAN QoS Configuration

QoS in an Aruba network is a system-level feature. Over-the-air Wi-Fi QoS is enforced using WMM, while tagging and queuing of the traffic based on traffic type is enforced by the integrated firewall engine. RF-related features like band steering, Call Admission Control (CAC), voice aware scanning, and spectrum load balancing help enforce the QoS settings for the voice and video traffic by ensuring the timely and reliable delivery of the over-the-air traffic.

At the Branch Sites, QoS is enforced by pushing the firewall and Wi-Fi settings from the master Mobility Controller to the branch office Mobility Controller, if any, and remote APs. For wired phones connected directly to wired ports on the Mobility Controller, wired QoS is achieved by applying the media classification ACL (Lync) to the wired ports

The following subsections highlight the system configurations required to ensure QoS for Lync. Please see Appendix C for the actual configuration used in Lync validation testing.

1. **Licensing Requirements:** Ensure that the firewall license is installed and enabled on the Aruba Mobility Controller. The license must be enabled in order for the Media Classification and additional QoS enforcement features to work.
2. **Adaptive Radio Management Settings:** Ensure that “Enable Adaptive Radio Management” and “Enable voice aware ARM scanning” options are selected in the active Adaptive Radio Management profile.
3. **Access Policies and User Roles:** Lync media traffic is encrypted (SIP-TLS) and the Media classify option in the ACLs should be used to prioritize the media traffic. The media classify feature works for Lync on Aruba OS releases 6.1 and higher.

Session ACL configuration for Lync

```
ip access-list session Lync
  any any tcp 5061 permit classify-media
  any any udp 5061 permit classify-media
```

Ensure that the ACL is assigned to the user role derived by the Lync clients. The ACL needs to be assigned to position 1.

Example:

```
user-role Employee
  session-acl Lync position 1
  session-acl corp-access
!
user-role Employee-Remote
  session-acl Lync position 1
  session-acl corp-access
  session-acl internet-traffic-bridged
!
```

---

Verify the settings using the command below

```
(rfi-testbox-3200) #show rights Employee-Remote
Derived Role = 'authenticated'
Up BW:No Limit   Down BW:No Limit
L2TP Pool = default-l2tp-pool
PPTP Pool = default-pptp-pool
Periodic reauthentication: Disabled
ACL Number = 62/0
Max Sessions = 65535
```

access-list List

```
-----
Position  Name          Location
-----  -
1         Lync
2         corp-access
3         Internet-traffic-bridged
```

Lync

```
---
Priority  Source  Destination  Service  Action  TimeRange  Log  Expired  Queue  TOS  8021P  Blacklist  Mirror  DisScan  ClassifyMedia  IPv4/6
-----  -
1         any     any          tcp 5061  permit                    Low                    Yes     4
2         any     any          udp 5061  permit                    Low                    Yes     4
3         any     any          any      permit                    Low                    Yes     4
```

---

## Appendix C: Aruba Mobility Controller Configuration

show running-config  
Building Configuration...

```
version 6.0
enable secret
"0078b61601db950378d3d27a33c0b4d61f95b653ce9480a229"
telnet cli
hostname "PSE-Lab.Master"
clock timezone PST -8
location "Building1.floor1"
controller config 168
ip NAT pool dynamic-srcnat 0.0.0.0 0.0.0.0
ip access-list eth validuserethacl
  permit any
!
netSERVICE svc-netbios-dgm udp 138
netSERVICE svc-snmp-trap udp 162
netSERVICE svc-https tcp 443
netSERVICE svc-dhcp udp 67 68 alg dhcp
netSERVICE svc-syslog udp 514
netSERVICE svc-l2tp udp 1701
netSERVICE svc-ike udp 500
netSERVICE svc-smb-tcp tcp 445
netSERVICE svc-pptp tcp 1723
netSERVICE svc-sec-papi udp 8209
netSERVICE svc-sccp tcp 2000 alg sccp
netSERVICE svc-http-accl tcp 88
netSERVICE svc-telnet tcp 23
netSERVICE svc-netbios-ssn tcp 139
netSERVICE svc-sip-tcp tcp 5060
netSERVICE svc-kerberos udp 88
netSERVICE svc-tftp udp 69 alg tftp
netSERVICE svc-lpd tcp 515
netSERVICE svc-http-proxy3 tcp 8888
netSERVICE svc-noe udp 32512 alg noe
netSERVICE svc-cfgm-tcp tcp 8211
netSERVICE svc-adp udp 8200
netSERVICE svc-pop3 tcp 110
netSERVICE svc-lpd-tcp tcp 631
netSERVICE svc-dns udp 53 alg dns
netSERVICE svc-rtsp tcp 554 alg rtsp
netSERVICE svc-msrpc-tcp tcp 135 139
netSERVICE svc-http tcp 80
netSERVICE svc-h323-udp udp 1718 1719
netSERVICE svc-h323-tcp tcp 1720
netSERVICE svc-vocera udp 5002 alg vocera
netSERVICE svc-http-proxy2 tcp 8080
netSERVICE svc-sip-udp udp 5060
netSERVICE svc-nterm tcp 1026 1028
netSERVICE svc-noe-oxo udp 5000 alg noe
netSERVICE svc-papi udp 8211
netSERVICE svc-natt udp 4500
netSERVICE svc-ftp tcp 21 alg ftp
netSERVICE svc-microsoft-ds tcp 445
netSERVICE svc-svp 119 alg svp
netSERVICE svc-smtp tcp 25
netSERVICE svc-gre 47
```

```
netSERVICE svc-netbios-ns udp 137
netSERVICE svc-sips tcp 5061 alg sips
netSERVICE svc-smb-udp udp 445

netSERVICE svc-cups tcp 515
netSERVICE svc-esp 50
netSERVICE svc-ipp-tcp tcp 631
netSERVICE svc-v6-dhcp udp 546 547
netSERVICE svc-snmp udp 161
netSERVICE svc-bootp udp 67 69
netSERVICE svc-msrpc-udp udp 135 139
netSERVICE svc-ntp udp 123
netSERVICE svc-icmp 1
netSERVICE svc-ssh tcp 22
netSERVICE svc-ipp-udp udp 631
netSERVICE svc-lpd-udp udp 631
netSERVICE svc-v6-icmp 58
netSERVICE svc-http-proxy1 tcp 3128
time-range night-hours periodic
  weekday 18:01 to 23:59
  weekday 00:00 to 07:59
!
time-range weekend periodic
  weekend 00:00 to 23:59
!
time-range working-hours periodic
  weekday 08:00 to 18:00
!
ip access-list session control
  user any udp 68 deny
  any any svc-icmp permit
  any any svc-dns permit
  any any svc-papi permit
  any any svc-sec-papi permit
  any any svc-cfgm-tcp permit
  any any svc-adp permit
  any any svc-tftp permit
  any any svc-dhcp permit
  any any svc-natt permit
!
ip access-list session allow-diskservices
  any any svc-netbios-dgm permit
  any any svc-netbios-ssn permit
  any any svc-microsoft-ds permit
  any any svc-netbios-ns permit
!
ip access-list session v6-icmp-acl
  ipv6 any any svc-v6-icmp permit
!
ip access-list session validuser
  network 169.254.0.0 255.255.0.0 any any deny
  any any any permit
  ipv6 any any any permit
```

```

!
ip access-list session vocera-acl
  any any svc-vocera permit queue high
!
ip access-list session v6-https-acl
  ipv6 any any svc-https permit
!
ip access-list session icmp-acl
  any any svc-icmp permit
!
ip access-list session captiveportal
  user alias controller svc-https dst-nat 8081
  user any svc-http dst-nat 8080
  user any svc-https dst-nat 8081
  user any svc-http-proxy1 dst-nat 8088
  user any svc-http-proxy2 dst-nat 8088
  user any svc-http-proxy3 dst-nat 8088
!
ip access-list session v6-dhcp-acl
  ipv6 any any svc-v6-dhcp permit
!
ip access-list session allowall
  any any any permit
!
ip access-list session v6-dns-acl
  ipv6 any any svc-dns permit
!
ip access-list session https-acl
  any any svc-https permit
!
ip access-list session sip-acl
  any any svc-sip-udp permit queue high
  any any svc-sip-tcp permit queue high
!
ip access-list session dns-acl
  any any svc-dns permit
!
ip access-list session Lync-priority
  any any tcp 5061 permit classify-media
  any any udp 5061 permit classify-media
!
ip access-list session tftp-acl
  any any svc-tftp permit
!
ip access-list session skinny-acl
  any any svc-sccp permit queue high
!
ip access-list session srcnat
  user any any src-nat
!
ip access-list session vpnlogon
  user any svc-ike permit
  user any svc-esp permit
  any any svc-l2tp permit
  any any svc-pptp permit
  any any svc-gre permit
!
ip access-list session logon-control
  user any udp 68 deny
  any any svc-icmp permit

```

```

  any any svc-dns permit
  any any svc-dhcp permit
  any any svc-natt permit
!
ip access-list session allow-printservices
  any any svc-lpd permit
  any any svc-ipp-tcp permit
  any any svc-ipp-udp permit
!
ip access-list session v6-allowall
  ipv6 any any any permit
!
ip access-list session allowall-high
  any any any permit queue high
!
ip access-list session cplogout
  user alias controller svc-https dst-nat 8081
!
ip access-list session http-acl
  any any svc-http permit
!
ip access-list session dhcp-acl
  any any svc-dhcp permit
!
ip access-list session v6-http-acl
  ipv6 any any svc-http permit
!
ip access-list session ap-uplink-acl
  any any udp 68 permit
  any any svc-icmp permit
  any host 224.0.0.251 udp 5353 permit
!
ip access-list session noe-acl
  any any svc-noe permit queue high
!
ip access-list session svp-acl
  any any svc-svp permit queue high
  user host 224.0.1.116 any permit
!
ip access-list session ap-acl
  any any svc-gre permit
  any any svc-syslog permit
  any user svc-snmp permit
  user any svc-snmp-trap permit
  user any svc-ntp permit
  user alias controller svc-ftp permit
!
ip access-list session Lync-wired-acl
  any any tcp 5061 permit classify-media
  any any udp 5061 permit classify-media
  any any svc-sip-tcp permit queue high
  any any svc-sip-udp permit queue high
!
ip access-list session h323-acl
  any any svc-h323-tcp permit queue high
  any any svc-h323-udp permit queue high
!
ip access-list session v6-logon-control
  ipv6 user any udp 68 deny
  ipv6 any any svc-v6-icmp permit

```

```

ipv6 any any svc-v6-dhcp permit
ipv6 any any svc-dns permit
!
vpn-dialer default-dialer
ike authentication PRE-SHARE changeme
!
user-role WiredLyncPhones
access-list session Lync-wired-acl
!
user-role ap-role
access-list session control
access-list session ap-acl
!
user-role data-user
access-list session allowall
!
user-role denyall
!
user-role cpbase
!
user-role default-vpn-role
access-list session allowall
access-list session v6-allowall
!
user-role Employee
access-list session Lync-priority
access-list session allowall
access-list session v6-allowall
!
user-role voice
access-list session sip-acl
access-list session noe-acl
access-list session svp-acl
access-list session vocera-acl
access-list session skinny-acl
access-list session h323-acl
access-list session dhcp-acl
access-list session tftp-acl
access-list session dns-acl
access-list session icmp-acl
access-list session Lync-priority
!
user-role default-via-role
access-list session allowall
!
user-role guest-logon
captive-portal "default"
access-list session logon-control
access-list session captiveportal
!
user-role guest
access-list session http-acl
access-list session https-acl
access-list session dhcp-acl
access-list session icmp-acl
access-list session dns-acl
access-list session v6-http-acl
access-list session v6-https-acl
access-list session v6-dhcp-acl
access-list session v6-icmp-acl

```

```

access-list session v6-dns-acl
!
user-role stateful-dot1x
!
user-role authenticated
access-list session Lync-priority
access-list session allowall
access-list session v6-allowall
!
user-role logon
access-list session logon-control
access-list session captiveportal
access-list session vpnlogon
access-list session v6-logon-control
!
!
controller-ip vlan 12
interface mgmt
    shutdown
!
dialer group evdo_us
init-string ATQOV1E0
dial-string ATDT#777
!
dialer group gsm_us
init-string AT+CGDCONT=1,"IP","ISP.CINGULAR"
dial-string ATD*99#
!
dialer group vivo_br
init-string AT+CGDCONT=1,"IP","zap.vivo.com.br"
dial-string ATD*99#
!
vlan 12
vlan 14
no spanning-tree
interface gigabitethernet 1/0
description "GE1/0"
trusted
trusted vlan 1-4094
switchport mode trunk
switchport access vlan 12
switchport trunk native vlan 12
switchport trunk allowed vlan 12,14
!
interface gigabitethernet 1/1
description "GE1/1"
trusted
trusted vlan 1-4094
switchport access vlan 12
!
interface gigabitethernet 1/2

```

```

description "GE1/2"
trusted vlan 1-4094
ip access-group Lync-wired-acl session
switchport access vlan 14
no spanning-tree
!
interface gigabitethernet 1/3
description "GE1/3"
trusted vlan 1-4094
ip access-group Lync-wired-acl session
switchport access vlan 14
no spanning-tree
!
interface vlan 12
ip address 172.25.12.3 255.255.255.0
ip helper-address 172.25.10.10
!
interface vlan 1
!
interface vlan 14
ip address 172.25.14.3 255.255.255.0
ip helper-address 172.25.10.10
!
ip default-gateway 172.25.12.2
uplink disable
ap mesh-recovery-profile cluster RecoveryHdv3qwiv6NkmANoy
wpa-hexkey!
413D4E919FB389AF2A1884E8987A106A0B862990F972D93AD41B
3F275BB8B47E
wms
general poll-interval 60000
general poll-retries 3
general ap-ageout-interval 30
general adhoc-ap-ageout-interval 5
general sta-ageout-interval 30
general learn-ap disable
general persistent-neighbor enable
general propagate-wired-macs enable
general stat-update enable
general collect-stats disable
!
crypto isakmp policy 20
encryption aes256
!
crypto ipsec transform-set default-boc-bm-transform esp-3des esp-
sha-hmac
crypto ipsec transform-set default-aes esp-aes256 esp-sha-hmac
crypto dynamic-map default-dynamicmap 10000
set transform-set default-transform default-aes
!
ip local pool "RAP Pool" 172.25.22.50 172.25.22.100
vpdn group l2tp
!
ip dhcp excluded-address 172.25.14.0 172.25.14.100
ip dhcp excluded-address 172.25.14.201 172.25.14.254
ip dhcp pool VLAN14
default-router 172.25.14.3
dns-server 172.25.20.24
network 172.25.14.0 255.255.255.0
authoritative
!
service dhcp
ip dhcp default-pool private
!
syslocation "PSE-Lab"
syscontact "Javier Urtubia"
snmp-server community PSE-Lab
vpdn group pptp
!
mux-address 0.0.0.0
adp discovery enable
adp igmp-join enable
adp igmp-vlan 0
voice rtcp-inactivity disable
voice sip-midcall-req-timeout disable
no database synchronize
database synchronize rf-plan-data
ip mobile domain default
!
ip igmp
!
no firewall attack-rate cp 1024
!
firewall cp
!
firewall cp
packet-capture-defaults tcp disable udp disable sysmsg disable other
disable
!
ip domain lookup
!
country US
aaa authentication mac "default"
delimiter colon
!

```

```

aaa authentication dot1x "ABS1-dot1x-dot1x_prof"
  termination enable
  termination eap-type eap-peap
  termination inner-eap-type eap-mschapv2
!
aaa authentication dot1x "ABS1-psk-dot1x_prof"
!
aaa authentication dot1x "apse-dot1x-dot1x_prof"
  termination enable
  termination eap-type eap-peap
  termination inner-eap-type eap-mschapv2
!
aaa authentication dot1x "apse-psk-dot1x_prof"
!
aaa authentication dot1x "default"
!
aaa server-group "ABS1-dot1x"
  auth-server Internal
  set role condition role value-of
!
aaa server-group "apse-dot1x"
  auth-server Internal
  set role condition role value-of
!
aaa server-group "default"
  auth-server Internal
  set role condition role value-of
!
aaa authentication via connection-profile "default"
!
aaa authentication via web-auth "default"
!
aaa authentication via global-config
!
aaa profile "ABS1-dot1x-aaa_prof"
  authentication-dot1x "ABS1-dot1x-dot1x_prof"
  dot1x-default-role "authenticated"
  dot1x-server-group "ABS1-dot1x"
!
aaa profile "ABS1-psk-aaa_prof"
  initial-role "authenticated"
  authentication-dot1x "ABS1-psk-dot1x_prof"
!
aaa profile "apse-psk-aaa_prof"
  initial-role "ArubaCertPSK"
  authentication-dot1x "apse-psk-dot1x_prof"
!
aaa profile "default"
  initial-role "voice"
  authentication-dot1x "default"
!
aaa profile "default-mac-auth"
  authentication-mac "default"
  mac-default-role "WiredLyncPhones"
!
aaa authentication captive-portal "default"
!
aaa authentication wispr "default"
!

```

```

aaa authentication vpn "default"
!
aaa authentication vpn "default-rap"
!
aaa authentication mgmt
!
aaa authentication stateful-ntlm "default"
!
aaa authentication stateful-kerberos "default"
!
aaa authentication stateful-dot1x
!
aaa authentication via auth-profile "default"
!
aaa authentication wired
  profile "default-mac-auth"
!
web-server
!
papi-security
!
guest-access-email
!
voice logging
!
voice dialplan-profile "default"
!
voice real-time-config
!
voice sip
!
aaa password-policy mgmt
!
control-plane-security
  no cpsec-enable
!
ids management-profile
!
ids ap-rule-matching
!
valid-network-oui-profile
!
ap system-profile "apsys_prof-jmz58"
!
ap system-profile "apsys_prof-ubb52"
!
ap system-profile "default"
!
ap system-profile "RAP-profile"
  rf-band a
!
ap regulatory-domain-profile "default"
  country-code US
  valid-11g-channel 1
  valid-11g-channel 6
  valid-11g-channel 11
  valid-11a-channel 36
  valid-11a-channel 40
  valid-11a-channel 44
  valid-11a-channel 48

```

```

valid-11a-channel 149
valid-11a-channel 153
valid-11a-channel 157
valid-11a-channel 161
valid-11a-channel 165
valid-11g-40mhz-channel-pair 1-5
valid-11g-40mhz-channel-pair 7-11
valid-11a-40mhz-channel-pair 36-40
valid-11a-40mhz-channel-pair 44-48
valid-11a-40mhz-channel-pair 149-153
valid-11a-40mhz-channel-pair 157-161
!
ap wired-ap-profile "default"
!
ap wired-ap-profile "PSE-Test-RAP"
wired-ap-enable
forward-mode split-tunnel
switchport access vlan 14
!
ap enet-link-profile "default"
!
ap mesh-ht-ssid-profile "default"
!
ap mesh-cluster-profile "default"
!
ap wired-port-profile "default"
!
ap wired-port-profile "pse_tunnel"
wired-ap-profile "PSE-Test-RAP"
no rap-backup
aaa-profile "apse-psk-aaa_prof"
!
ap mesh-radio-profile "default"
!
ids general-profile "default"
!
ids rate-thresholds-profile "default"
!
ids signature-profile "default"
!
ids impersonation-profile "default"
!
ids unauthorized-device-profile "default"
!
ids signature-matching-profile "default"
signature "Deauth-Broadcast"
signature "Disassoc-Broadcast"
!
ids dos-profile "default"
!
ids profile "default"
!
rf arm-profile "ARM-disable"
assignment disable
40MHz-allowed-bands None
no multi-band-scan
no scanning
!
rf arm-profile "default"
max-tx-power 33
min-tx-power 30
voip-aware-scan
no ps-aware-scan
!
rf arm-profile "RAP-profile-scan"
voip-aware-scan
mode-aware
scan-mode reg-domain
!
rf ht-radio-profile "default-a"
!
rf optimization-profile "default"
!
rf event-thresholds-profile "default"
!
rf am-scan-profile "default"
!
rf dot11a-radio-profile "airmonitor"
mode am-mode
!
rf dot11a-radio-profile "default"
channel 48
tx-power 50
cap-reg-eirp 3
!
rf dot11a-radio-profile "RAP-profile"
arm-profile "RAP-profile-scan"
!
rf dot11g-radio-profile "default"
no radio-enable
tx-power 3
cap-reg-eirp 3
!
rf dot11g-radio-profile "g_profile"
tx-power 3
!
wlan dot11k-profile "default"
!
wlan voip-cac-profile "default"
!
wlan ht-ssid-profile "apse-psk-htssid_prof"
!
wlan ht-ssid-profile "default"
!
wlan edca-parameters-profile station "default"
video aifsn 2 ecw-min 3 ecw-max 4 txop 94 acm 1
voice aifsn 2 ecw-min 2 ecw-max 3 txop 47 acm 1
!
wlan edca-parameters-profile ap "default"
video aifsn 1 ecw-min 3 ecw-max 4 txop 94 acm 1
voice aifsn 1 ecw-min 2 ecw-max 3 txop 47 acm 1
!
wlan ssid-profile "ABS2-psk-ssid_prof"
ssid "ABS2-psk"
wpa-passphrase "arubacert"
ht-ssid-profile "ABS1-psk-htssid_prof"
!
wlan ssid-profile "ABS3-psk-ssid_prof"
ssid "ABS3-psk"

```

```

wpa-passphrase "arubacert"
ht-ssid-profile "ABS1-psk-htssid_prof"
!
wlan ssid-profile "apse-psk-ssid_prof"
  essid "apse-psk"
  opmode wpa2-psk-aes wpa2-psk-tkip
  wmm
  wpa-passphrase "arubacert"
  ht-ssid-profile "apse-psk-htssid_prof"
!
wlan ssid-profile "default"
!
wlan virtual-ap "ABS2-psk-vap_prof"
  aaa-profile "ABS1-psk-aaa_prof"
  ssid-profile "ABS2-psk-ssid_prof"
  vlan 14
  band-steering
!
wlan virtual-ap "ABS3-psk-vap_prof"
  aaa-profile "ABS1-psk-aaa_prof"
  ssid-profile "ABS3-psk-ssid_prof"
  vlan 14
  band-steering
!
wlan virtual-ap "apse-psk-aaa_prof"
!
wlan virtual-ap "apse-psk-vap_prof"
  aaa-profile "apse-psk-aaa_prof"
  ssid-profile "apse-psk-ssid_prof"
  vlan 14
  dynamic-mcast-optimization
  dynamic-mcast-optimization-thresh 40
  band-steering
!
wlan virtual-ap "default"
!
wlan traffic-management-profile "fair-access"
  shaping-policy fair-access
!
ap provisioning-profile "default"
!
ap spectrum local-override
!
ap-group "AirMonitor"
  dot11a-radio-profile "airmonitor"
!
ap-group "Main Site"
  virtual-ap "apse-psk-vap_prof"
  enet4-port-profile "pse_tunnel"
  ap-system-profile "apsys_prof-jmz58"
  dot11a-traffic-mgmt-profile "fair-access"
  dot11g-traffic-mgmt-profile "fair-access"
!
ap-group "Branch site 2"
  virtual-ap "ABS2-psk-vap_prof"
  dot11a-radio-profile "RAP-profile"
  enet3-port-profile "pse_tunnel"
  enet4-port-profile "pse_tunnel"
  ap-system-profile "RAP-profile"

```

```

dot11a-traffic-mgmt-profile "fair-access"
dot11g-traffic-mgmt-profile "fair-access"
!
ap-group "Branch site 3"
  virtual-ap "ABS3-psk-vap_prof"
  dot11a-radio-profile "RAP-profile"
  enet3-port-profile "pse_tunnel"
  enet4-port-profile "pse_tunnel"
  ap-system-profile "RAP-profile"
!
ap-group "default"
  virtual-ap "default"
!
logging level warnings security subcat ids
logging level warnings security subcat ids-ap
logging level debugging system process stm
logging level debugging system
logging level debugging user process stm
logging level debugging user

snmp-server enable trap

process monitor log
end

```

---

## About Aruba Networks

Aruba is the global leader in distributed enterprise networks. Its award-winning portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to all corporate applications and services – regardless of the user’s device, location, or network. This dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at [www.arubanetworks.com](http://www.arubanetworks.com). For real-time news updates follow Aruba on [Twitter](#), [Facebook](#), or the [Green Island News Blog](#).



1344 Crossman Ave. Sunnyvale, CA 94089-1113  
Tel. 408.227.4500 | Fax. 408.227.4550 | 1-866-55-ARUBA  
info@arubanetworks.com | <http://www.arubanetworks.com>