

Skype for Business over Aruba

Authors:

Makarios Moussa

Scott Koster

Ashutosh Dash



Validated Reference Design

Copyright Information

© Copyright 2017 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company

Attn: General Counsel

3000 Hanover Street

Palo Alto, CA 94304

USA

Contents	3
Figures	8
Symbols	11
About this Guide	13
Acronyms	13
Scope	16
Reference Material	17
Introduction	18
SfB Overview	19
SfB Security	19
SfB Over WLAN	19
Aruba Network Optimizer	20
Supported Client Platforms	20
SfB Architecture	21
SfB Topology	21
SfB Front End Pool	22
SfB SDN Manager	22
Active Directory	22
SfB Edge Server	22
Reverse Proxy	22
Quality of Experience Server	22
SfB Network Characteristics	23
Upstream QoS	23
Client Roam Time	23
Aruba WLAN and SfB	24
Aruba Controller-Based WLAN and SfB	25
Heuristics Method	25
SfB SDN API Method	25
SDN API and ArubaOS Version Compatibility Matrix	28
Deployment Considerations with Heuristics and SDN API	29
IAPs and SfB	29

Aruba Network Optimizer	30
Open Flow Architecture	30
Single Site Deployment	30
Multisite Deployment	31
Aruba Infrastructure Configuration Guidelines	32
AP Selection and Placement Recommendations	32
Capacity Based RF Design	32
AP Placement Recommendations	33
Carpeted Office Space	33
High Ceiling and Long Corridor Spaces	34
Retail Stores	34
Conference Rooms and Large Auditoriums	35
AP Selection Recommendations	35
802.11ac AP Considerations	35
RF Considerations	35
Controller Settings	36
IAP Configuration Recommendations	36
Remote AP Configuration Recommendations	37
Authentication and Encryption Guidelines	37
High Availability Guidelines	37
Network Performance Guidelines	37
Network Topology Considerations	38
Campus Deployment Considerations	38
SfB SDN Message Flow in Controller Deployment	40
Distributed Enterprise Deployment Considerations	41
Controller Based Solution at Remote Sites	41
IAP Based Remote Deployment	42
RAP Based Deployment	43
Multisite SfB Architecture	44
Multisite Deployment with SDN API	44
Multisite Deployment with SDN API and Heuristics	45
Guest and BYOD Access Topology	45
VLAN Based BYOD Latency Challenge	46
Optimal BYOD SfB Traffic Engineering	47
Forwarding Mode Considerations	48

QoS	49
Classifying Unmarked Traffic	50
Incoming Traffic is Marked	51
Remarking Traffic to a Different Class	52
WMM and QoS	53
QoS Segments	54
QoS Considerations	55
QoS Flow	56
WMM Only Mode	57
Heuristics Mode	58
SDN API Mode	58
Wired to Wireless	59
Wireless to Wired	59
DSCP Considerations	60
DSCP-EF 46 and WMM	62
SfB on VDI	63
Scalability Considerations	64
Call Scalability Per AP Per Radio	64
SDN API Scalability	64
Aruba Solution for SfB E911	65
Network Optimizer Deployment Guidelines	66
Switch Scalability Considerations	66
Network Optimizer Use Cases	67
Instant AP	67
Wired Users	67
Network Optimizer Configuration	67
Adding SfB SDN Manager	67
Adding SfB FE Server	68
DSCP Configuration	69
Troubleshooting	71
SDN Integration Troubleshooting	71
Controller Troubleshooting	73
AP Troubleshooting	75
RF Troubleshooting	75
Wired Network Troubleshooting	76

SfB Troubleshooting Using UCC Dashboard and CLI Commands	76
UCC Dashboard	76
Call Distribution per AP and Call Quality Trend	77
Call Quality per Device and Call Quality per AP	78
WLAN Call Quality vs. Client Health Co-relation	78
End-to-End Call Quality vs. Client Health Co-relation	79
Call Detail Records	79
WLAN Call Metrics	80
End-to-End Call Metrics	80
QoS Correction	81
Per Client Troubleshooting	81
Per Client Call Quality Trend	82
CLI Commands for SfB Troubleshooting	83
UCC Troubleshooting on AirWave 8.2.1	85
UCC Dashboard	85
Call Detail Records	86
End-to-end Call Quality Analysis	86
SfB Troubleshooting on Network Optimizer	89
Session Details	89
Location Heat Map	90
Top 10 Reports	91
OpenFlow Troubleshooting	92
Appendix	93
SfB SDN API Installation and Configuration Guidelines	93
SfB Server Side Configuration	93
Configuration	93
SDN Manager Configuration	94
Dialog Listener Configuration	94
Subscriber Configuration	95
Subscriber Backward Compatibility	96
Configuring Aruba Controller for SDN API Interoperability	96
Controller Configuration for SDN API Communication	96
Configuring Aruba Controllers to Listen for HTTP (XML) Messages	96
Configuring Aruba Controllers to Listen for HTTPS (XML) Messages	97
Uploading a Certificate to the Server	99
Uploading a Root Server Certificate	99

Configuring SfB Signaling Traffic on Aruba Controller	101
Configuration Specific to ArubaOS 6.3	102
Enhancements with ArubaOS 6.4 Onwards	103
Aruba Controller Configuration for AirWave 8.x UCC Integration	104
Aruba Controller SfB Heuristics Configuration	104
Configuring the Aruba Mobility Controller to Detect SfB Traffic	104
Configuring the Aruba Mobility Controller to Detect SfB Online Traffic	105
Verifying Operation of Heuristics Detection of SfB Traffic	106
Default DSCP-WMM Mapping for Heuristics	106
Heuristics Enhancements with ArubaOS 6.4.x	106
Enable SDN API and SfB Heuristics Simultaneously	106
Dynamic Opening of Ports for SfB Voice/Video Traffic	106
Classification of SfB Voice and Video Traffic	107
Aruba Instant SfB Heuristics Configuration	107
Network Optimizer SDN API Configuration	108
ArubaOS-Switch Configuration	108
Creating QoS Policy on a Windows Client	109
Managing QoS from SfB Server through Group Edit Policy	110
Network Bandwidth Requirements for Different Codecs	110

Figure 1 Aruba Reference Architectures	17
Figure 2 SfB Network Components	21
Figure 3 Aruba Solution SfB Architecture	24
Figure 4 SfB SDN Message Flow	26
Figure 5 SfB Call Flow with SDN API	27
Figure 6 Single Site Deployment	30
Figure 7 Multisite Deployment	31
Figure 8 Coverage vs. Capacity-Based WLAN Design	33
Figure 9 AP Deployment-Honeycomb Pattern	34
Figure 10 Master Redundancy Controller Deployment	38
Figure 11 Master - Local Controller Deployment	39
Figure 12 SDN Message Flow in Controller Deployment	40
Figure 13 Branch Controller Deployment	41
Figure 14 IAP Based Branch Deployment	42
Figure 15 RAP Based Branch Deployment	43
Figure 16 Multisite SfB Architecture with SDN API	44
Figure 17 Multisite SfB Architecture with On-Premise and Office 365	45
Figure 18 VLAN Based Latency Challenge with SfB	46
Figure 19 Policy Based Routing for BYOD Devices	47
Figure 20 Classifying Unmarked Traffic	50
Figure 21 Marking Incoming Traffic	51
Figure 22 Remarking Traffic to a Different Class	52
Figure 23 QoS Segments	54
Figure 24 DSCP-WMM Mapping Configuration	55
Figure 25 QoS Flow in WMM Only Mode	57
Figure 26 QoS Flow in Heuristics Mode	58
Figure 27 QoS Flow Wired to Wireless	59
Figure 28 QoS Flow Wireless to Wired	59
Figure 29 QoS Flow with DSCP 46	60
Figure 30 DSCP 46 Consideration	61
Figure 31 DSCP EF 46 and WMM	62
Figure 32 SfB with VDI Plug-in Call Flow	63
Figure 33 Aruba SfB E911 Solution	65
Figure 34 SDN Manager Configuration	68
Figure 35 SfB FE Server Configuration	69
Figure 36 DSCP Configuration	70

Figure 37 Sfb Video Call	71
Figure 38 Sfb Sample Debug Logs	72
Figure 39 SSID Profile	73
Figure 40 Performance Dashboard	73
Figure 41 Usage	74
Figure 42 AP Debug Screen	75
Figure 43 UCC Dashboard	76
Figure 44 Call Distribution per AP and Call Quality Trend	77
Figure 45 Call Quality per Device and Call Quality per AP	78
Figure 46 WLAN Call Quality vs. Client Health Co-relation	78
Figure 47 End-to-End Call Quality vs. Client Health Co-relation	79
Figure 48 Call Detail Records	79
Figure 49 WLAN Call Metrics	80
Figure 50 End-to-End Call Metrics	80
Figure 51 QoS Correction	81
Figure 52 Per Client Troubleshooting	81
Figure 53 Per Client Call Quality Trend	82
Figure 54 show ucc trace-buffer skype4b	83
Figure 55 show ucc client-info	83
Figure 56 show ucc client-info sta	84
Figure 57 show ucc call-info cdrs	84
Figure 58 show ucc call-info cdrs detail	84
Figure 59 UCC Dashboard	85
Figure 60 Call Detail Records	86
Figure 61 Client Device	86
Figure 62 Access Point	86
Figure 63 Call Quality Summary and Call Quality Trend	87
Figure 64 End-to-end, WLAN, and Client Device Microphone Call Metrics	87
Figure 65 Client Device End Point Details and Speaker Call Metrics	88
Figure 66 In Call Quality Metrics Minute by Minute Analysis	88
Figure 67 Session Details	89
Figure 68 Location Heat Map	90
Figure 69 Top 10 Reports	91
Figure 70 Sample Top 10 Report	91
Figure 71 OpenFlow Troubleshooting	92
Figure 72 Switch CLI Output	92
Figure 73 SDN Manager Configuration	94
Figure 74 hidepii is False	94
Figure 75 Dialog Listener Configuration	95
Figure 76 Subscriber Configuration	95

Figure 77 Schema-C	96
Figure 78 Configure SfB Listening Port	97
Figure 79 Signing Request	98
Figure 80 Submit Certificate Request	99
Figure 81 Upload Certificate	99
Figure 82 Root Server Certificate	100
Figure 83 SfB Listening Port	100
Figure 84 Stateful SIPS Processing	101
Figure 85 Firewall Policies	101
Figure 86 Classify Media	102
Figure 87 CLI Classify Media	103
Figure 88 SfB on Premise Based Deployment	107
Figure 89 SfB Online Based Deployment	107
Figure 90 QoS Policy	109

The table below describes the symbols used in the figures in this guide.

Table 1: *Symbols*










Description	Symbol
Wireless Controller	
Access Point	
Layer 2 Switch	
Layer 3 Switch	
Router	

Table 1: *Symbols*

Description	Symbol
Servers/PBX	
Wired Client - Desktop Computer	
Wireless Client - Laptop	
Wireless Client - Smart Phone	

This chapter includes the following topics:

- [Acronyms on page 13](#)
- [Scope on page 16](#)
- [Reference Material on page 17](#)

Acronyms

[Table 2](#) describes the acronyms used in this guide.

Table 2: *Acronyms*

Acronym	Definition
AC	Access Category
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
ALG	Application Layer Gateways
AMP	AirWave Management Platform
AP	Access Point
API	Application Program Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AV	Audio and Video
BE	Best Effort
BK	Background
BYOD	Bring Your Own Device
CA	Certificate Authority
CDR	Call Detail Records
CLI	Command Line Interface
COS	Class of Service
CPPM	ClearPass Policy Manager

Table 2: Acronyms

Acronym	Definition
CPU	Central Processing Unit
CSR	Cell Size Reduction
DMZ	Demilitarized Zone
DNS	Domain Name System
DPI	Deep Packet Inspection
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol (EAP) over LAN
EF	Expedited Forwarding
FE	Front End
FQDN	Fully Qualified Domain Name
GRE	Generic Router Encapsulation
HD	High Definition
HTTP	Hyptertext Transfer Protocol
HTTPS	Hyptertext Transfer Protocol Secure
IAP	Instant AP
IM	Instant Messaging
IP	Internet Protocol
IPsec	Internet Protocol Security
LAN	Local Area Network
LIS	Location Information Service
MAC	Media Access Control
MOS	Mean Opinion Score
MTLS	Mutual Transport Layer Security
NAT	Network Address Translation
OKC	Opportunistic Key Caching
PEAP	Protected Extensible Authentication Protocol
PEF	Policy Enforcement Firewall

Table 2: Acronyms

Acronym	Definition
PHY	Physical Layer
PMK	Pairwise Master Key
PMKID	Pairwise Master Key Identification
PSK	Pre-Shared Keys
PSOM	Persistent Shared Object Model
PSTN	Public Switched Telephone Network
QoE	Quality of Experience
QoS	Quality of Service
RAP	Remote Access Point
RDP	Remote Desktop Protocol
RF	Radio Frequency
RSSI	Received Signal Strength Indication
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
RX Sensitivity	Receive Sensitivity
SBC	Session Border Controller
SDN	Software-Defined Networking
SfB	Skype for Business
SIP	Session Initiation Protocol
SNR	Signal to Noise Ratio
SRTP	Secure Real-time Transport Protocol
SSID	Service Set Identifier
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOS	Type of Service
TX Power	Transmit Power
UCC	Unified Communication and Collaboration

Table 2: Acronyms

Acronym	Definition
UDP	User Datagram Protocol
VAN	Virtual Application Networks
VAR	Value-Added Reseller
VDI	Virtual Desktop Infrastructure
VI	Video
VLAN	Virtual Local Area Network
VM	Virtual Machine
VO	Voice
VoIP	Voice over IP
VPN	Virtual Private Network
VRD	Validated Reference Design
WLAN	Wireless Local Area Network
WMM	Wireless Multimedia
WPA2	Wi-Fi Protected Access 2
XML	eXtensible Markup Language

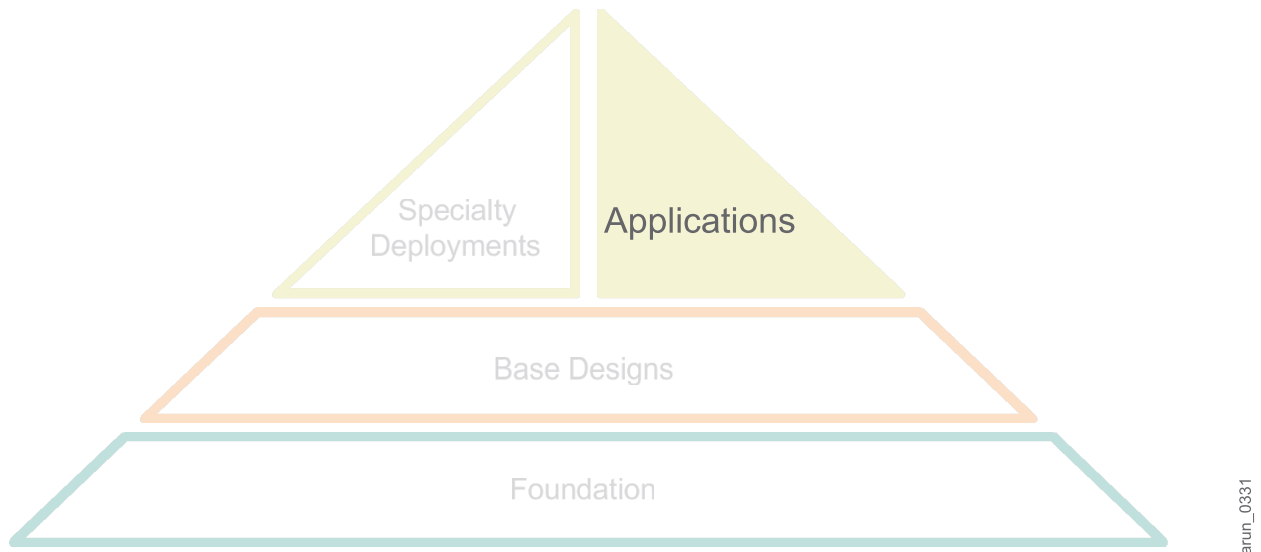
Scope

The Validated Reference Design (VRD) series focuses on particular aspects of Aruba technologies and deployment models.

Together the guides provide a structured framework to understand and deploy Aruba wireless LANs (WLANs). The VRD series has four types of guides:

- **Foundation:** These guides explain the core technologies of an Aruba WLAN. The guides also describe different aspects of planning, operation, and troubleshooting deployments.
- **Base Design:** These guides describe the most common deployment models, recommendations, and configurations.
- **Applications:** These guides build on the base designs. These guides deliver specific information that is relevant to deploying particular applications such as voice, video, or outdoor campus extension.
- **Specialty deployments:** These guides involve deployments in conditions that differ significantly from the common base design deployment models, such as high-density WLAN deployments.

Figure 1 *Aruba Reference Architectures*



This Skype for Business over Aruba VRD is considered part of the Applications guides within the VRD core technologies series.

Reference Material

This VRD will not cover the fundamental wireless concepts. Readers should have a good understanding of wireless concepts and the Aruba technology explained in the foundation-level guides.

- For information on Aruba Mobility Controllers and deployment models, see the Aruba Mobility Controllers and Deployment Models Validated Reference Design, available on the Aruba website at <http://www.arubanetworks.com/vrd>
- The complete suite of Aruba technical documentation is available for download from the Aruba support site. These documents present complete, detailed feature and functionality explanations beyond the scope of the VRD series. The Aruba support site is located at: <https://support.arubanetworks.com/>
- For more training on Aruba products, or to learn about Aruba certifications, visit the Aruba training and certification page on our website. This page contains links to class descriptions, calendars, and test descriptions: <http://www.arubanetworks.com/support-services/training-services/>
- Aruba hosts a user forum site and user meetings called Airheads. The forum contains discussions of deployments, products, and troubleshooting tips. Airheads Online is an invaluable resource that allows network administrators to interact with each other and Aruba experts. Please visit: <http://community.arubanetworks.com/>

Enterprises and institutions around the world are moving away from the wired phone technology and towards the [all wireless workplace](#). Wi-Fi connected smart phones and soft phones that support Microsoft Skype for Business (SfB) (previously known as Microsoft Lync) unified communications enhance productivity and collaboration while delivering uninterrupted mobility to users.

Listed below are the steps to deploy a SfB solution:

1. Scope the requirements.
2. Conduct a SfB mobility readiness assessment to determine if the network infrastructure is suitable. If needed, run a pilot.
3. Use only SfB qualified equipment in the actual roll out.
4. To ensure good end user experience, do not apply the appropriate tags and quality of service mechanisms if you are unable to differentiate between Instant Messaging (IM) and voice. As SfB's end-to-end encryption is ideal for security but it breaks traditional quality of service mechanisms.
5. Ensure the best possible insights into system performance for quick root cause analysis.



To resolve a problem quickly, you need to open a window in the system from the SfB client to the SfB server. If you are unable to open the window, you will be unable to analyze where the problem occurs resulting in wastage of resource and delay in the root cause analysis.

The SfB Software-Defined Networking (SDN) Application Program Interface (API) was developed to make call related data, SfB statistics, and call history information available through a single API. Aruba SfB qualified SDN API can access the SfB server and create comprehensive picture of applications, users, devices, and the Wi-Fi and Local Area Network (LAN) network infrastructure. The SfB SDN API and Aruba's network and device related data provides an end-to-end view into real-time calls, identifies fault locations and device issues, and allows you to run root-cause diagnostics from client to server. These features enable you to move away from wired Internet Protocol (IP) phones as you can deliver full SfB user mobility, enhance productivity, and workplace collaboration, resulting in cost savings from rightsizing your wired infrastructure.

This document details all aspects of Wi-Fi network engineering and design for an enterprise-wide mobile SfB deployment that includes:

- Access Point (AP) placement
- Radio Frequency (RF) design
- Network topology considerations
- WLAN configuration
- Quality of Service (QoS)
- SfB visibility
- Troubleshooting

It also discusses SfB design considerations when deploying both controller and virtual controller based Aruba Wi-Fi. Design considerations encompass the use of:

- SfB for voice
- High Definition (HD) video
- Conferencing
- Desktop sharing

- File transfers

This chapter includes the following sections:

- [SfB Overview on page 19](#)
- [Supported Client Platforms on page 20](#)

SfB Overview

Microsoft SfB is a real time communication platform based on the Microsoft SfB server and Office productivity suite. SfB is commonly deployed in enterprises that use Microsoft Active Directory and Exchange e-mail, though hosted and cloud-based SfB deployments are very common.

Listed below are the five primary SfB features:

- Voice calling - peer to peer or to/from the Public Switched Telephone Network (PSTN) through Session Border Controller (SBC)
- Video conferencing - HD quality video
- Desktop sharing - screen share and application collaboration
- File sharing - securely transfer files peer-to-peer
- Conferencing - video, voice, content sharing, file share, and dial-in-access

This section includes the following topics:

- [SfB Security on page 19](#)
- [SfB Over WLAN on page 19](#)
- [Aruba Network Optimizer on page 20](#)

SfB Security

SfB communication channels are encrypted. Server-to-server data exchange is also encrypted and authenticated using Mutual Transport Layer Security (MTLS). Each server is issued a server certificate by a trusted Certificate Authority (CA), which is then used for authentication and to exchange a symmetric key to encrypt the network session.

SfB uses Session Initiation Protocol (SIP) as the signaling protocol, which is encrypted using Transport Layer Security (TLS). Since SfB leverages a secured SIP channel, SfB IM traffic also benefits from the same TLS encryption.

Application sharing uses Remote Desktop Protocol (RDP). This TCP traffic uses TLS as the underlying transport, and authentication is established over a secure SIP channel.

Web conferencing traffic uses Persistent Shared Object Model (PSOM), which uses TLS as the underlying transport, and authentication is established over a secured SIP channel.

To prevent eavesdropping and packet rejection, Secure Real-time Transport Protocol (SRTP) uses 128-bit AES stream encryption to protect audio and video (A/V) traffic traveling to and from the SfB server. The SfB server establishes a media path that can traverse firewalls and Network Address Translations (NATs) before allowing A/V traffic to flow between two endpoints.

SfB Over WLAN

The three core design components of a SfB ready WLAN includes access to airtime, QoS, and visibility. Delay in or disruptions to the flow of SfB traffic can cause quality issues. Addressing each of the core design components in a systematic approach can help minimize latency and improve user experience.

SfB is an application that typically runs on a general-purpose device, so it is typically not feasible to dedicate Central Processing Unit (CPU) time exclusively to SfB applications. Rather the objective is to achieve coexistence of SfB and other applications while being able to prioritize SfB traffic over the air to minimize latency and improve QoS.

Best case scenarios expect that you achieve the following goals as measured peer-to-peer (local and remote), peer-to-gateway (SBC), peer-to-conference bridge:

- Round trip delay < 100 ms
- Jitter < 10 ms
- Packet loss <5%

The above parameters should be measured with load and typical background traffic ≥ 100 Mbps.

Aruba Network Optimizer

Aruba Network Optimizer SDN application automates policy deployment dynamically on a per-session basis for voice, video, and application sharing to deliver a better user experience and reduce operational costs. When a desktop sharing, voice, or video session is initiated using a Microsoft® Skype for Business client in the campus or branch office, the Skype for Business Server in the data center provides the Aruba Network Optimizer SDN Application with session details via the Skype for Business SDN API, such as source and destination IP address, protocol type, application ports, and bandwidth requirements at the start and end of every call. Network Optimizer then uses these per-session application details to dynamically provision QoS policy in a trusted manner via the Aruba Virtual Application Networks (VAN) SDN Controller using OpenFlow.

The Aruba Network Optimizer SDN Application uses the intelligence from Skype for Business Server and the Skype for Business SDN API, along with the robust capabilities of the Aruba VAN SDN controller to dynamically prioritize traffic at the edge of a network using OpenFlow. This allows the network administrator to implement consistent and trusted QoS policies across the network. All of this is done dynamically through a central point of control; eliminating the need for manual, device-by-device configuration via the Command Line Interface (CLI), which greatly simplifies policy deployment and reduce the likelihood of human errors.

In addition, the Network Optimizer displays a graphical dashboard of Skype for Business call quality metrics to provide an intuitive way to understand Skype for Business call statistics in your network. This includes the number of active sessions and peak call time, quality of experience metrics for completed calls and poor call quality analysis details to assist with monitoring and diagnosing Skype for Business call quality issues.

This document assumes that you are using a fully functional and tested Microsoft SfB deployment and have an advanced understanding of network topology and WLAN deployments.

Supported Client Platforms

SfB clients are available for the most common computing and telecommunication platforms, including:

- Desktop OS - Windows (XP, Vista, 7, 8, 10), OSX
- Mobile - iOS, Android, Windows Mobile, Windows 8 RT
- SfB room systems
- Dedicated SfB endpoints - Polycom, Snom, and so on
- Embedded applications using the SfB API

SfB Topology

SfB clients are assigned to a cluster of front end servers, called SfB front end pool. Large SfB deployments have many front end pools deployed to serve a wide geographic area. In a global deployment, SfB clients will register with their home front end servers despite their proximity to a closer front end server and this information is very useful while troubleshooting SfB issues.

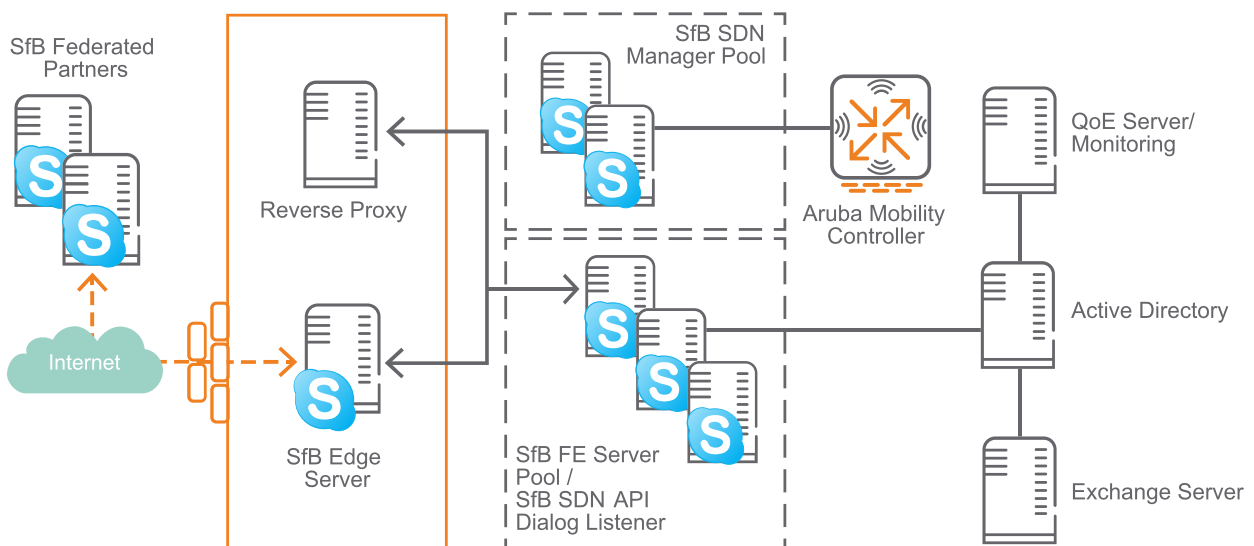


Failure to understand the distribution of SfB users to SfB front end servers in relation to the configured SDN API results in SDN API messages missed or not sent at all.

SfB is designed to traverse the public Internet without any additional components like Virtual Private Networks (VPNs) or specialized ports. The SfB client detects the public Internet that is outside the corporate network using a Domain Name System (DNS) query. When using outside network, SfB can traverse the corporate border through the SfB Edge server.

Figure 2 shows different components of the SfB network.

Figure 2 SfB Network Components



This chapter includes the following topics:

- [SfB Front End Pool on page 22](#)
- [SfB SDN Manager on page 22](#)
- [Active Directory on page 22](#)
- [SfB Edge Server on page 22](#)
- [Reverse Proxy on page 22](#)
- [Quality of Experience Server on page 22](#)

SfB Front End Pool

The front end SfB server pool performs call processing and can be pooled together with other front end servers to create a fault tolerant front end pool. Front end servers can also perform bridging or conferencing functions in the absence of a dedicated bridge. Clients connect directly to a SfB front end server to make or setup calls and communicate with other users. The front end server communicates with Aruba infrastructure using **SfB SDN API Dialog Listener** and **SfB SDN Manager**.

SfB SDN Manager

The SfB SDN Manager is a component of the SDN API architecture that acts as a collector and forwarding agent for SDN API messages. The SDN Manager receives SfB SDN messages from multiple SfB front end servers and sends these messages to Aruba Mobility Controllers. SfB SDN Managers can be deployed in a pool. Within a pool, these SDN Managers can share load and can do automatic failover in case of SDN manager failure.

Active Directory

SfB is integrated with Microsoft Active Directory. The Active Directory (AD) is the repository for SfB user credentials and also stores the SfB topology in the directory schema. SfB users are created in the AD and then enabled in the SfB server manager control panel.

SfB Edge Server

The SfB Edge server enables external users such as authenticated and anonymous remote users, federated partners, mobile clients, and users of public IM services to communicate with other users inside the SfB domain. The SfB Edge server uses port 443 to communicate to the front end pool.

Reverse Proxy

Reverse proxy is used for external discovery of a SfB front end pool assignment. Reverse proxy is required for external clients to access the SfB server web services that are on the internal network.

Quality of Experience Server

The Quality of Experience (QoE) server provides end-to-end call quality metrics for SfB calls. The QoE server is a mandatory part of the SfB SDN API integration for Aruba to get visibility to end-to-end call quality metrics. SfB clients collect data during a call and send the data to the front end server, which forwards it to the QoE server that includes a Microsoft SQL server database. The QoE server is responsible for calculating call quality metrics such as Mean Opinion Score (MOS), packet loss, jitter, and call delay. MOS represents the end-to-end call quality for SfB voice calls which ranges from 0 (worst) to 5 (toll quality).

SfB call classification and prioritization works without the QoE Server.



The SDN API plug-in on the SfB front end server will only send a MOS score if an active QoE server is installed.

SfB follows a SIP registration and call control ladder model. The SfB client uses a DNS service discovery model to determine how it will sign into SfB. When the client signs into SfB, it registers with a SfB front end server, or if it is an external network the client registers with an edge server. When a call is made, the SfB client communicates to the front end or edge server to setup the call over Transmission Control Protocol (TCP). Once the call is setup, Real-time Transport Protocol (RTP) data traffic flows between the clients or media gateways directly using User Datagram Protocol (UDP).

Listed below are the ports used for SfB communications:

- TCP 53 - SfB DNS query
- TCP 5061 - SfB clients inside a corporate network
- TCP 5063 - Used for incoming SIP requests for A/V conferencing
- TCP 443 - Used by SfB clients outside a corporate network or all online SfB clients
- UDP 3478 - Used for Session Traversal Utilities for NAT (STUN) messages. SfB clients initiate STUN connectivity check prior to media transmission. Once STUN connectivity check is succeeded, media transmission occurs.
- UDP 50000 - 65000 - Typical port range used for RTP, can be set to a specific port range on the SfB server.

This chapter includes the following sections:

- [Upstream QoS on page 23](#)
- [Client Roam Time on page 23](#)

Upstream QoS

Only Windows clients (Vista/Win7/8) are capable of performing upstream tagging of SfB RTP packets with QoS markings. Enabling upstream tagging provides significant improvement on SfB quality, to enable upstream tagging, configure a group policy. For detailed instructions, see [Managing QoS from SfB Server through Group Edit Policy on page 110](#).



Refer to the client QoS section for caveats related to upstream tagging.

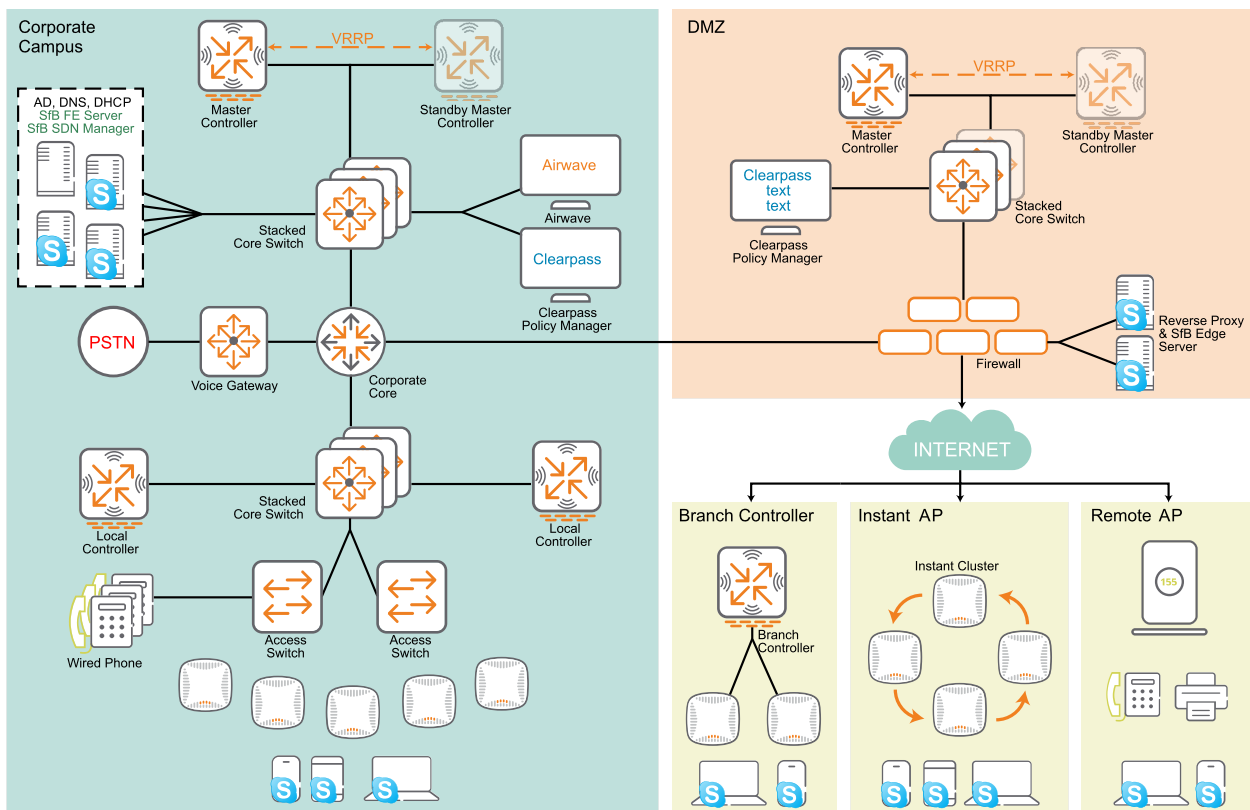
Client Roam Time

When SfB wireless clients roam from one access points to another, they might face connectivity issues. A roam interval > 200 ms results in SfB voice quality issues and causes SfB clients to disconnect and re-register with the front end server. To minimize the roaming interval, refer to configuration best practices.

Aruba controller and Instant AP (IAP) based architectures have built in Application Layer Gateways (ALG) that detect and classify different types of SfB applications. Both controller and IAP infrastructures dynamically prioritize high priority SfB traffic such as voice and video over other SfB data traffic.

The following figure provides an overview of Aruba's SfB solution architecture in controller and IAP deployments. Both campus APs and remote APs with VPN connections are supported in the controller based architecture.

Figure 3 Aruba Solution SfB Architecture



This chapter includes the following sections:

- [Aruba Controller-Based WLAN and SfB on page 25](#)
- [SDN API and ArubaOS Version Compatibility Matrix on page 28](#)
- [Deployment Considerations with Heuristics and SDN API on page 29](#)
- [IAPs and SfB on page 29](#)

Aruba Controller-Based WLAN and SfB

Listed below are the methods used by Aruba controllers to detect and classify SfB applications:

- **Heuristics method** - Is a built in method that detects SfB traffic and works with all on-premises and SfB online (Office 365) deployments. See [Heuristics Method on page 25](#).
- **SfB SDN API method** - Requires an SDN API to be installed on SfB front end servers with accurate SfB media classification. This method is currently not supported by Office 365. See [SfB SDN API Method on page 25](#).

Heuristics Method

In the heuristics method, the Aruba controller does deep packet inspection on the SfB traffic to determine SfB voice and video traffic. No changes or additional components are required on the SfB server for this classification method.

The SfB client and server sends call control signals through the Aruba controller using TCP port 5061 or TCP 443, which initiates a SfB call. This information is used to identify clients in the call and further classify and prioritize SfB media packets.

Listed below are heuristics classification methods:

- An Access Control List (ACL) is defined on the controller to listen on port TCP 5061 and 5063. The classify media option in the ACL is enabled and is mapped to a user role.
- Once SfB voice/video calls are established, SfB classify media ACL is triggered and SfB clients are marked as media capable clients.
- Any subsequent UDP dataflow with source/destination port > 1023 from/to media capable users go through SfB media Deep Packet Inspection (DPI).
- If an RTP session is based on DPI, the payload type in the RTP header is used to determine if it is a voice or video session.
- Once the media type is determined, the Type of Service (TOS) bits are set on the session. TOS mapping for the media type is configured in SSID profile.

For more details on SfB heuristics-based configuration, see [Aruba Controller SfB Heuristics Configuration on page 104](#).

SfB SDN API Method

SfB SDN API can be installed on a Lync 2010, Lync 2013 or SfB 2015 server. SfB SDN API provides an interface through which the Aruba controller can access SfB network diagnostic information for voice and video calls, desktop sharing, and file transfer. The Aruba controller uses this data to prioritize SfB traffic and provide information on the usage of SfB applications on the network. The SfB server communicates with the controller through eXtensible Markup Language (XML) messages over Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS).

SfB SDN API has several revisions over last few years. The SDN revision as of April 2016 is 2.4.1. Listed below are the SfB SDN API 2.4.1 components:

- SfB Dialog Listener installed on the SfB front end server.
- SfB SDN Manager installed on a Windows 2008/2012 server.

SfB server SDN API should be obtained directly from [Microsoft](#). For more information on SfB Dialog Listener and SfB SDN Manager installation requirements, see the installation guide.

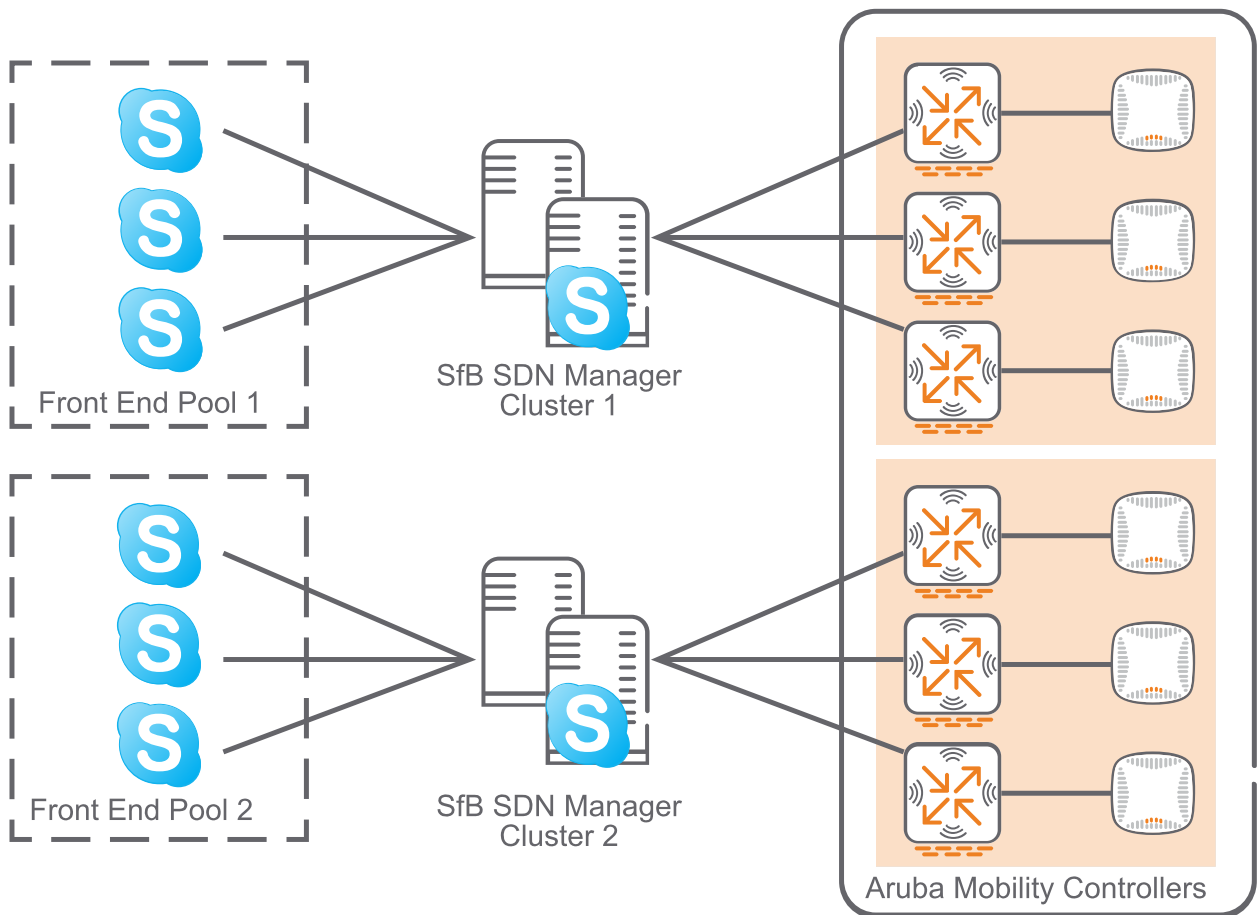


NOTE

It is critical to review the installation instructions to ensure that you meet Microsoft specific requirements before proceeding with the SDN API installation.

Figure 4 displays the SDN API message flow.

Figure 4 SfB SDN Message Flow



- SfB front end SDN API sends messages to the SDN manager.
- The SDN manager then sends messages to the Aruba controllers, where the APs terminate.

SDN API and ArubaOS Version Compatibility Matrix

Table 3 provides a compatibility matrix between ArubaOS versions and major releases of SDN API.

Table 3: SDN API and ArubaOS Version Compatibility Matrix

SDN API Version	Backward Compatibility Flag	ArubaOS Version		Highlights
		Supported	Not Supported	
2.0	TRUE	6.3.1.x 6.4.1.x 6.4.2.x 6.4.3.x 6.4.4.x	N/A	<ul style="list-style-type: none"> SDN API 2.0 can be configured to be compatible with the XML schema used in SDN API 1.2.
2.0	FALSE	6.4.3.x 6.4.4.x	6.3.1.x 6.4.1.x 6.4.2.x	<ul style="list-style-type: none"> Configuration replication issue was addressed using LSM (Lync SDN Manager). Front End (FE) servers communicated to SDN manager. SDN manager sent SDN messages to Aruba controllers. Call reporting functions were the same as SDN 1.2.
2.1	N/A	6.4.3.x 6.4.4.x	6.3.1.x 6.4.1.x 6.4.2.x	<ul style="list-style-type: none"> SDN Manager Cluster to load balance the clients and provide SDN manager redundancy. Subnet based filtering redirects SDN messages for clients to specific controllers to enhance scalability. In-call quality metrics reporting: call metrics are reported during the call.
2.2 Schema C	N/A	6.4.3.x 6.4.4.x	6.3.1.x 6.4.1.x 6.4.2.x	<ul style="list-style-type: none"> Improved filtering of messages for subscribers based on domain name, SIP trunk name etc. IPv6 support for subscriber filters. Powershell based configuration.
2.2 Schema D	N/A	6.4.4.x 6.5.x	6.3.1.x 6.4.1.x 6.4.2.x 6.4.3.x	<ul style="list-style-type: none"> Support additional fields such as stream quality etc. Powershell based configuration.
2.4.1 Schema C	N/A	6.4.3.x 6.4.4.x	6.3.1.x 6.4.1.x 6.4.2.x	<ul style="list-style-type: none"> Auto-activation of In-call QoE with installation of SfB 2016 dialog listener for all W16 clients. Per Subscriber PII Obfuscation.
2.4.1 Schema D	N/A	6.4.4.x 6.5.x	6.3.1.x 6.4.1.x 6.4.2.x 6.4.3.x	<ul style="list-style-type: none"> Same as Schema-C.

Deployment Considerations with Heuristics and SDN API

The SDN API provides additional troubleshooting and diagnostics information including end-to-end call quality metrics like MOS and real-time call quality metrics like Unified Communication and Collaboration (UCC) score. The following table provides feature support and deployment scenario comparison between heuristics and the SDN API.

Table 4: SfB Feature Support Matrix

Feature	Heuristics	SDN API
Tagging and re-tagging of Wireless Multimedia (WMM)/Differentiated Services Code Point (DSCP) values.	X	X
Classification and prioritization of SfB voice and video traffic.	X	X
Classification and prioritization of SfB desktop sharing and file transfer traffic.		X
End-to-end call quality metrics such as MOS for diagnostics and troubleshooting.		X
Co-relation between MOS score and Wi-Fi RF health metrics.		X
Real time call quality analysis using UCC score.	X	X
Co-relation between UCC score and Wi-Fi RF health metrics.	X	X
UCC dashboard for network-wide visibility and troubleshooting.	X	X
Advanced troubleshooting with detailed call statistics and reports.		X
Accurate identification of 100% of all SfB traffic.		X
UCC dashboard and diagnostics capabilities using AirWave.	X	X
Visibility into device endpoint speaker and microphone glitch rates.		X
Prioritization of Office 365/SfB Online traffic.	X	
Support for Aruba Instant AP products.	X	
Independent of SfB infrastructure.	X	

IAPs and SfB

Currently IAPs support heuristics based classification for Lync clients. IAPs can classify Lync voice and video media traffic and dynamically apply QoS for these traffic types. The procedure to classify SfB traffic using heuristics on IAPs is similar to what is described for controller based installations. Heuristics based media classification for SfB clients will be available from IAP v4.3.x.x onwards.

However, in environments with Aruba IAPs and Aruba switches with the Aruba Network Optimizer, the Network Optimizer SDN Application can apply QoS values to IAP wireless devices on the switch thus offering the majority of the SDN API benefits to IAP wireless devices.

For more information on heuristics based configuration on IAPs, refer to [Aruba Instant SfB Heuristics Configuration on page 107](#).

Open Flow Architecture

SDN applications will have varying deployment requirements. SDN applications that operate in a proactive method have more flexibility in their deployment options. Whereas, reactive SDN applications should be deployed as close as possible to the network they control. This is important to reduce the SDN control plane latency and improve the overall network performance. While HP Network Optimizer is a proactive SDN application it is beneficial, but not required, that it be deployed in the proximity of the networks it is controlling. Therefore, it may be necessary to deploy several instances of Network Optimizer to support physically separated and large scale networks.

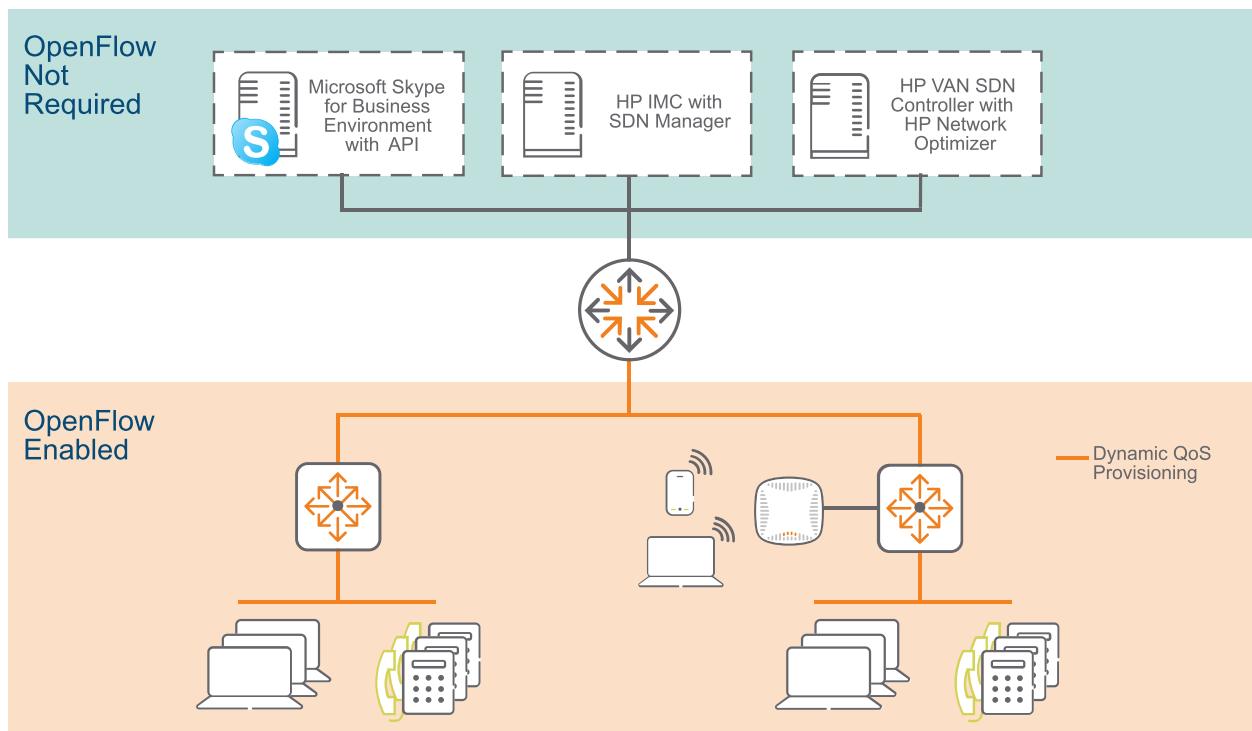
This chapter includes the following sections:

- [Single Site Deployment on page 30](#)
- [Multisite Deployment on page 31](#)

Single Site Deployment

[Figure 6](#) shows a typical deployment for a single site with less than 10,000 users.

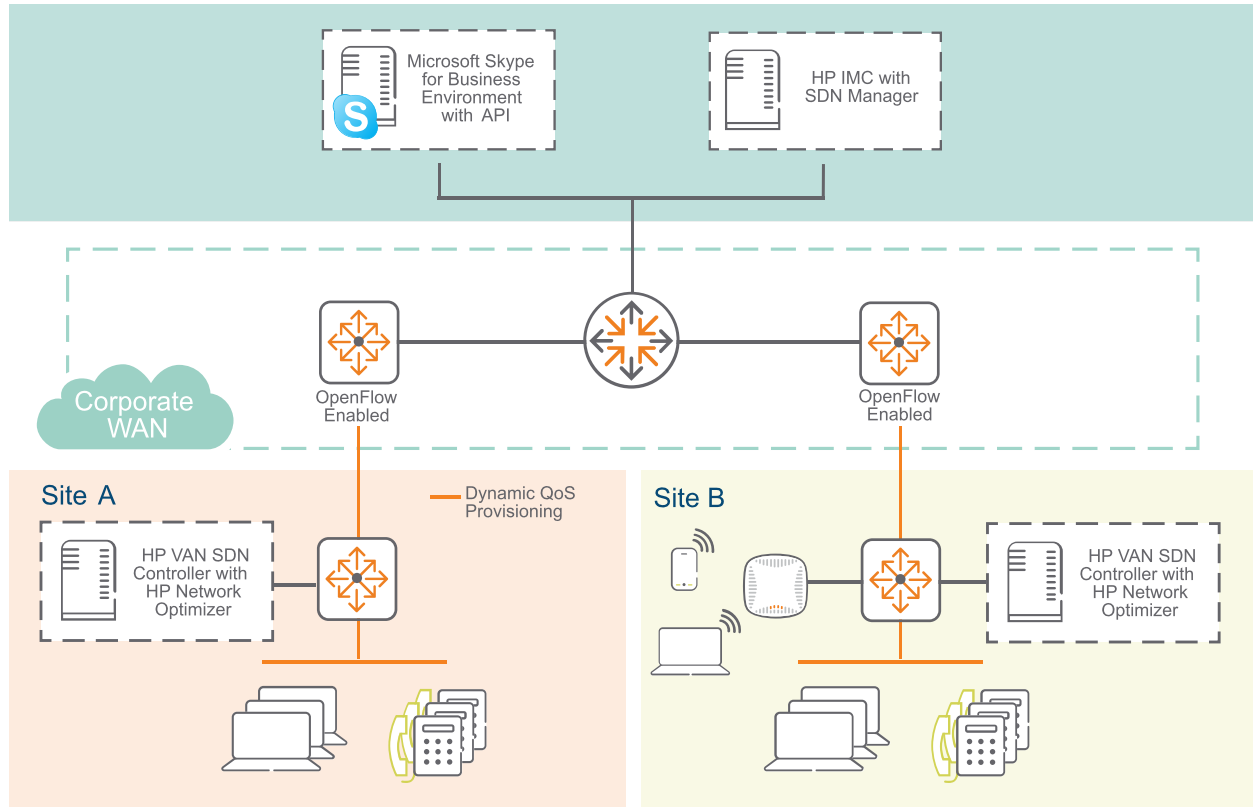
Figure 6 *Single Site Deployment*



Multisite Deployment

[Figure 7](#) shows a typical deployment with multiple sites where the HP VAN SDN Controller with HP Network Optimizer is deployed on each site. This deployment does require additional configuration. Within the configuration of Network Optimizer on each site it is necessary to define the IP address range on the other site and the address of the gateway used to reach the other site. This enables dynamic provisioning of QoS between the client and the gateway.

Figure 7 *Multisite Deployment*



If there is a single site with more than 10,000 users, it would be necessary to break up the site as if it were multiple sites.

Refer to [Network Optimizer Deployment Guidelines on page 66](#) for deployment guidelines, configuration, and troubleshooting.

Pervasive RF coverage, optimum RF signal level, and end-to-end QoS are key requirements of a SfB ready network. Sub optimal WLAN designs degrade network performance and result in poor SfB call quality. The right WLAN design ensures that SfB clients are reliably and continuously communicating with Aruba APs and IAPs. This chapter details RF considerations, including AP selection and placement, and QoS considerations required for SfB deployments. In this chapter APs and IAPs will be used interchangeably.

AP Selection and Placement Recommendations

This section provides details on the considerations and placement of APs for optimum performance.

This section includes the following topics:

- [Capacity Based RF Design on page 32](#)
- [AP Placement Recommendations on page 33](#)
- [IAP Configuration Recommendations on page 36](#)
- [Remote AP Configuration Recommendations on page 37](#)
- [Authentication and Encryption Guidelines on page 37](#)
- [High Availability Guidelines on page 37](#)
- [Network Performance Guidelines on page 37](#)

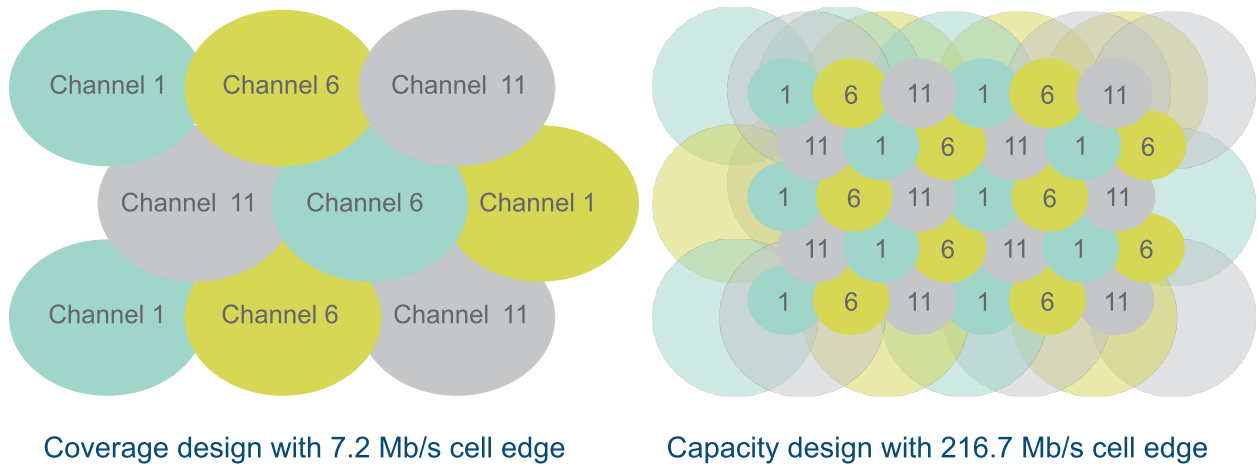
Capacity Based RF Design

Capacity based networks rely on more closely spaced APs, operating at lower Transmit Power (TX power), to deliver low-latency, high signal strength, and high bandwidth Wi-Fi to densely packed clients. By restricting the cell size this design enables clients within each cell to associate at higher Physical Layer (PHY) rates and obtain better performance. In this design the objective is to use the least number of APs, typically operating at the highest TX power, to cover the largest area at the expense of performance, latency, and client density.

The following example provides a comparison between capacity and coverage based designs in a 802.11n WLAN deployment. In the capacity based design, the clients achieve 216.7 Mbps data rate whereas in the coverage based design, clients get 7.2 Mbps data rate at the cell edge.

A capacity based network design is required to achieve optimal network performance in an enterprise SfB WLAN network.

Figure 8 Coverage vs. Capacity-Based WLAN Design



AP Placement Recommendations

This section covers AP placement recommendations for various deployment environments. AP placement is important to ensure 100% pervasive coverage. With SfB 2013 all major mobile platforms can now act as SfB clients, thus increasing the mobility of SfB users, which requires wider coverage to accommodate mobile users. This includes, office space, conference rooms, lobbies, end of hallways, stairwells, elevators, bathrooms, mechanical rooms, cafeterias, and parking garages.

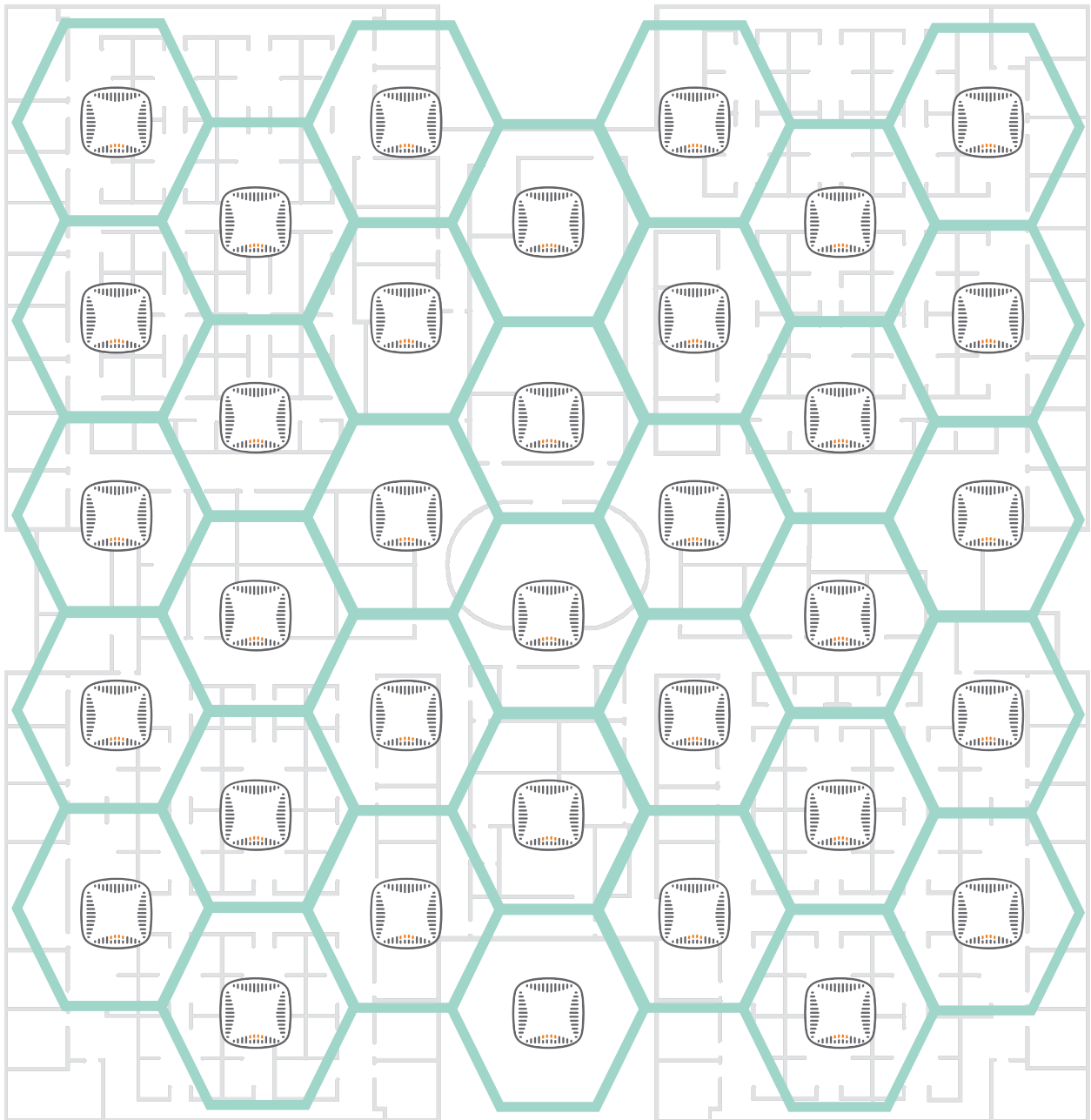
This section includes the following topics:

- [Carpeted Office Space on page 33](#)
- [High Ceiling and Long Corridor Spaces on page 34](#)
- [Retail Stores on page 34](#)
- [Conference Rooms and Large Auditoriums on page 35](#)

Carpeted Office Space

The recommended distance from the center of one AP to a neighboring AP is 50 feet. [Figure 9](#) is an example of a honeycomb pattern with 36 APs. This pattern ensures that distance is normalized along all directions to have the best coverage.

Figure 9 *AP Deployment-Honeycomb Pattern*



High Ceiling and Long Corridor Spaces

High ceilings and long corridor spaces can cause Wi-Fi signals to spread resulting in poor WLAN efficiency. If the ceiling height is 13 meters (40 feet) or less, ceiling mount is recommended. If the ceiling is higher, a wall mount or under floor installation is recommended.

Retail Stores

Both 2.4 GHz and 5 GHz frequencies can have difficulty penetrating walls, shelving, freezers, containers, and other typical obstructions in a retail setting. For environments with floor to ceiling shelving, Aruba recommends ceiling mount APs. To learn more about AP placements for retail store deployments, refer to [Indoor Site survey and planning VRD](#).

Conference Rooms and Large Auditoriums

In high-density environments with ceiling heights more than 13 meters (40 feet), wall mount or under the floor AP installation is recommended. Since these deployments have higher client density, capacity based AP network design is recommended. For more details about AP placement guidelines for large auditoriums and conference rooms, refer to the [High Density Wireless Network Design VRD](#).

AP Selection Recommendations

802.11ac AP Considerations

802.11ac is a high speed and performance next-generation Wi-Fi that is rolled out in a wide variety of client devices. 802.11ac is ideal for the high bandwidth requirements of clients running unified communications. Aruba recommends 200 Series indoor and outdoor access points that are 802.11ac based, for high performance applications.

RF Considerations

The following recommendations should be followed to ensure proper device operation for a high density SfB deployment:

- Power Settings
 - Transmit power values are 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, and 127 dbm. Consistent power level results in higher data rates. Minimum and maximum AP transmit power difference should not be more than two steps apart. For example, if the minimum transmit power is 9 dbm then the maximum transmit power should not exceed 15 dbm.
 - AP power setting should use low to moderate power. For example, in a high density AP deployment set, minimum/maximum power should be 9 -12 dbm for 2.4 GHz and 12 -18 dbm for 5 GHz.
- Disable lower transmit data rates.
 - If there are no 11b clients in the network, disable lower rates 1 - 11 Mbps.
- Set supported beacon rate to more than 12 Mbps.
 - Beacons that are transmitted at the lowest basic rate, such as 1 Mbps, can consume a considerable amount of air time. Set beacons rates higher than 12 Mbps to avoid unnecessarily consuming bandwidth.
- Minimum RF signal (Received Signal Strength Indication (RSSI)) levels of -65 dbm in 2.4 and 5 GHz.
- Minimum Signal to Noise Ratio (SNR) of 25 dB.
 - Higher signal level and high SNR are the indicators of superior RF environment and will improve client transmission rates.
- Cell Size Reduction (CSR): Reducing the cell size reduces the AP receive sensitivity, that is it shrinks the range of a client by reducing the Receiver Sensitivity (RX sensitivity) of the AP. By default CSR is disabled (0 dB). CSR can be carefully set only after consultation with an experienced engineer.
- Local Probe Request Threshold: The default value of Local Probe Request Threshold parameter is 0 and should be adjusted only by the engineer after a careful analysis. This value is recommended not to be higher than 10.
- Mitigate interference sources, such as microwave ovens, distributed antenna systems, and game consoles.
- Use both 2.4 GHz and 5 GHz bands.
- Use 20 MHz channel bandwidth on 2.4 GHz.
- 40 MHz or less channel bandwidth on 5 GHz.
 - It is recommended that high density deployments use 40 MHz or less channel bandwidth to reduce adjacent and co-channel interference. Using 80 MHz channel bandwidth in high density AP deployment may result in adjacent or co-channel interference.

Controller Settings

- Broadcast Filter Address Resolution Protocol (ARP)
 - Is enabled on the virtual AP profile and all broadcast ARP requests are converted to unicast and sent directly to the client instead of flooding the network with broadcast ARP packets. Sending broadcast packets at higher unicast data rates improves transmission.
- Service Set Identifier (SSID) profile
 - Set maximum retries to 8 to limit the re-transmission of packets to a total of 8 attempts.
 - Configure QoS settings (DSCP-WMM mapping on the SSID profile) to match QoS settings on the wired network and any upstream QoS settings on the client. This ensures that the same DSCP values are used throughout the wireless and wired network for SfB voice/video traffic.
- Adaptive Radio Management (ARM) profile
 - Enable voice/video aware scan to prevent APs from conducting off channel scans during a SfB voice or video call.
 - Enable client match to provide dynamic spectrum load balancing and dynamic band steering. Client match continuously scans the wireless environment and steers clients to the best available AP. This helps address sticky clients that remain associated with a non-optimal AP, often a distant one, because the client driver does not roam correctly.
- Enable Opportunistic Key Caching (OKC) for 802.1x authentication in the 802.1x profile to assist client roaming. OKC reduces the number of frames sent during authentication and is supported only on Windows devices and a few Android devices, but is not supported on Apple OSX or iOS devices.
- Enable validate pmkid so that the controller looks for Pairwise Master Key Identification (PMKID) in association or re-association requests from the client, indicating that the client supports OKC or Pairwise Master Key (PMK) Caching. This configuration is essential if there are devices that do not support OKC, such as Apple OSX or iOS devices. If this option is not enabled, 802.1x authentication is initiated. Apple OSX and iOS devices do support PMK caching.
- Enable Extensible Authentication Protocol (EAP) over LAN (EAPoL) rate optimization to ensure that APs send EAPoL frames at the lowest possible rates, thereby avoiding authentication delay due to packet retransmission.



OKC is only supported on Windows devices and a few Android devices. For Apple OSX or iOS devices where OKC is not supported, use PMK Caching or 802.11r.

IAP Configuration Recommendations

Listed below are RF best practices for IAPs. For a detailed explanation of these parameters refer to the controller [Aruba Infrastructure Configuration Guidelines on page 32](#) section.

- 100% coverage in all areas of SfB is in use.
- Capacity based RF network design.
- Minimum RF signal (RSSI) levels of -65 dBm.
- Minimum SNR of 25 dB.
- Enable Client Match in the ARM configuration.
- Broadcast Filter ARP enabled.
- Local probe request threshold should be adjusted only by the engineer after a careful analysis. This value is recommended not to be higher than 10.
- Traffic shaping ensures that voice and video packets are processed and only background and best effort traffic is modified to preserve SfB quality. These settings can be modified in WLAN settings under Advanced options. Adjust the voice and video percentages based on the expected voice/video traffic in your environment.

Remote AP Configuration Recommendations

Remote Access Points (RAPs) are intended for use at remote sites and to setup an Internet Protocol Security (IPsec) VPN tunnel for secure communications. RAPs support heuristics based SfB classification in Tunnel and D-Tunnel modes only. SDN API based SfB classification is supported in Split Tunnel, Tunnel, and D-Tunnel modes. Select and configure the appropriate forwarding mode for your application.

Authentication and Encryption Guidelines



Ensure that latency and jitter intervals are minimum during authentication/re-authentication process.

To maximize security, 802.1x with Advanced Encryption Standard (AES) is the preferred authentication/encryption method over Wi-Fi protected access 2 pre-shared keys (WPA2-PSK). For 802.1x based authentication, ensure that OKC or PMK caching is enabled for faster authentication.

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) certificate based authentication is preferred over Protected Extensible Authentication Protocol (PEAP) authentication as it reduces delays introduced with password authentication through Active Directory. For networks in which the Certificate Authority is separate from Active Directory, the EAP-TLS authentication request is processed on the Clear Pass server, for example, when Aruba ClearPass Policy Manager (CPPM) is used. PEAP transactions require CPPM to send the password authentication request to the Active Directory server which delays the authentication process.

High Availability Guidelines

In a multi-controller based architecture, ensure that AP fast failover is enabled for hitless failover in case of a controller failure. With AP fast failover, access points will not go down but SfB clients will be de-authenticated and re-associated. For example, if there are two controllers in the network and the SfB clients are associated to an AP on controller-1 and if controller-1 fails, SfB clients are re-authenticated to controller-2 and SfB calls in process are initiated again and new SfB session entries are created based on call re-initiation.



By default IAP virtual controllers support hitless failover.

Network Performance Guidelines

Ensure your deployment meets the following conditions to achieve optimum network performance:

- Ensure that the same QoS tagging is configured and validated across all wired switches/routers and in end-to-end wireless infrastructure. Ensure that APs are included in QoS trust to enable upstream markings.
- Round trip delay < 100 ms between clients.
- Jitter < 10 ms.
- Packet loss < 5%.
- Configure QoS trust on all voice ports to honor the QoS markings.

This chapter describes the SfB deployment design considerations for controller-based campus deployments, branch office deployments, and multisite SfB deployments. The design consideration explains how a SfB network is tailored for each scenario.

This chapter includes the following sections:

- [Campus Deployment Considerations on page 38](#)
- [SfB SDN Message Flow in Controller Deployment on page 40](#)
- [Distributed Enterprise Deployment Considerations on page 41](#)
- [Multisite SfB Architecture on page 44](#)

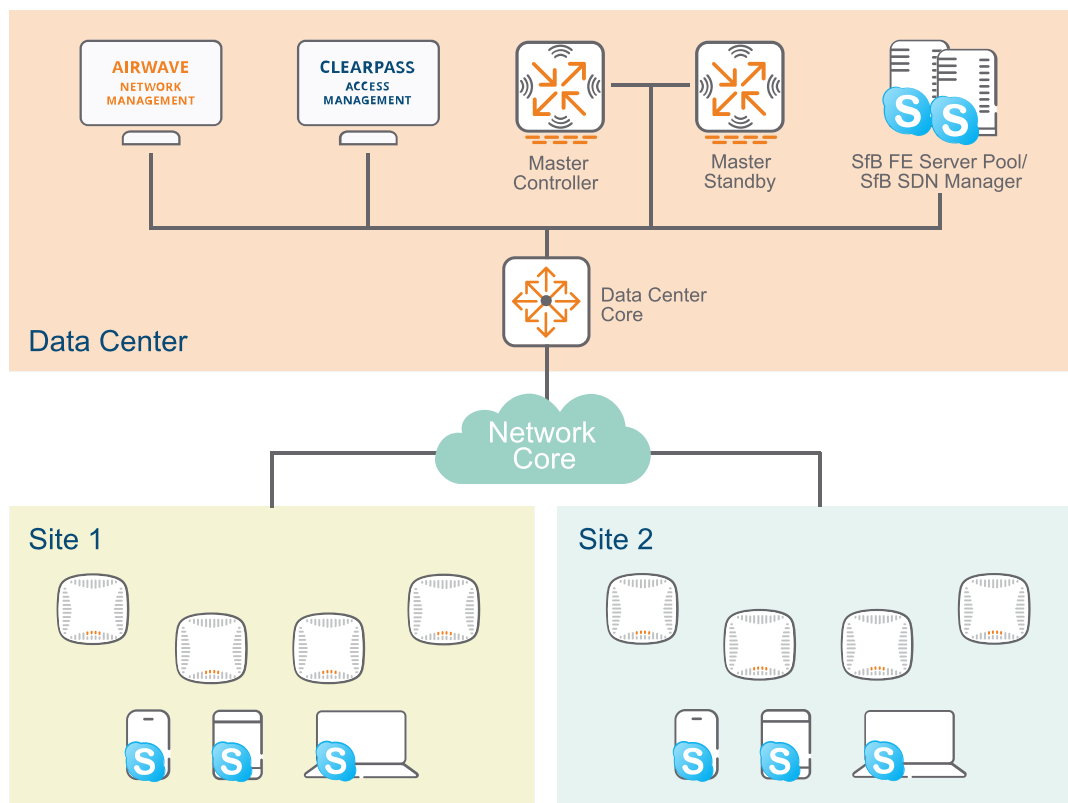
Campus Deployment Considerations

In a campus deployment, controllers can be deployed in either of the following modes:

- **Master Redundancy Deployment** - All the APs terminate on the master controller. This deployment is best suited for a small to medium campus environment. Both heuristics and SDN API-based SfB classifications are supported in this deployment model. For SfB SDN deployments, the SfB SDN manager configuration is pointed to the controllers in the network.

For more information on different traffic forwarding mode considerations, see [Forwarding Mode Considerations on page 48](#).

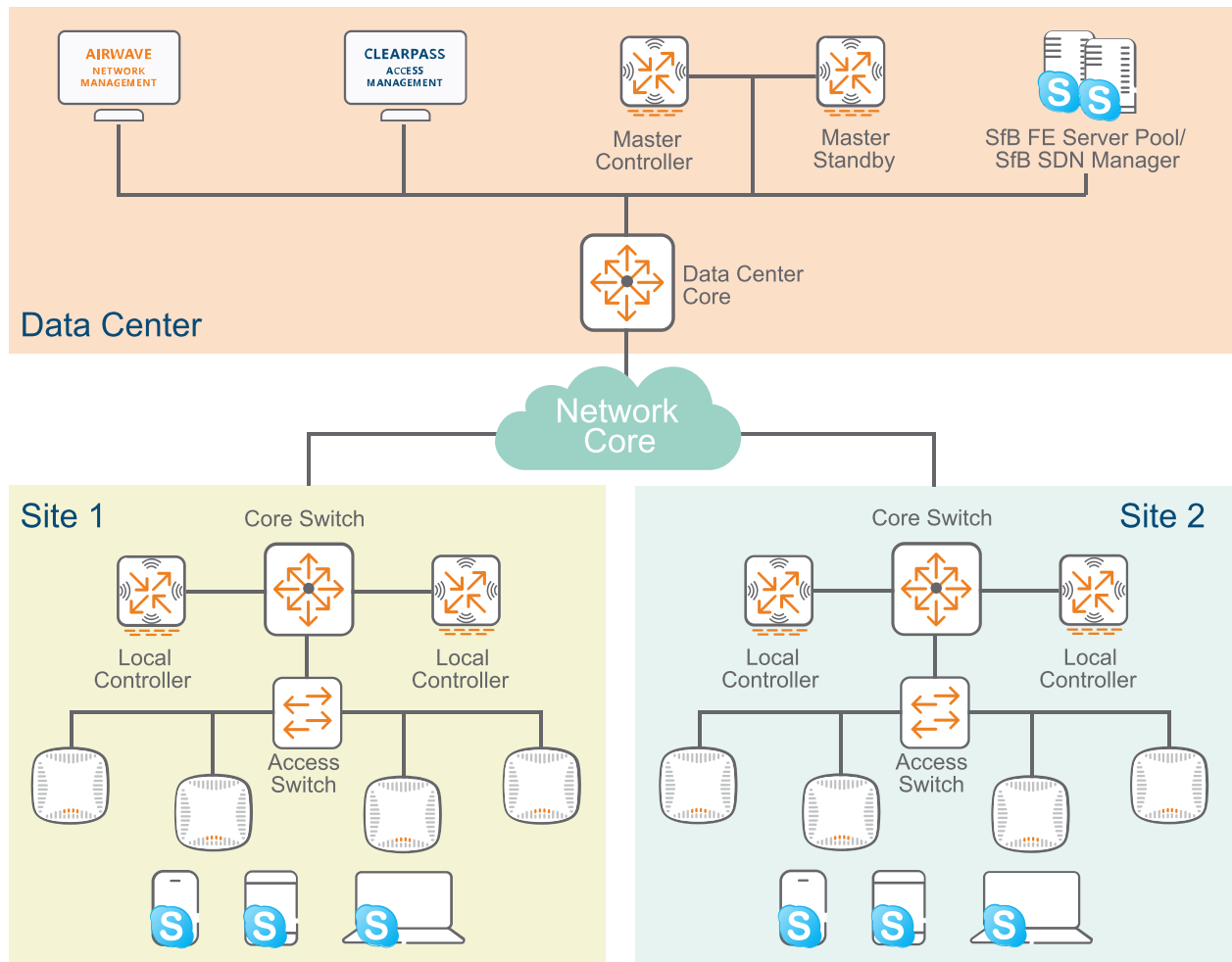
Figure 10 Master Redundancy Controller Deployment



- **Master-Local** - This deployment is designed to handle large campuses, in which APs in close proximity terminate on multiple local controllers. APs terminate on local controllers with a master controller that coordinates the RF domain and configuration across all local controllers. Both heuristics and SDN API based SfB classifications are supported in this deployment model. For SfB SDN deployment, the SfB SDN manager must be configured to send SDN API messages to all local controllers.

Refer to [Forwarding Mode Considerations on page 48](#) for additional details on different traffic forwarding mode considerations.

Figure 11 Master - Local Controller Deployment

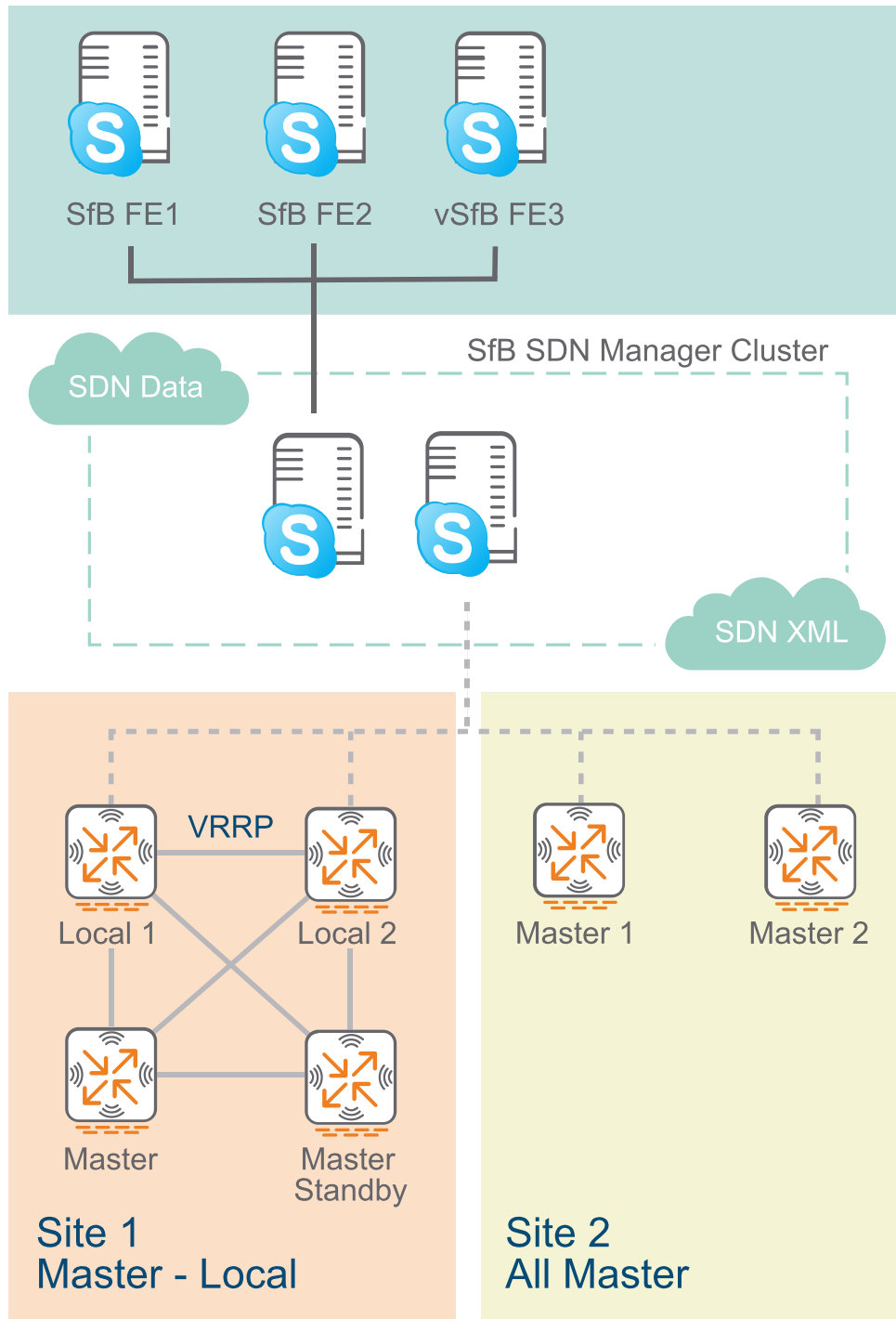


SfB SDN Message Flow in Controller Deployment

[Figure 12](#) below displays the SfB SDN message flow between the SfB Dialog Listener, SfB SDN Manager, and Aruba controllers. SDN messages are sent to the controllers on which the APs terminate.

In a master local deployment, the SfB SDN manager sends SDN messages in XML format to the local controllers on which the APs terminated. In an all master deployment, master controllers terminate the APs, therefore SDN manager sends SDN messages to the master controllers.

Figure 12 SDN Message Flow in Controller Deployment



Distributed Enterprise Deployment Considerations

Secure communication protocols over the Internet allows most of the organizations to adopt distributed enterprise model, with multiple offices/locations spread across a specific geographic region or across the globe. Examples of distributed enterprise include retail chains, healthcare clinics, government offices, restaurant, hospitality chains, and distributed enterprises with branches and home offices.

Different organizations have different solution requirements. For example, a retail chain might require a distributed network that supports everyday business operations and guest services, whereas a financial institution requires remote employee access. The ideal distributed enterprise network must be cost effective and satisfy all the business use cases without compromising on security, scalability, ease of deployment, or manageability. Aruba can meet all these objectives using the following deployment models:

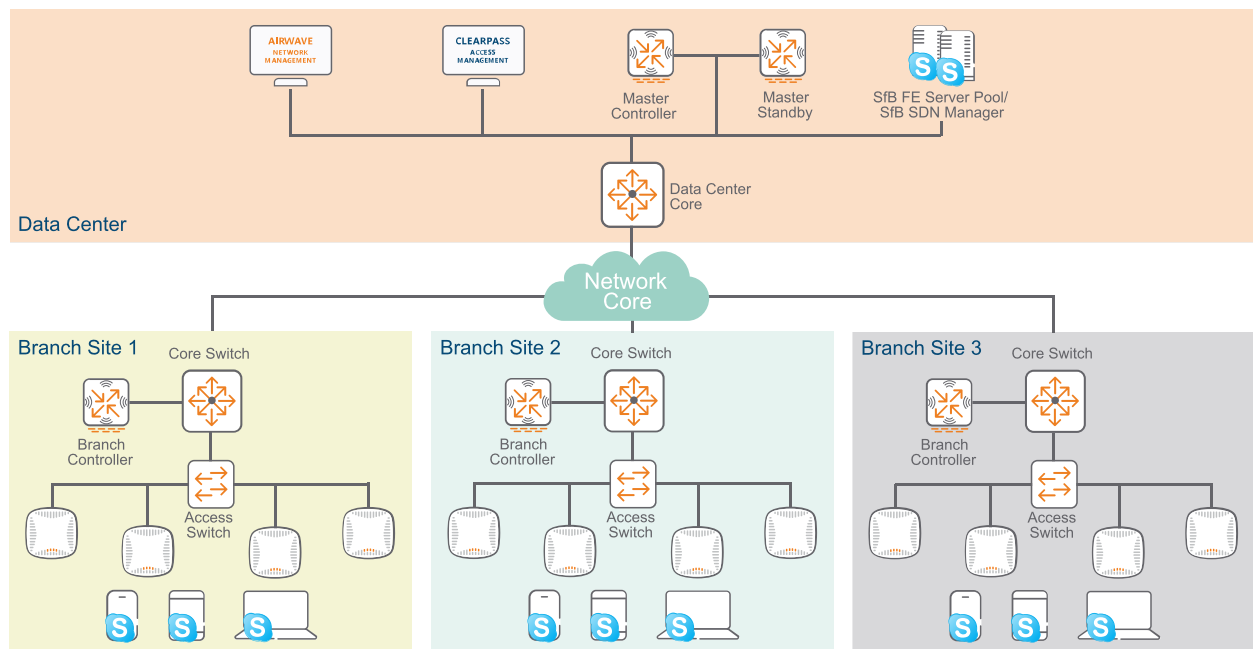
- [Controller Based Solution at Remote Sites on page 41](#)
- [IAP Based Remote Deployment on page 42](#)
- [RAP Based Deployment on page 43](#)

Controller Based Solution at Remote Sites

In this scenario, controllers are deployed at each remote branch and SfB servers are deployed at the data center. This deployment model is ideal for large distributed enterprises.

SfB SDN API and heuristics based classification are supported in this deployment. Refer to [Forwarding Mode Considerations on page 48](#) for additional details on different traffic forwarding mode considerations.

Figure 13 Branch Controller Deployment

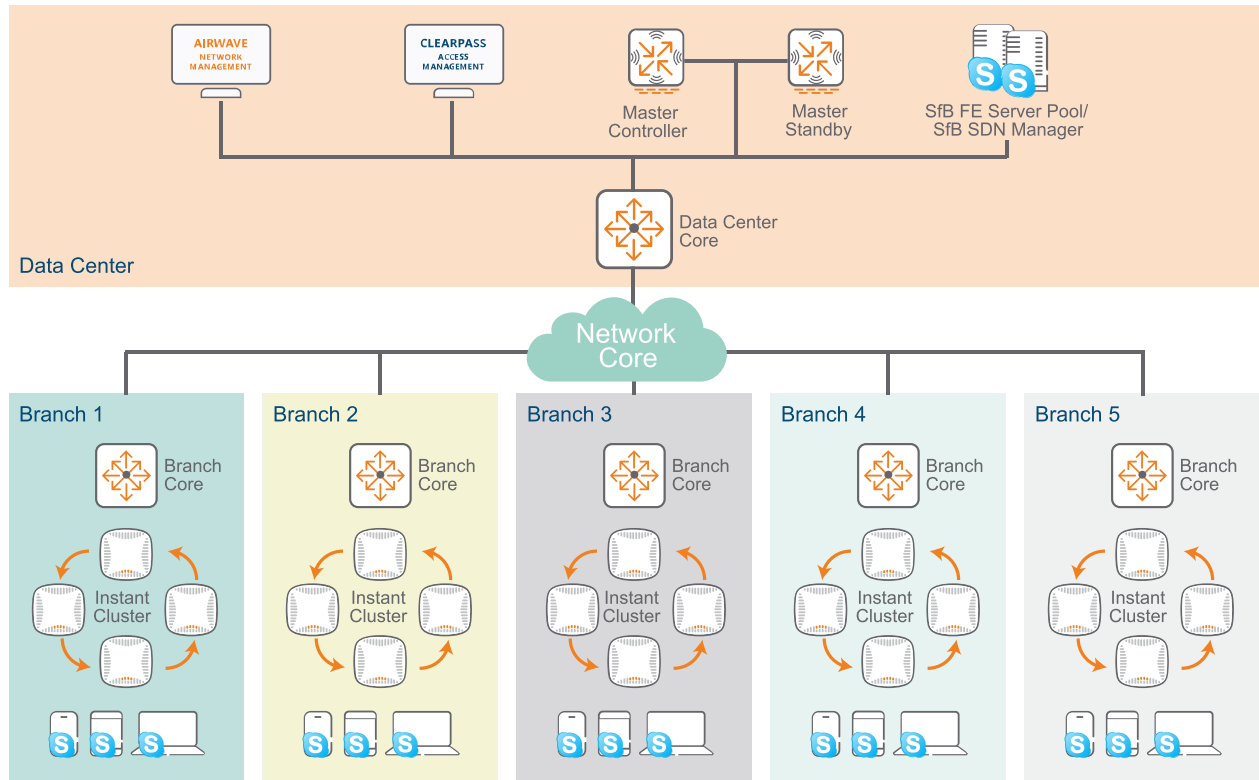


IAP Based Remote Deployment

IAPs are used on board virtual controllers to deliver enterprise grade security, resiliency, and SfB heuristics. The SfB server pool can be deployed in the data center and IAPs in the remote branch sites, this is ideal for a large or medium size distributed enterprise types of deployments.

Only SfB heuristics based classification is supported in this deployment.

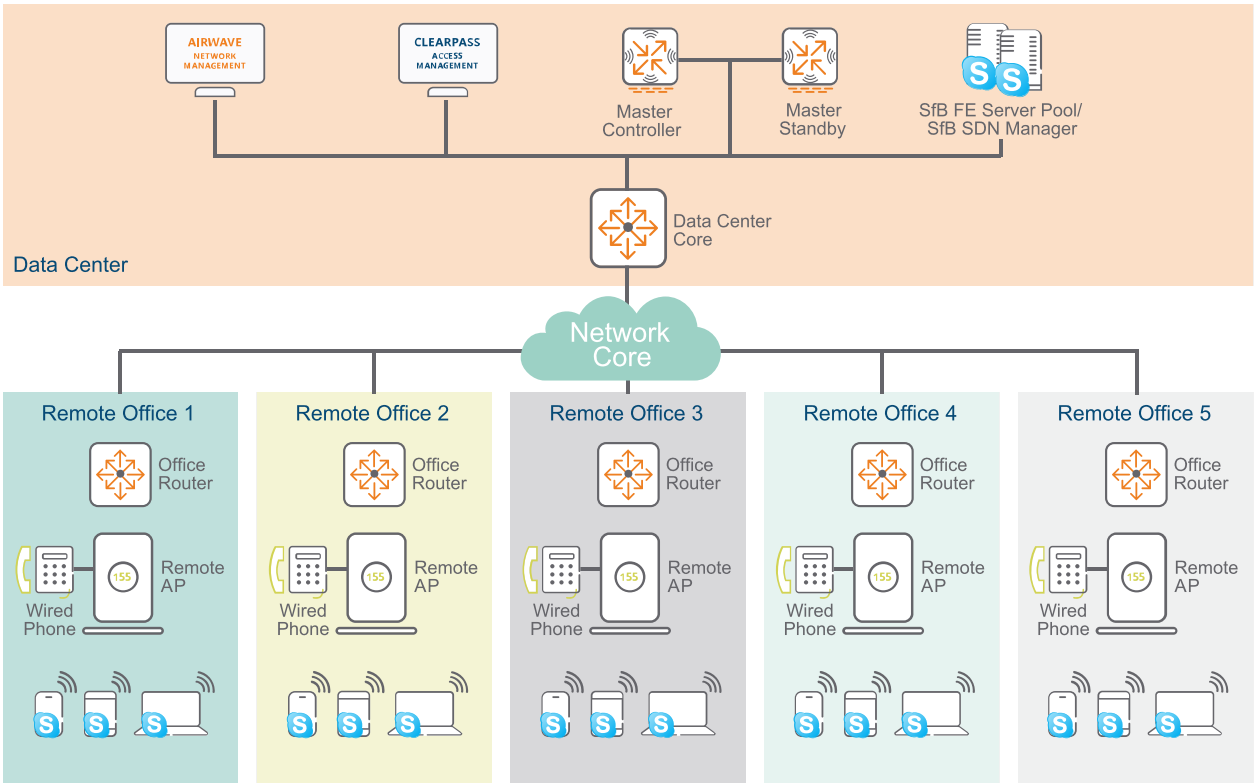
Figure 14 IAP Based Branch Deployment



RAP Based Deployment

SfB SDN API and heuristics based classification are supported in RAP deployments. Refer to [Forwarding Mode Considerations on page 48](#) for additional details on different traffic forwarding mode considerations.

Figure 15 RAP Based Branch Deployment



Multisite SfB Architecture

A multisite SfB architecture is commonly deployed at large enterprises with multiple office locations. The architecture can be divided into two types:

- **Multisite deployment with SDN API** is suitable for on premise SfB deployments.
- **Multisite deployment with SDN API and heuristics** is deployed on sites that have both on premise and Office 365 SfB solutions.

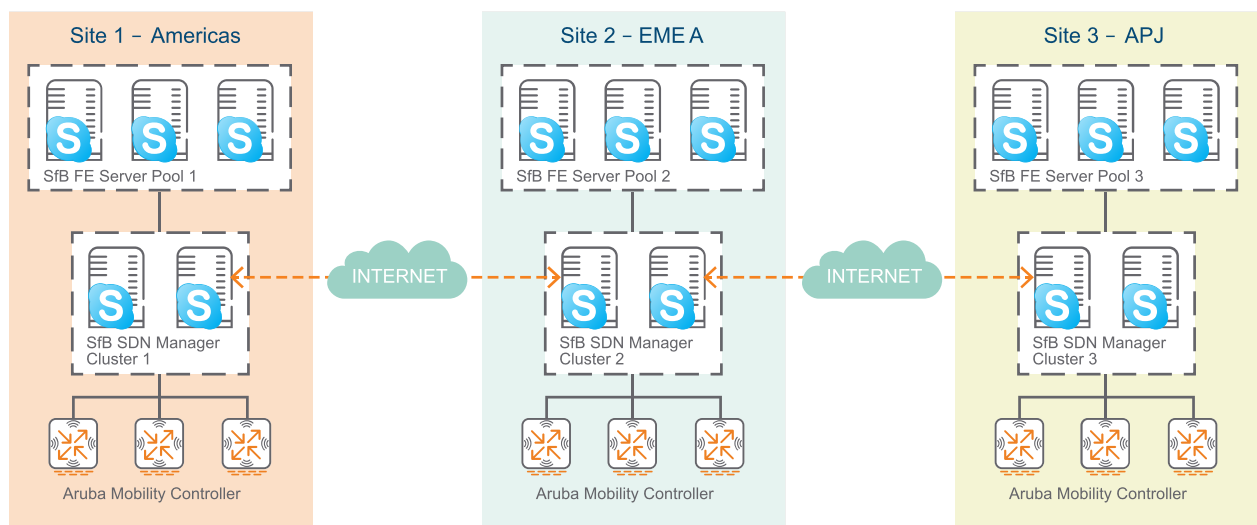
This section includes the following topics:

- [Multisite Deployment with SDN API on page 44](#)
- [Multisite Deployment with SDN API and Heuristics on page 45](#)
- [Guest and BYOD Access Topology on page 45](#)

Multisite Deployment with SDN API

In [Figure 16](#), the SfB deployment is divided into three sites, with one SDN manager pool per site, assigned to the regional SfB FE server pool. The SDN manager is configured to communicate with all Aruba controllers in that region.

Figure 16 Multisite SfB Architecture with SDN API



The following guidelines should be applied to multisite architectures with SDN API:

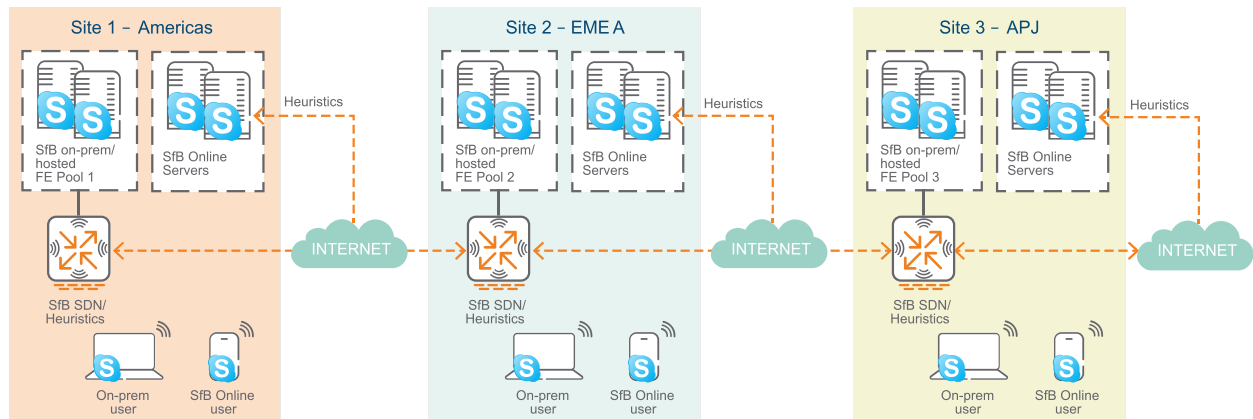
- One SfB FE server pool per region, for example, North America or Europe.
- One SDN manager pool per region.
- SDN manager configured to communicate with all Aruba controllers in that region.
- All SfB clients in a region are served by the front end servers in that region.
- SfB calls across multiple regions are managed by the local front end server in that region.

Check with your local Value-Added Reseller (VAR) or Aruba SfB expert on the number of Aruba controllers and SfB clients that can be managed by the SDN manager and FE server pool.

Multisite Deployment with SDN API and Heuristics

[Figure 17](#) describes a SfB topology with both on premise SfB servers and Office 365 SfB online. Office 365 is only supported with heuristics based classification. Starting with ArubaOS 6.4.0, controllers can simultaneously enable both heuristics and SDN API based classification.

Figure 17 *Multisite SfB Architecture with On-Premise and Office 365*



Guest and BYOD Access Topology

In this topology network security is context-based, in this model there is no L1/L2 separation, one common network is shared between all users/devices/applications, and security is achieved through contextually enforced profiles (roles) assigned to users and devices.

The following guidelines should be applied to Bring Your Own Device (BYOD) networks:

1. Configure the user roles and network access rules for employee, guest, and BYOD profiles.
2. Apply SfB ACL to a specific user role such as Guest, or employees for whom SfB traffic needs to be classified and prioritized. Without a SfB ACL, the SfB traffic will be treated as best effort and not prioritized, and the user experience will suffer.

This section includes the following topics:

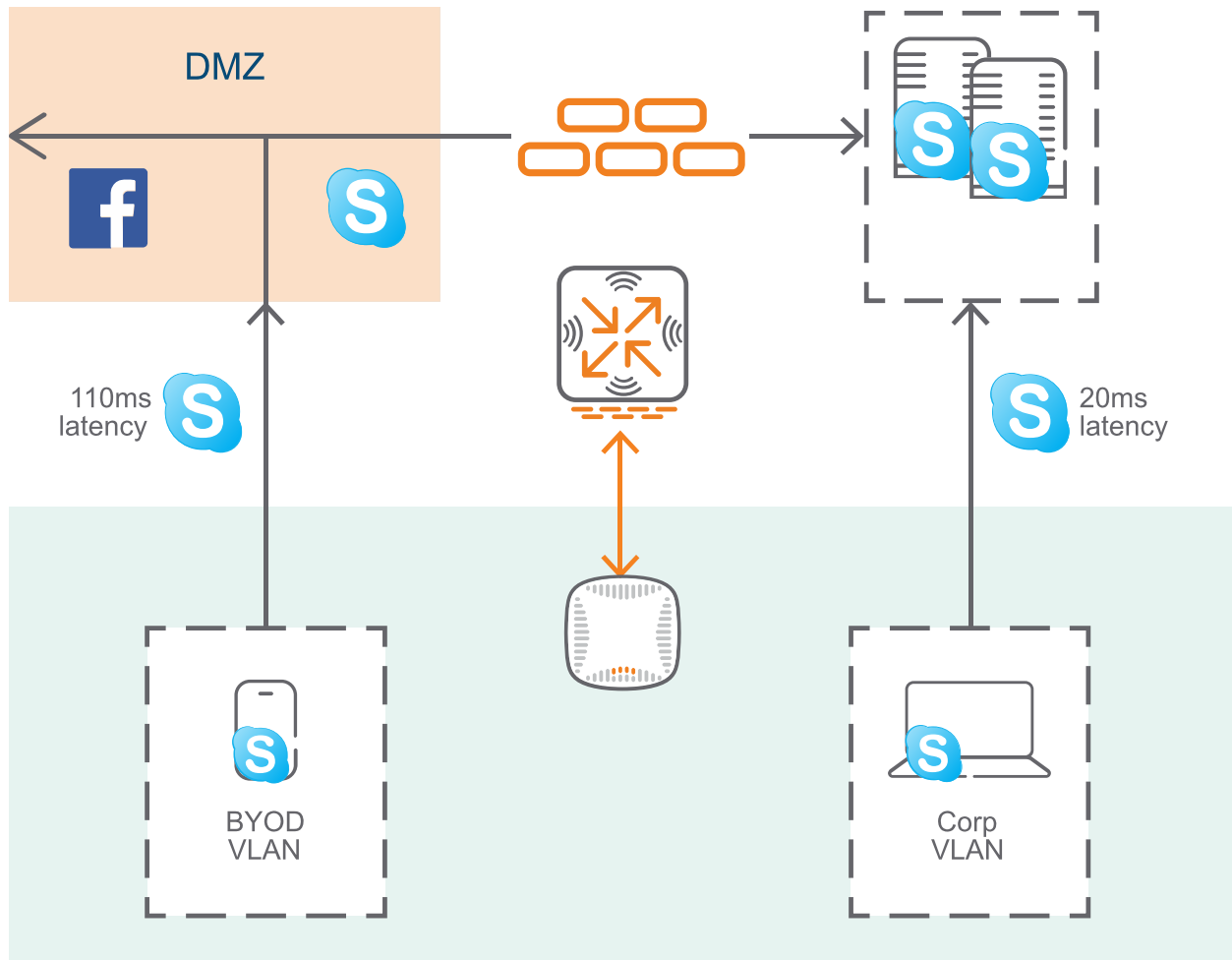
- [VLAN Based BYOD Latency Challenge on page 46](#)
- [Optimal BYOD SfB Traffic Engineering on page 47](#)
- [Forwarding Mode Considerations on page 48](#)

VLAN Based BYOD Latency Challenge

In this scenario, BYOD and corporate issued devices are separated by different VLANs, and all BYOD traffic flows through Demilitarized Zone (DMZ). Corporate bound traffic is routed through the firewall. For BYOD devices, NATing and firewall adds latency and loss, whereas traffic from corporate devices flows directly to the SfB server, to deliver a better user experience.

In the figure below latency for BYOD devices is 110 ms, whereas corporate device latency is just 20 ms.

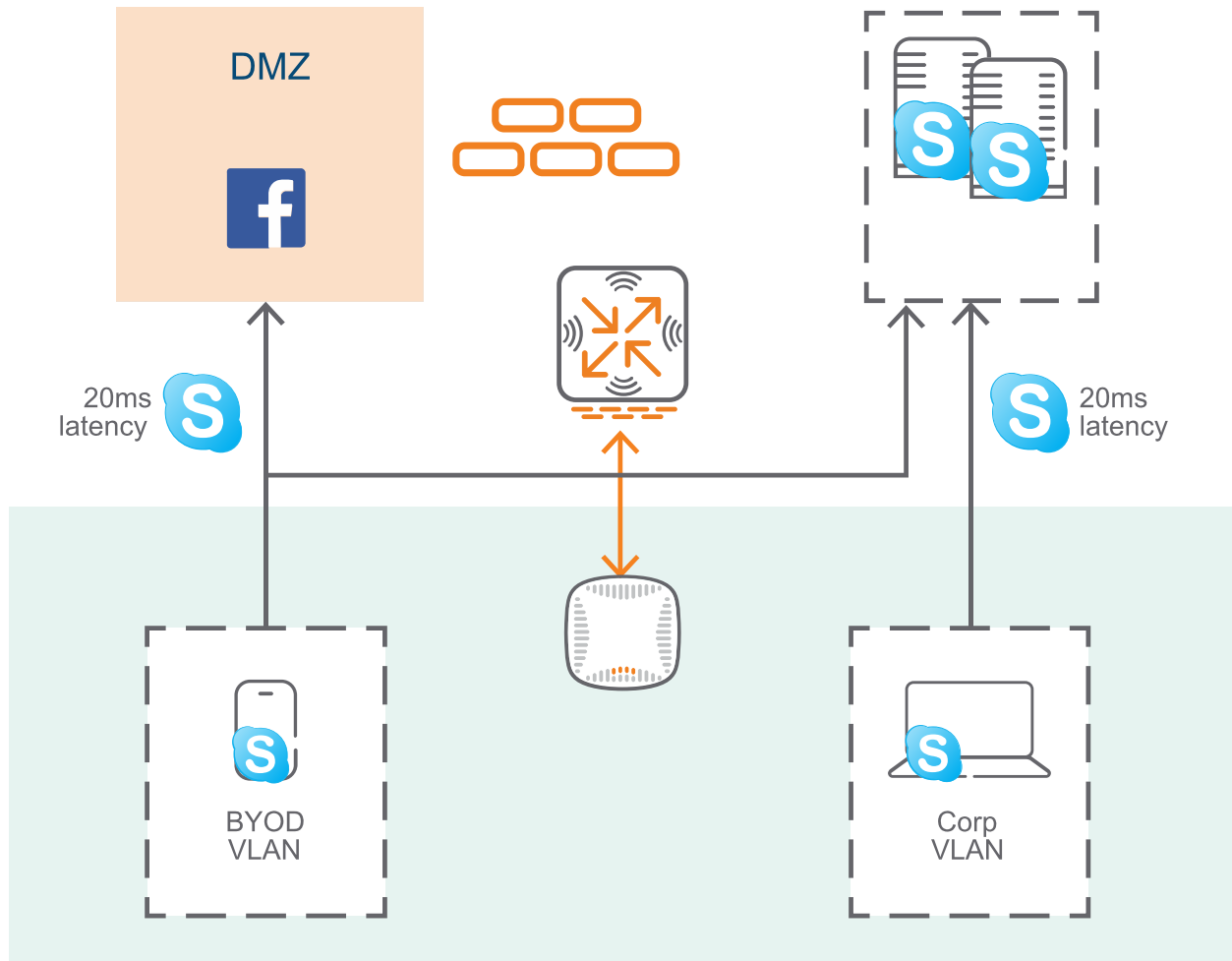
Figure 18 VLAN Based Latency Challenge with SfB



Optimal BYOD SfB Traffic Engineering

When BYOD and corporate issued devices are placed in the corporate Virtual Local Area Network (VLAN), the best result will be obtained through an ACL that forces BYOD traffic to take the best route. Thereby reducing latency to 20 ms for both BYOD and corporate issued devices.

Figure 19 Policy Based Routing for BYOD Devices



Forwarding Mode Considerations

Access points can be deployed using different forwarding modes:

- **Tunnel mode** - SfB heuristics and SDN API based classification are supported. SfB traffic is forwarded to the controller which classifies and prioritizes SfB traffic.
- **D-Tunnel mode** - APs can decrypt packets but cannot analyze the SfB traffic type. The SfB ALG resides on the controller which analyzes all SfB traffic analysis and classification.
- **QoS mode** - Traffic flow is similar to the logic used in the Tunnel mode.
- **Split Tunnel mode** - SDN API SfB classification is supported only for RAPs. The heuristics mode of SfB classification is not supported in Split Tunnel mode.
- **Bridge mode** - Heuristics and SDN API based SfB classification are not supported.

[Table 5](#) is a summary of forwarding modes and SfB classification methods.

Table 5: *Forwarding Modes vs. SfB Classification Methods Support Matrix*

SfB Classification	Tunnel	D-Tunnel	Split-Tunnel	Bridge
SfB Heuristics	Yes	Yes	No	No
SfB SDN API	Yes	Yes	Yes (RAPs only)	No

Aruba's Policy Enforcement Firewall (PEF) is a stateful firewall that applies policies to user roles and traffic sessions. Among other functions, the PEF can dynamically reclassify traffic, using firewall policies, and application layer gateways to prevent abuse and prioritize traffic whose tags are otherwise mismarked. Aruba controller traffic classification use cases that are described below.

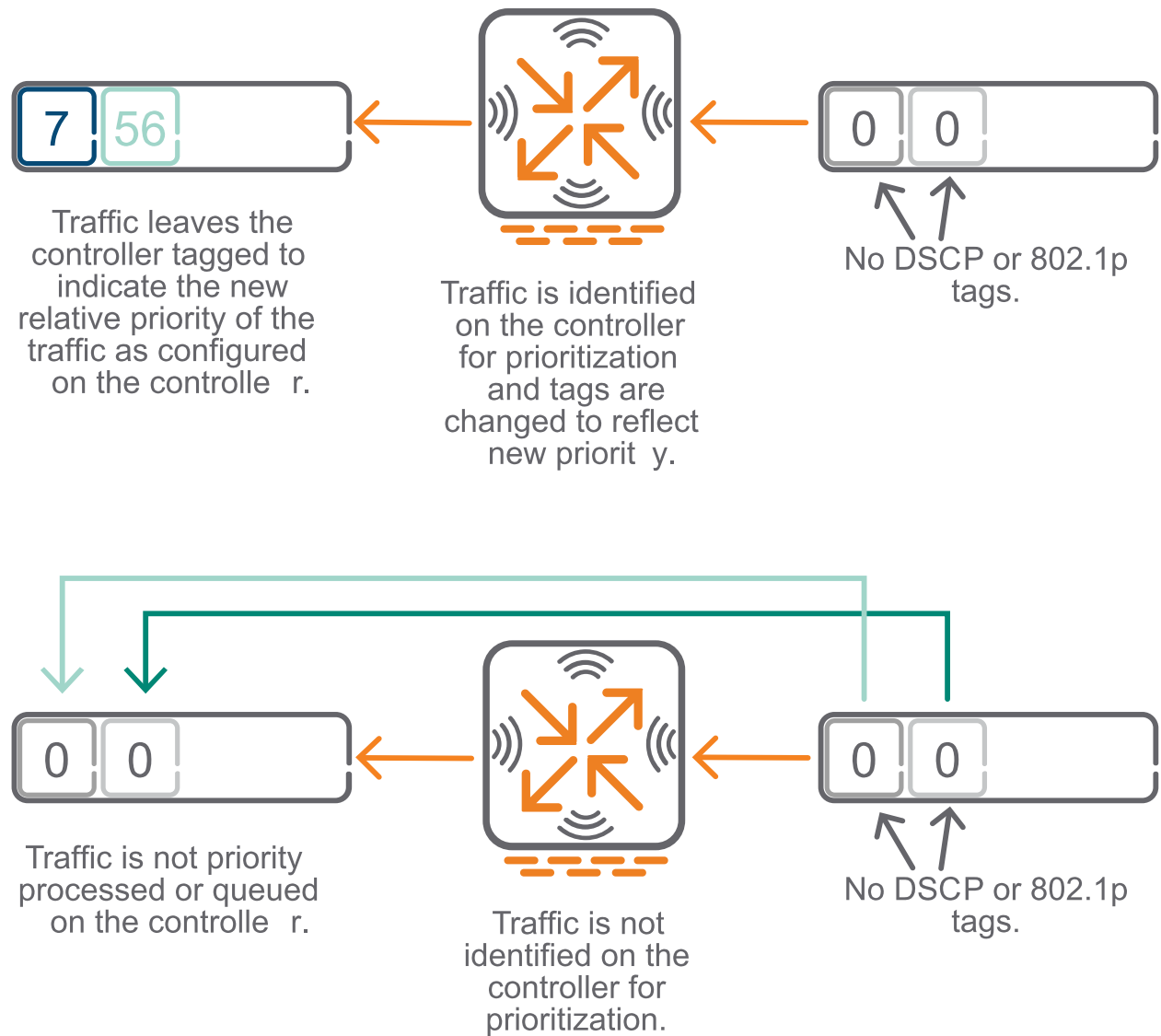
This chapter includes the following sections:

- [Classifying Unmarked Traffic on page 50](#)
- [Incoming Traffic is Marked on page 51](#)
- [Remarking Traffic to a Different Class on page 52](#)
- [WMM and QoS on page 53](#)

Classifying Unmarked Traffic

When traffic with no DSCP or 802.1p markings reaches a controller, it is compared with the policy assigned to the user role. Based on the class that the traffic is classified, the controller marks the traffic and forwards it. For example, traffic classified at the voice session level. If the traffic is unmarked and the controller determines that it should not be marked, it is forwarded without any modifications. [Figure 20](#) illustrates traffic marking.

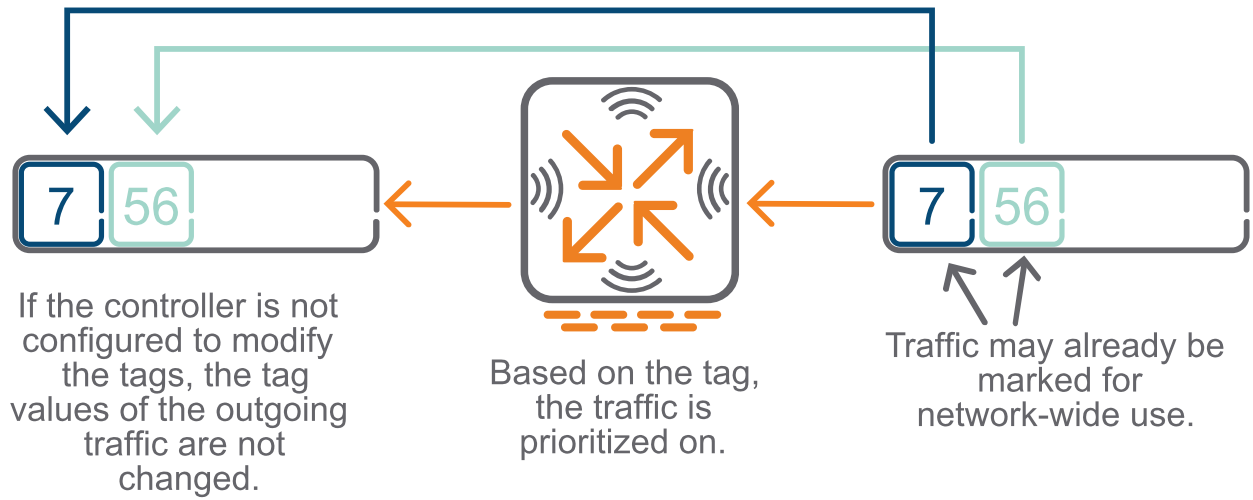
Figure 20 *Classifying Unmarked Traffic*



Incoming Traffic is Marked

Marked traffic is compared to the system policy. If the marks are correct for the policy and traffic type, the traffic is forwarded without any modifications.

Figure 21 *Marking Incoming Traffic*



Remarking Traffic to a Different Class

Marked traffic is compared to the system policy. If the marks are correct for the policy and traffic type, the traffic is forwarded without any modifications.

- Client is configured for a DSCP tag for voice (VO). Client sends voice packets with the correct DSCP tag, but when it reaches the controller, it has a different DSCP tag. For example, DSCP 46 is configured on the client as VO, but when the client sends a voice packet over Wi-Fi it gets classified as WMM-AC with priority as video (VI). The AP assigns a DSCP tag corresponding to the VI defined in DSCP-WMM configuration in the controller, which is different from the VO DSCP tag set by the client.
- Switches and routers in the wired network should be configured to honor the DSCP tag set by the client or in the controller. In the upstream direction, the client sets the DSCP tag for VO as 56, and the AP sends VO packet with DSCP 56 to the controller. Any intermediate wired switches that are not configured properly might change the original DSCP Tag.
- The controller is configured by a network administrator to reclassify traffic.

Figure 22 *Remarking Traffic to a Different Class*



WMM and QoS

WMM is based on the 802.11e standard and defines the basic QoS features for 802.11 networks. WMM uses the 802.1p classification scheme, which has eight priorities. WMM maps these priorities to four access categories:

- AC_BK
- AC_BE
- AC_VI
- AC_VO

These access categories map to four queues required by WMM devices as shown in [Table 6](#).

Table 6: 802.11p and WMM-AC Classification

Priority	802.1P Priority	802.1P Designation	Access Category	WMM Designation
Lowest	1	BK	AC_BK	Background
	2	BK		
	0	BE	AC_BE	Best Effort
	3	EE		
	4	CL	AC_VI	Video
	5	VI		
	6	VO	AC_VO	Voice
Highest	7	NC		

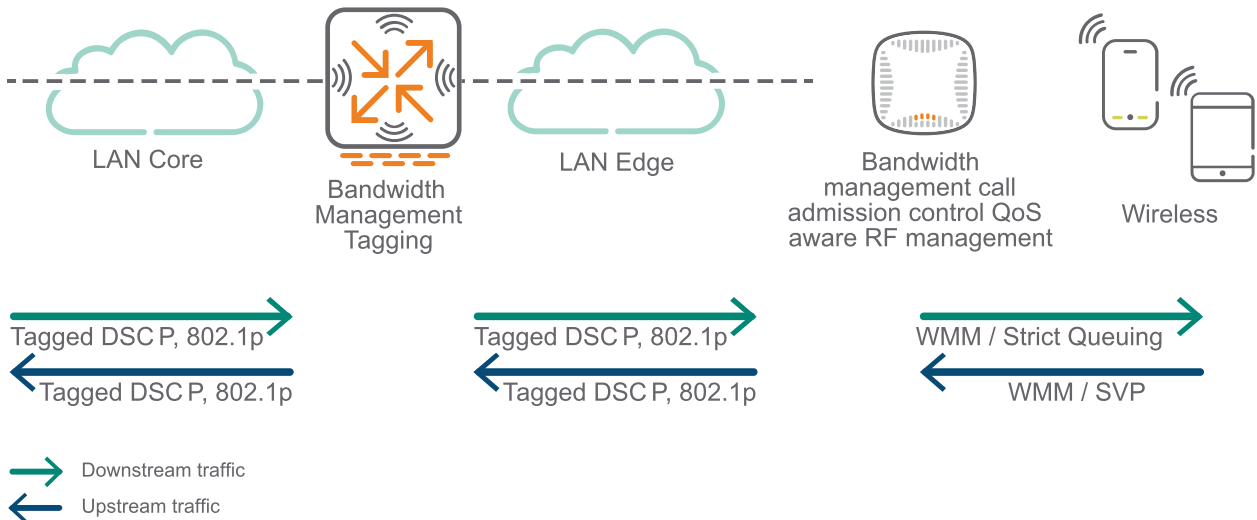
This section includes the following topics:

- [QoS Segments on page 54](#)
- [QoS Considerations on page 55](#)
- [QoS Flow on page 56](#)
- [DSCP Considerations on page 60](#)

QoS Segments

Figure 23 presents QoS related segments of the network. Wired traffic is prioritized with DSCP tags or 802.1p priority, while wireless traffic is prioritized with WMM-AC tags.

Figure 23 QoS Segments



QoS Considerations

QoS ensures that SfB real-time traffic is prioritized on both wired and wireless networks. On wired networks, QoS is applied through a DiffServ (DSCP) marking for Layer 3 and class of service (COS) for Layer 2 routing. On wireless networks, QoS is applied through WMM also known as 802.11e markings. QoS markings can be applied either at the client layer, if supported by the client and application, or in the switching or AP layer.

- **Client Side QoS** - Windows clients can tag traffic and can be configured on the client or set through Group Edit Policy using the SfB Server. See [Appendix on page 93](#) for more details.
- **Controller QoS Configuration** - DSCP-WMM mapping can be done on the controller where DSCP values can be set for different application categories such as VO/VI/BE/BK.

Figure 24 DSCP-WMM Mapping Configuration

Configuration > AP Group > Edit "default-a"

Profiles		Profile Details	
Wireless LAN		RTS Threshold	2333 bytes
Virtual AP		Short Preamble	<input checked="" type="checkbox"/>
SEEL_Ethersphere_Aruba		Max Associations	64
SEEL-Aruba-Guest		Wireless Multimedia (WMM)	<input type="checkbox"/>
aruba-hotspot-vap_prof		Auth-Surv	<input type="checkbox"/>
SEEL-PSK-Aruba		Wireless Multimedia U-APSD (WMM-UAPSD) Powersave	<input checked="" type="checkbox"/>
AAA	SEEL-Access-aaa_prof	WMM TSPEC Min Inactivity Interval	0 msec
802.11K	default	Override DSCP mappings for WMM clients	<input type="checkbox"/>
Hotspot 2.0	default	DSCP mapping for WMM voice AC	56
SSID	SEEL-Access-ssid_prof	DSCP mapping for WMM video AC	40
EDCA Parameters Station		DSCP mapping for WMM best-effort AC	24
EDCA Parameters AP		DSCP mapping for WMM background AC	8
High-throughput SSID	SEEL-Access-htssid_prof	Hide SSID	<input type="checkbox"/>



SfB SDN API tags SfB Desktop-Sharing with the Video DSCP tag and the SfB File Transfer traffic is marked with a best effort DSCP tag.

- **AP QoS Considerations** - In a controller environment, DSCP-WMM configuration is forwarded to the APs. The APs translate WMM <> DSCP values according to this mapping while sending traffic both upstream (wireless client to controller) and downstream (controller to wireless client).
 - The DSCP tag is placed outside the Generic Router Encapsulation (GRE) header when the AP sends the packet to the controller.
- **IAP QoS Configuration** - IAP version 6.4.0.2-4.1 and higher enables the IAP to customize Wi-Fi multimedia to DSCP mapping configuration for upstream (client to IAP) and downstream (IAP to client) traffic. The following table presents DSCP to WMM mappings for different traffic types. For example, if incoming traffic type is marked with DSCP 48 or 56 then it is linked to the WMM voice queue.

Table 7: DSCP-WMM Configuration IAP

DSCP Decimal Value	Description
8	Background
16	
0	Best Effort
24	
32	Video
40	
48	Voice
56	

Customized mappings can be created between WMM AC and the DSCP tag to prioritize traffic types and apply these changes to a WMM-enabled SSID profile. When WMM AC mapping values are configured, all packets received are matched against the entries in the mapping table and prioritized accordingly.

Refer to the [IAP 6.4.0.2-4.1 CLI Reference Guide](#) for the DSCP-WMM configuration. Customized DSCP-WMM configuration was not supported prior to IAP 6.4.0.2-4.1 and earlier IAP versions mapped DSCP 48 to voice traffic and DSCP 40 to video traffic.

QoS Flow

The use cases below demonstrate how QoS is translated for different call scenarios such as wireless-to-wireless and wireless-to wired calls. The use cases apply to WMM-only mode (no SfB voice classification or prioritization), SfB heuristics, and SDN API modes. These use cases are described under the tunnel forwarding mode of operation.

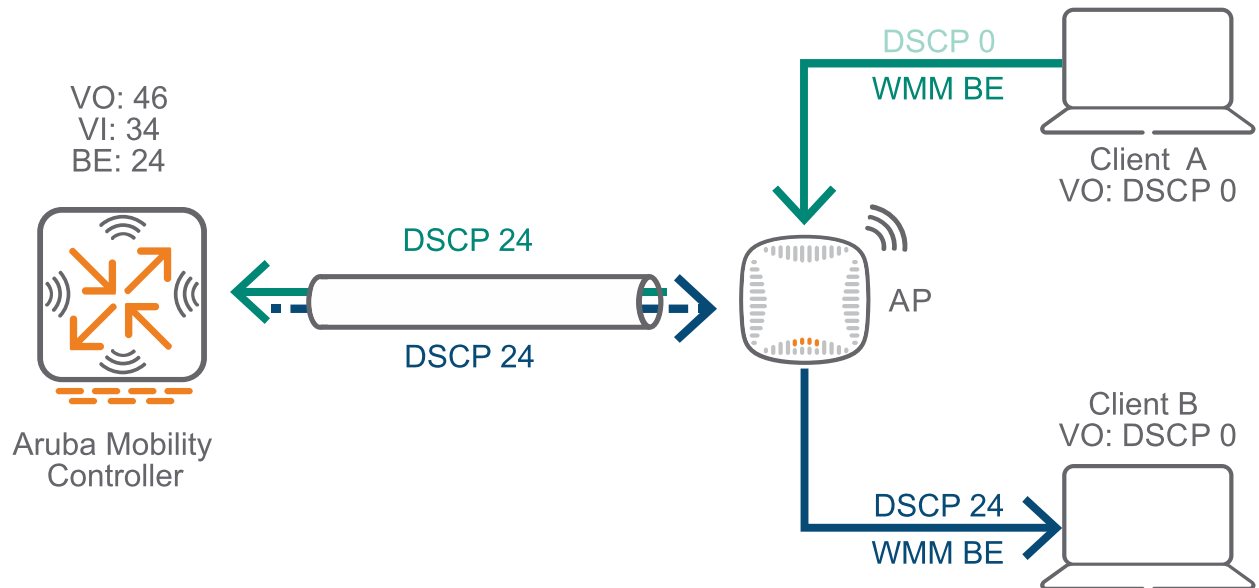
This section includes the following topics:

- [WMM Only Mode on page 57](#)
- [Heuristics Mode on page 58](#)
- [SDN API Mode on page 58](#)
- [Wired to Wireless on page 59](#)
- [Wireless to Wired on page 59](#)

WMM Only Mode

Client A initiates a SfB voice call to Client B and Client A is not tagging SfB voice traffic.

Figure 25 QoS Flow in WMM Only Mode



1. In upstream direction (Client to Controller), AP looks at L2 Priority (WMM-AC as BE) and sets DSCP 24 as per DSCP-WMM mapping in the controller.
2. The controller decrypts the packet and uses L2 priority to assign DSCP 24 in the downstream direction (controller to client).
3. The AP assigns WMM-AC as BE corresponding to the DSCP-WMM mapping on the controller.

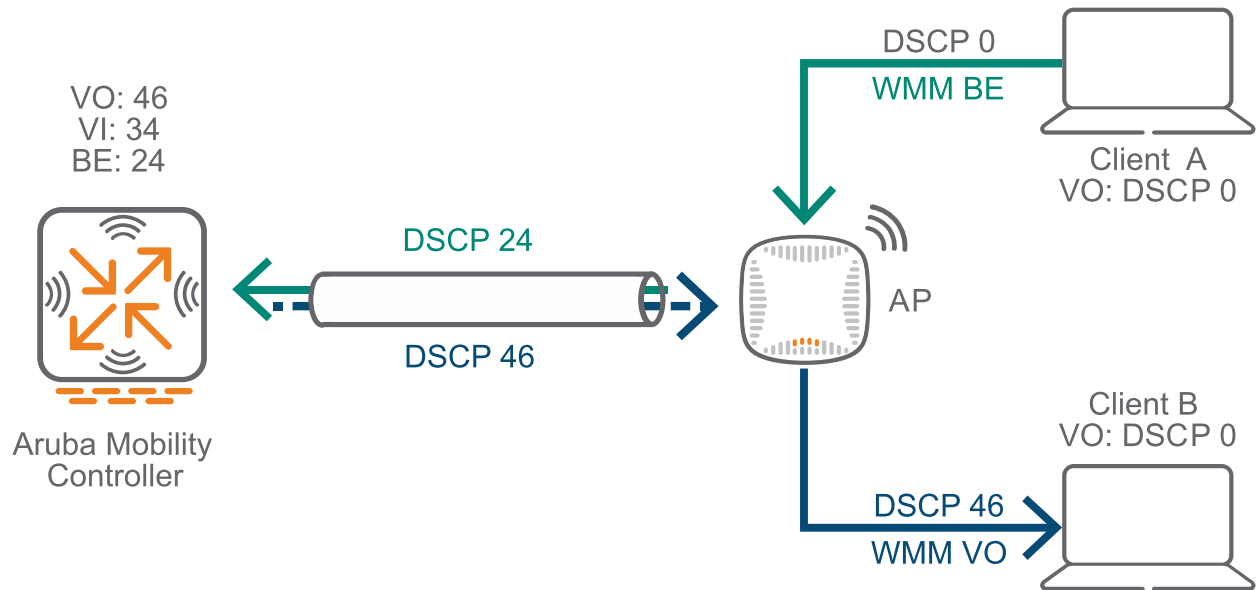


SfB Best effort traffic is sent with Best Effort Priority in entire network.

Heuristics Mode

Client A initiates a SfB voice call to Client B but Client A does not tag SfB voice traffic. The controller is configured to detect SfB VO traffic through heuristics.

Figure 26 QoS Flow in Heuristics Mode



1. In upstream direction (client to controller) the AP looks at L2 Priority (WMM-AC as BE) and allocates the DSCP 24 according to the DSCM-WMM mapping in the controller.
2. The controller identifies the SfB VO traffic type using heuristics and corrects the DSCP tag to 46 in the downstream direction (controller to client).
3. AP assigns WMM-AC as VO as per DSCP-WMM mapping in the controller.



SfB voice traffic gets best effort priority in upstream direction, but gets corrected to VO priority in downstream direction.

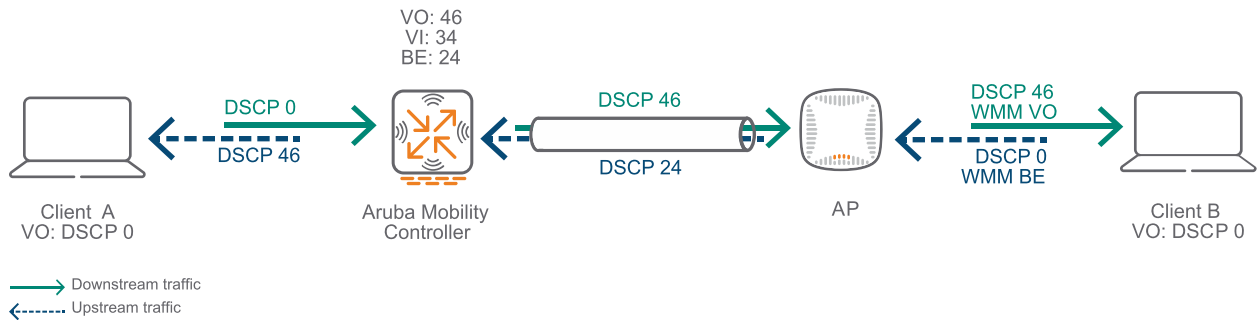
SDN API Mode

QoS flows in the SfB SDN API are identical to QoS flows in the heuristics mode. The SfB SDN API module on the SfB server sends SfB VO traffic type information to the controller when Client A initiates a voice call to Client B.

Wired to Wireless

This use case applies to SfB VO calls between a wired client and a wireless client, either with SfB heuristics or SfB SDN API based classification.

Figure 27 QoS Flow Wired to Wireless

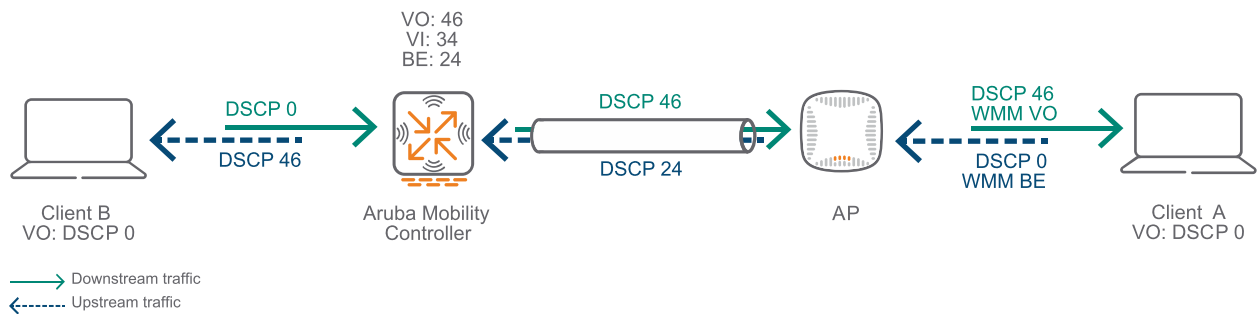


1. In upstream direction (wired client to wireless client) the controller locates SfB VO traffic in data path and assigns DSCP 46 per DSCP-WMM mapping. The AP assigns WMM VO per the DSCP-WMM mapping.
2. In downstream direction (wireless client to wired client), the AP looks at L2 Priority (WMM-AC as BE) and sets DSCP 24 per DSCM-WMM mapping in the controller.
3. The controller locates a SfB VO packet and sets DSCP tag to 46 for VO when sending the packet to the wired SfB client.

Wireless to Wired

This use case applies to SfB VO call from a wireless client to a wired client either with SfB heuristics or SfB SDN API based SfB classification.

Figure 28 QoS Flow Wireless to Wired

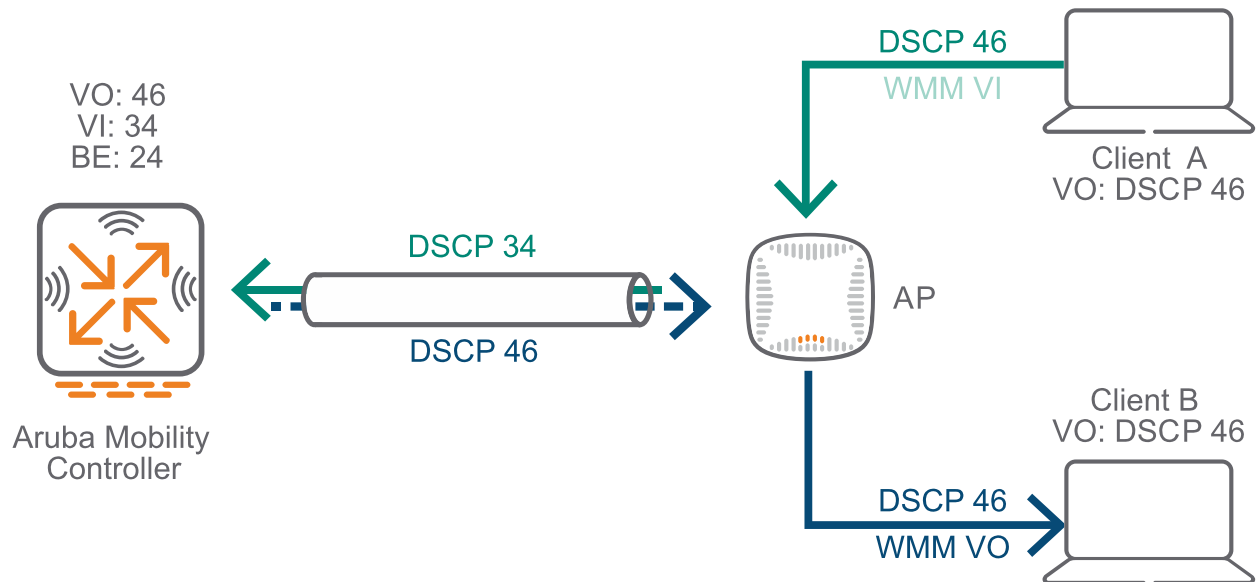


1. In upstream direction (wireless client to wired client) the AP looks at L2 Priority (WMM-AC as BE) and sets DSCP 24 per DSCM-WMM mapping in the controller.
2. The controller finds a SfB VO packet and sets the DSCP tag to 46 for VO when sending the packet to the wired SfB client.
3. In downstream direction, the controller locates a SfB VO packet sent from the wired client and retags the DSCP tag to 46 for VO.
4. The AP assigns WMM-AC as VO based on the DSCM-WMM mapping in the controller.

DSCP Considerations

It is recommended that the wireless controller DSCP setting for VO/VI/BE/BK matches the configurations of the wired network and the client devices, if they are tagging the traffic. There are caveats based on how the WMM converts DSCP to WMM mapping as shown in [Figure 29](#).

Figure 29 QoS Flow with DSCP 46



1. Client A is configured to tag VO traffic with DSCP 46.
2. The controller is configured to DSCP-WMM map VO/VI/BE to 46/34/24, respectively and AP uses tunnel mode forwarding.
3. Client A makes a SfB voice call to Client B. The wireless driver on Client A converts DSCP to WMM-AC video and sends it over the air.
4. The AP sees WMM-AC as VI and sets DSCP tag to 34 per DSCP-WMM mapping in the controller.

VO traffic is sent with VI priority in the upstream direction. However, there is an issue with the way in which the wireless driver interprets DSCP and converts it to WMM-AC. [Table 8](#) outlines how the DSCP values are interpreted by WMM.

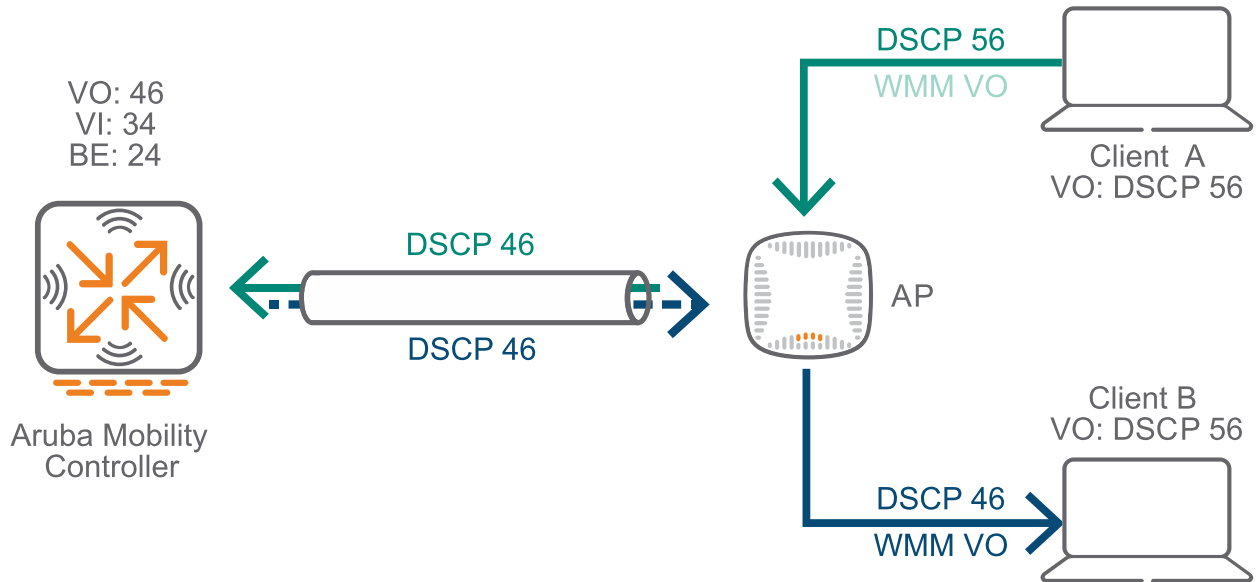
Table 8: DSCP to WMM-AC Mapping

DSCP Decimal Value	Description
48-63	VO
32-47	VI
22-31	BE
0-21	BK

It is recommended that the client applies a DSCP tag, to set the correct WMM-AC priority. If the wired network is configured with DSCP 46 for VO, and it is not trivial to reconfigure to DSCP 56, then use the following workaround:

1. Program Windows 7/8 clients with DSCP 56 and above using the Group Edit Policy configuration from the SfB server.
2. Client sends VO packets with WMM-AC as VO over wireless, and the APs applies the correct DSCP tag for VO (DSCP 46) when the packets are sent to the controllers.

Figure 30 DSCP 46 Consideration

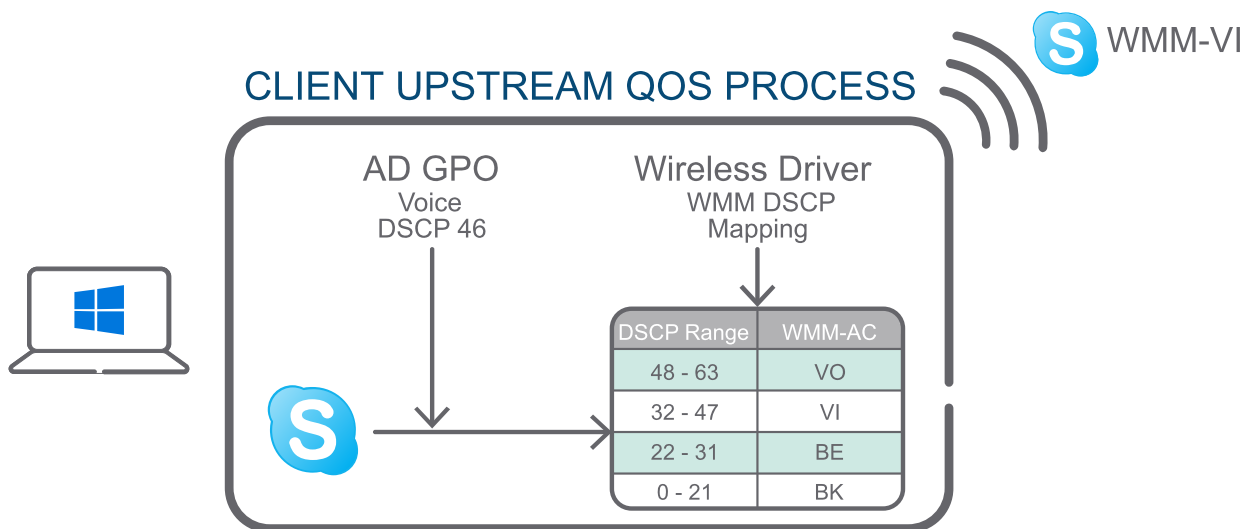


Group Edit Policy applies to Windows 7/8 clients only.

When the WMM standard was defined, the 802.1p COS model was used to define the eight WMM queues. The Voice over IP (VoIP) community established a standard DSCP value for voice traffic Expedited Forwarding-46 (EF-46): strictly mapping DSCP to WMM queuing resulting in EF-46 traffic being marked as WMM-VI as shown in [DSCP to WMM-AC Mapping on page 60](#).

Inappropriate classification of upstream EF-46 traffic to WMM VI is a side effect of the general purpose operating system on which SfB runs. Client devices and APs that run on purpose built operating systems are not classified inappropriately, as the mappings are set correctly by the manufacturer. The recommended workaround addresses upstream mistagging by applying higher DSCP values to wireless clients.

Figure 31 DSCP EF 46 and WMM

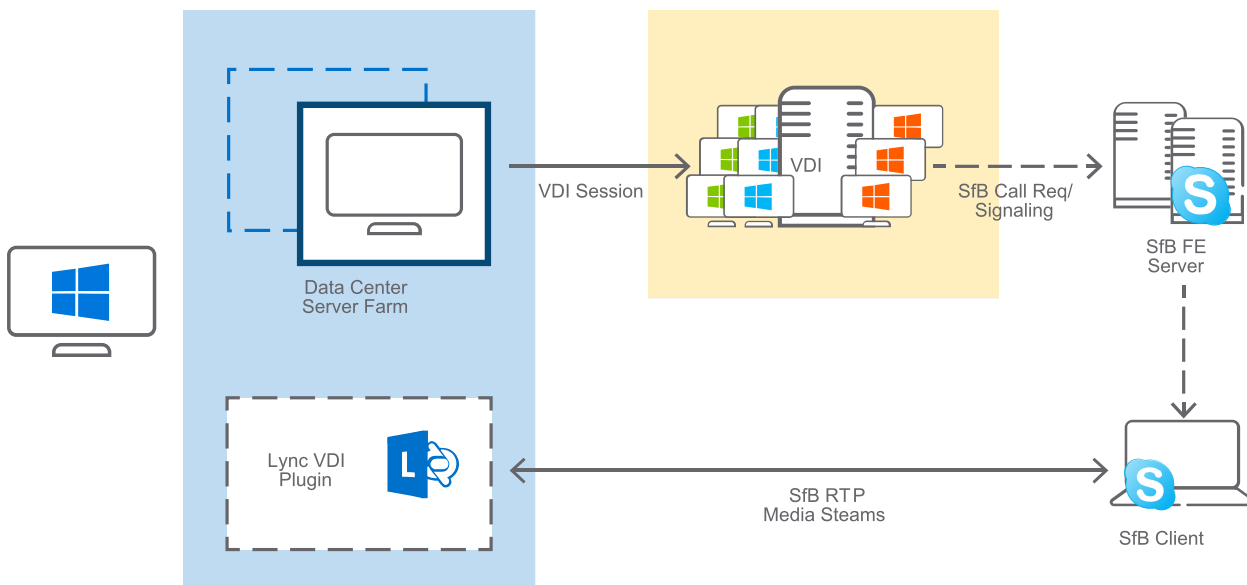


Virtual Desktop Infrastructure (VDI) is a centralized desktop delivery solution that stores and runs desktop workloads, enabling users to interact with the desktop through a remote connection. VDI includes a client operating system, applications, and data stored in a server based virtual machine (VM) in data centers.

Microsoft provides a Lync VDI Plug-in for Windows based thin clients through which they can use local audio and video in peer-to-peer and conference calls in a VDI environment. This plug-in was developed for Lync 2013 and is compatible with Lync 2013 and SfB 2015 clients. The Lync VDI Plug-in runs locally on thin or fat clients, and pairs with the SfB client in the virtual machine. This plug-in is still called **Lync VDI Plug-in** and is not rebranded to SfB VDI plug-in.

[Figure 32](#) describes the SfB call flow between a client with a Lync VDI Plug-in and another SfB client.

Figure 32 SfB with VDI Plug-in Call Flow



SfB media would remain in the VDI session without the plug-in, and not be separately prioritized or identified, resulting in poor audio and video performance. Aruba's wireless infrastructure can classify and prioritize SfB VDI voice and video sessions.



Lync 2013 or SfB on VDI is not supported or recommended without use of the Lync VDI Plug-in. Testing has demonstrated significant quality degradation when Lync 2013 or SfB is used within a VDI session on a WLAN.

You can download the Lync VDI Plug-in from the [Microsoft download center](#).

Refer to the [Microsoft deployment guidelines](#) to deploy the Lync VDI Plug-in with the SfB 2015 server.

This chapter includes the following sections:

- [Call Scalability Per AP Per Radio on page 64](#)
- [SDN API Scalability on page 64](#)

Call Scalability Per AP Per Radio

[Table 9](#) outlines the number of simultaneous SfB VO/Vl calls that have been tested by AP and software release.

Table 9: SfB Call Scalability Per AP

AP Type	Band Tested	Number of SfB VO/Vl Calls Tested	Background Traffic	Release
AP-135	5G	20	140 Mbps UDP downstream	ArubaOS 6.2
AP-225	5G	54	None	ArubaOS 6.4
IAP-135	5G	20	None	Instant 3.4.0.0

SDN API Scalability

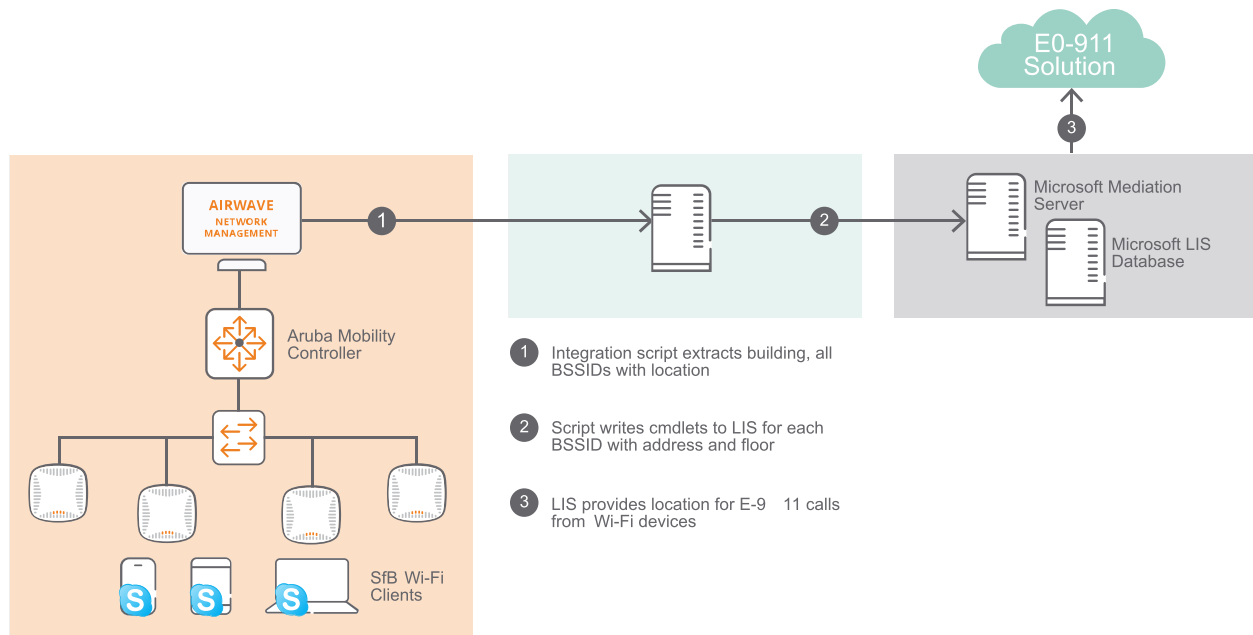
SDN API 2.1 introduced subnet based filtering and SDN manager pool. The subnet based filtering feature enabled SfB client subnets are mapped to Aruba controller IP addresses, so SDN API messages for those clients go to the specific controllers where they belong. This reduced the number of SDN API messages significantly between SDN manager and the controllers.

SDN managers can be configured as part of a pool and share the load across the cluster. It does automatic failover if one SDN manager goes down within the pool.

There is no scalability limitation in terms of number of Aruba controllers that can be used with SDN API.

The SfB E911 solution integrates with the Microsoft Location Information Service (LIS) server to obtain location users placing emergency calls. [Figure 33](#) presents Aruba's LIS Integration for SfB E-911.

Figure 33 Aruba SfB E911 Solution



To facilitate proper mapping updates, the BSSID to AP mappings using a script. See [Integrating Aruba Wireless LANs With Microsoft SfB's Emergency Call Architecture white paper](#) for a sample PowerShell script that automatically updates the LIS at regular intervals to synchronize the LIS and Wi-Fi network.

This chapter includes the following sections:

- [Switch Scalability Considerations on page 66](#)
- [Network Optimizer Use Cases on page 67](#)
- [Network Optimizer Configuration on page 67](#)

Switch Scalability Considerations

Another design consideration when deploying Network Optimizer and integrating with wireless is ensuring that the switch can support the number of devices present on the switch being managed by Network Optimizer and the VAN SDN Controller. The number of devices includes devices connected to wireless access points with local bridging and downstream non-SDN managed switches. Devices connected to APs with controlled traffic are not counted.

Table 10: *Switch Scalability Guidelines*

Model	VAN SDN Support (Number of Local Devices per Switch/Stack/VSF Cluster)	Network Optimizer
Aruba 2920	350	Supported
Aruba 2930F	1000	Supported
HPE 3500	750	Supported
HPE 3800	1000	Supported
Aruba 3810M	1000	Supported
HPE 5400 v1 / 8200 v1	1250	Supported
HPE 5400 v2 / 8200 v2	1250	Supported
Aruba 5400R v2	1250	Supported
Aruba 5400R v3	1250	Supported

Network Optimizer Use Cases

Network Optimizer is designed to listen to the SfB SDN API information and apply the policy associated with the specific voice/video/app share flow in the network. For devices known to Network Optimizer, the application instructs the switch local to the known device to apply a QoS remarking rule for the specific RTP or TCP session on both the source and destination endpoints.

This section includes the following topics:

- [Instant AP on page 67](#)
- [Wired Users on page 67](#)

Instant AP

Since the VAN SDN Controller and Network Optimizer have knowledge of devices connected to Instant AP's in the network (Instant APs bridge traffic locally) we apply the policy on the switch using Openflow to configure a specific remarking rule for the SfB traffic flow. If the Instant AP has applied a DSCP tag due to heuristics, this is overridden by Network Optimizer.

Wired Users

VAN SDN Controller and Network Optimizer have knowledge of wired users connected to a switch. We can apply the policy on the switch using Openflow to configure a specific remarking rule for the SfB traffic flow.

Network Optimizer Configuration

This section includes the following topics:

- [Adding SfB SDN Manager on page 67](#)
- [Adding SfB FE Server on page 68](#)
- [DSCP Configuration on page 69](#)

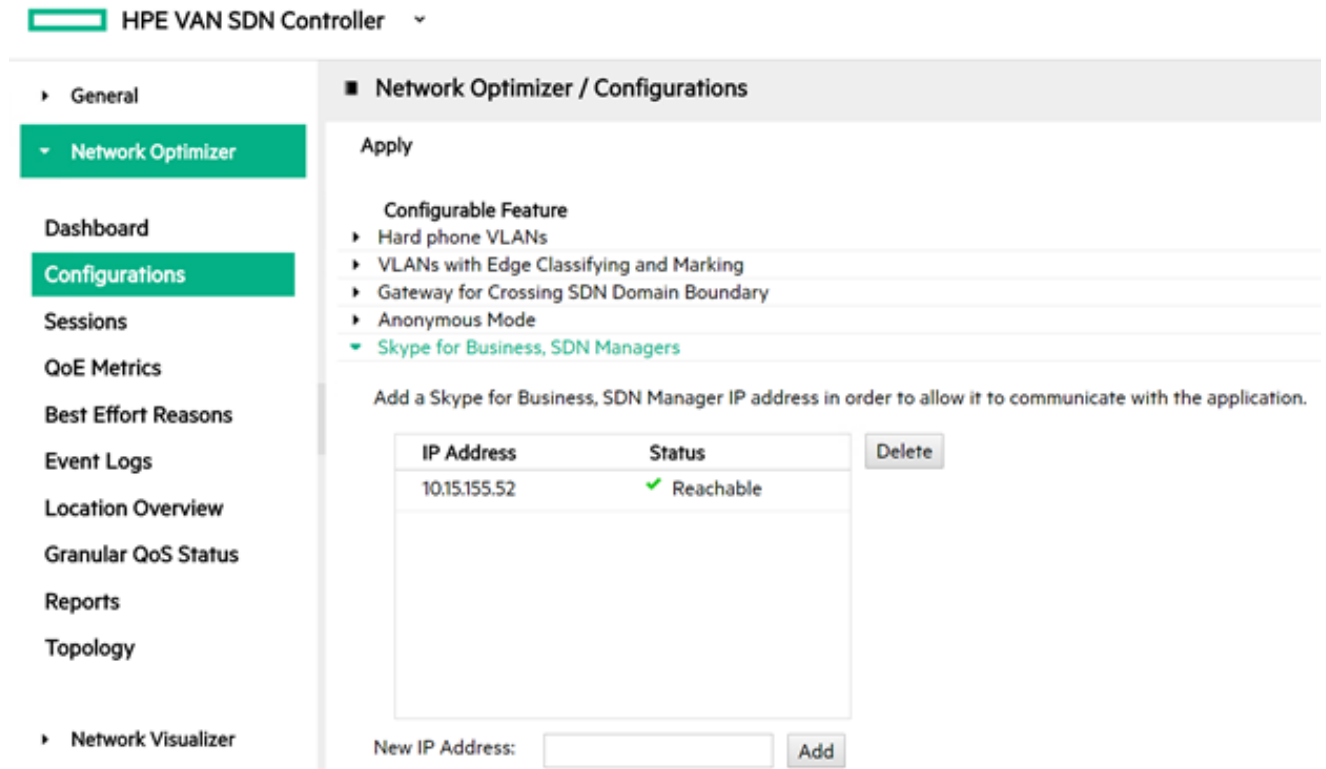
Adding SfB SDN Manager

Network Optimizer identifies a Skype for Business SDN Manager by its static IP address. Before Network Optimizer can manage the QoS deployment for Skype for Business calls from a Skype for Business SDN Manager, you must add that server to Network Optimizer.

To add a Skype for Business SDN Manager:

1. Login in to the console with username **sdn** and password **skyline**:
<https://sdn-controller-ip:8443/sdn/ui>
2. In the **Configurations** page, click the icon > to the left of **Skype for Business, SDN Managers**.
The Skype for Business SDN Manager configuration dialog box appears.
3. Enter the IP address of the Skype for Business SDN Manager in the **New IP Address box**.
4. Click **Add**.
5. Click **Apply** on the top of the configuration page.
A Status dialog box displays indicating whether the operation is successful.
6. In the **Status** dialog box, click **Close**.

Figure 34 SDN Manager Configuration



After you add a Skype for Business SDN Manager to the Network Optimizer, its reach ability is displayed alongside its IP address. For a newly added Skype for Business SDN Manager, the system might take a few minutes to display its reach ability in the Skype for Business SDN Manager table.

Alternatively, you can view the reach ability of the newly added Skype for Business SDN Manager in the Skype for Business SDN Managers page.

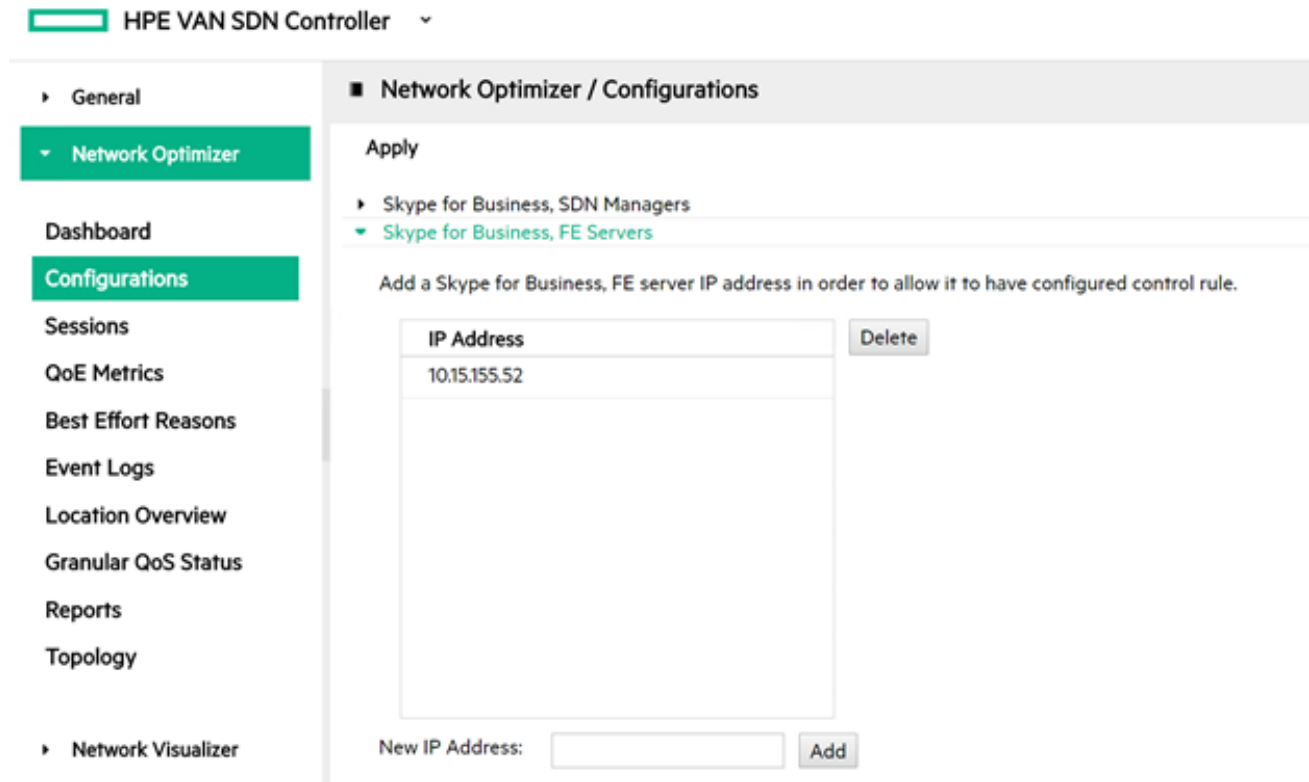
Adding SfB FE Server

In a Skype for Business deployment, the FE Server is the core server role, and runs many basic Skype for Business Server functions. The FE server configuration is to prioritize the control traffic between the Skype for Business Client and the Skype for Business FE Server.

To add a Skype for Business FE Server:

1. Login in to the console with username **sdn** and password **skyline**:
<https://sdn-controller-ip:8443/sdn/ui>
2. In the **Configurations** page, click the icon > to the left of **Skype for Business, FE Servers**.
The Skype4B FE Server configuration dialog box appears.
3. Enter the IP address of the Skype for Business FE server in the **New IP Address box**.
4. Click **Add**.
5. Click **Apply** on the top of the configuration page.
A Status dialog box displays indicating whether the operation is successful.
6. In the **Status** dialog box, click **Close**.

Figure 35 SfB FE Server Configuration



DSCP Configuration

The following information introduces how to modify the default DSCP settings for different media types.

1. In the Configurations page, click the icon > to the left of Global QoS Settings.
The DSCP Setting box appears. The default DSCP and L2 priority values for each media type are displayed.
2. To change the default DSCP value and L2 priority of a media type, select a value from the drop-down list to the left of the media type. The media types include:
 - **Control** - Used to communicate with FE server and is installed when an application is activated to ensure control packet connectivity
 - **Voice** - Used in voice calls between Skype for Business clients
 - **Video** - Used in video calls between Skype for Business clients
 - **Application Share** - Used in application share events initiated via Skype for Business
 - **Best Effort** - When the Network Optimizer fails to prioritize the configured DSCP and L2 priority values, the default best effort DSCP and L2 priority values are used to prioritize the calls

DSCP value range is from 0 to 63 and L2 priority (VLAN PCP) value range is 0 to 7. The table below lists recommended DSCP and L2 priority values for all the media types.

Table 11: Switch Scalability Guidelines

Media Type	Recommended DSCP Values	Recommended L2 Priority Values
Control	24 (CS3)	3
Voice	46 (EF)	5
Video	34 (AF41)	4
Application Share	26 (AF31)	3
Best Effort Value	0 (Off - Default)	0



DSCP does not default to rewrite best effort traffic in order to integrate with mixed network environments better. In an all ArubaOS-Switch environment the recommendation would be to set Best Effort rule to DSCP = 0 and L2 = 0.

Figure 36 DSCP Configuration

HPE VAN SDN Controller 104 sdn

General

Network Optimizer

Dashboard

Configurations

Sessions

QoE Metrics

Best Effort Reasons

Event Logs

Location Overview

Granular QoS Status

Reports

Topology

Network Optimizer / Configurations

Apply

Global QoS Setting

Enter DSCP and L2 priority value for each call type, and apply setting. DSCP value range [0-63] in decimal. L2 priority value range [0-7] in decimal.

	DSCP Setting:	L2 priority:
Control:	24 (CS3)	3
Voice:	46 (EF)	5
Video:	34 (AF41)	4
App Share:	26 (AF31)	3
Best Effort:	Off	0

Location QoS Setting

LDAP Profile

User Group Priority

This chapter includes the following sections:

- [SDN Integration Troubleshooting on page 71](#)
- [Controller Troubleshooting on page 73](#)
- [AP Troubleshooting on page 75](#)
- [RF Troubleshooting on page 75](#)
- [Wired Network Troubleshooting on page 76](#)
- [SfB Troubleshooting Using UCC Dashboard and CLI Commands on page 76](#)
- [SfB Troubleshooting on Network Optimizer on page 89](#)

SDN Integration Troubleshooting

The following section lists troubleshooting steps for SfB SDN API issues.

1. Check SfB traffic classification using one of the following methods:
 - Execute the `show datapath session` command.
 - Enter the IP address of the wireless client to check if the controller tags the traffic correctly.

Figure 37 illustrates a SfB video call in which the controller classifies voice and video traffic with VoIP flag - “V” and applies the correct DSCP tags “46” for voice and “34” for video.



A SfB video call has both SfB voice and video sessions, with their respective DSCP tags. In the following command output, only VI DSCP tagging is displayed.

Figure 37 SfB Video Call

(POD1-Local1) #show datapath session include 10.70.218.13													
10.70.218.13	191.232.139.68	6	63263	443	0/0	0	0	2	tunnel 20	7cbc 1069	106356	CG	
10.70.218.14	10.70.218.13	17	16448	32972	0/0	5	34	0	vlan 143	1f8e 377962	256851573	FHPTV	
10.70.218.13	10.70.218.14	17	28773	29944	0/0	6	46	0	vlan 158	1f8e 28137	8976879	FHPTCIQV	
10.70.218.14	10.70.218.13	17	29944	28773	0/0	6	46	0	vlan 158	1f8e 62484	13335523	FHPTIQV	
10.70.5.7	10.70.218.13	6	5061	63268	0/0	6	0	6	tunnel 20	7cb7 1004	315795	H	
10.70.218.13	10.70.218.11	6	139	49784	0/0	0	0	1	tunnel 20	1e 19	2819	F	
10.70.218.11	10.70.218.13	6	49784	139	0/0	0	0	1	tunnel 20	1e 21	2653	FC	
10.70.218.13	10.70.218.14	17	32972	16448	0/0	5	34	0	vlan 143	1f8e 131930	20549409	FHPTCV	
191.232.139.68	10.70.218.13	6	443	63263	0/0	0	0	2	tunnel 20	7cbc 544	107202		
10.70.218.13	10.70.5.7	6	63268	5061	0/0	6	0	5	tunnel 20	7cb7 1032	338667	HCG	

2. If SfB voice or video is not reaching the controller, check for:
 - Actual flow of SfB voice or video traffic.
 - Issues with call connectivity.

Voice debug logs provide information about SfB SDN API messages and prioritization. These logs provide granular visibility into the messages exchanged between SfB SDN manager and the controller.

Figure 38 illustrates sample debug logs and also shows that the controller is able to receive XML messages from the Sfb server.

Figure 38 Sfb Sample Debug Logs

```
(POD1-Local1) (config) #show log user all | include voice
Aug 26 10:24:57 :503188: <4013> <DEBUG> stm| voice| </Start>
Aug 26 10:24:57 :503188: <4013> <DEBUG> stm| voice| </LyncDiagnostics>
Aug 26 10:24:57 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_display:9889 ***** END *****
Aug 26 10:24:57 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_handle_xml_msg:1712 LYNC INFO: XML msg length before & after stripping off.. =
Aug 26 10:24:57 :503188: <4013> <DEBUG> stm| voice| VM: get_alg_status:1652 LYNC INFO: ALG status: 1
Aug 26 10:24:57 :503188: <4013> <DEBUG> stm| voice| VM: get_alg_status:1653 LYNC INFO: Web Lync Port(Lync SDN API) status: 1
Aug 26 10:24:57 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_check_xml_msg_syntax:3103 LYNC INFO: Start data: (0) (0) (0), End data (1) (1)
Aug 26 10:24:57 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_get_xml_msg_type:9742 LYNC INFO: XML method found LyncDiagnostics Version="C"
Aug 26 10:24:57 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_get_xml_msg_type:9766 LYNC INFO: XML version returned is = 4
Aug 26 10:24:57 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_is_v2dot0_bic_msg:1581 LYNC INFO: XML method found LyncDiagnostics Version="C"
Aug 26 10:24:57 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_is_v2dot0_bic_msg:1585 LYNC INFO: Inside if check... InCallQuality
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_wrapper:4645 LYNC INFO: Lync XML version is = 4
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:4939 LYNC INFO: before calling vm_lync_parse_xml_msg_vidot1:4939 LYNC INFO: Version for which processing is performed
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:4953 LYNC INFO: after SU check 0=Update, 1=audio
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:4961 LYNC INFO: Setting to UPDATE..
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:4975 LYNC INFO: hold_update = 0
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:4981 LYNC INFO: Leg 1 processing started...
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5001 LYNC INFO: SOURCE POOL is pool.tmelab.net...
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5012 LYNC INFO: USER AGENT is RTCC/6.0.0.0 UCWA/6.0.0.0
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5024 LYNC INFO: USER AGENT Type is ...
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5085 LYNC INFO: AppSharing Desktop call & ConversationId
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5104 LYNC INFO: received audio call.
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5111 LYNC INFO: port for audio call 25922.
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5121 LYNC INFO: from Incall_Enabled false.
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5133 LYNC INFO: ip for audio call 10.70.218.14.
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5144 LYNC INFO: peer ip for audio call 10.70.215.241.
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5153 LYNC INFO: leg_id for audio call 553fc09731.
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5192 LYNC INFO: Retrive codec details for V2.0..
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5198 LYNC INFO: codec info found & val is SILK/16000
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_get_codec_details_vidot1:2330 LYNC INFO: codec_rate = 16000
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5208 LYNC INFO: high bw value 105000
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5223 LYNC INFO: bandwidth maximum is 164600
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5243 LYNC INFO: after SU check 0=Start, 1=video
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5247 LYNC INFO: received video call. su_token = Start
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5257 LYNC INFO: 1,2 63 = 1 1 1
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5263 LYNC INFO: port for video call 29656.
Aug 26 10:24:58 :503188: <4013> <DEBUG> stm| voice| VM: vm_lync_parse_xml_msg_vidot1:5277 LYNC INFO: ip for video call 10.70.218.14.
```



If you are receiving SDN messages and Sfb traffic is still not prioritized, check if the Sfb SDN manager is sending start dialogue for calls and not an error message. If the Sfb SDN manager is sending an error message the controller will not prioritize traffic. The issue occurs due to misconfiguration on the Sfb server.

Packet capture between the controller and SDN manager will also show SDN API messages.

Controller Troubleshooting

Listed below are some of the controller troubleshooting procedures.

- DSCP to WMM mapping for VO/VI/BE/BK traffic types are defined in the SSID profile in the controller as shown in [Figure 39](#).

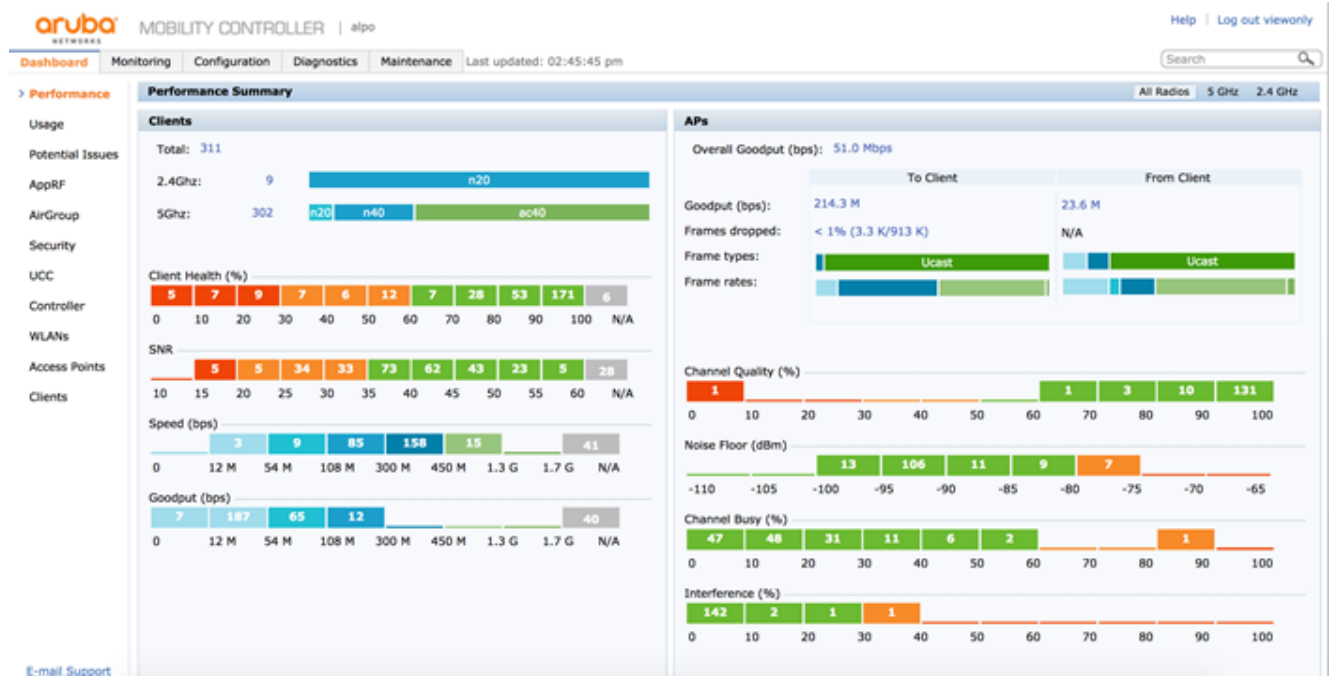
Figure 39 SSID Profile

```
(SE_PFE_1) #show wlan ssid-profile sko-vegas-fy-14
.. .. .
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
```

The controller prioritizes different SfB traffic types as per the above configuration. To verify if the controller is able to prioritize SfB traffic and is applying the correct QoS, see the `show datapath session` output in the [SDN Integration Troubleshooting on page 71](#).

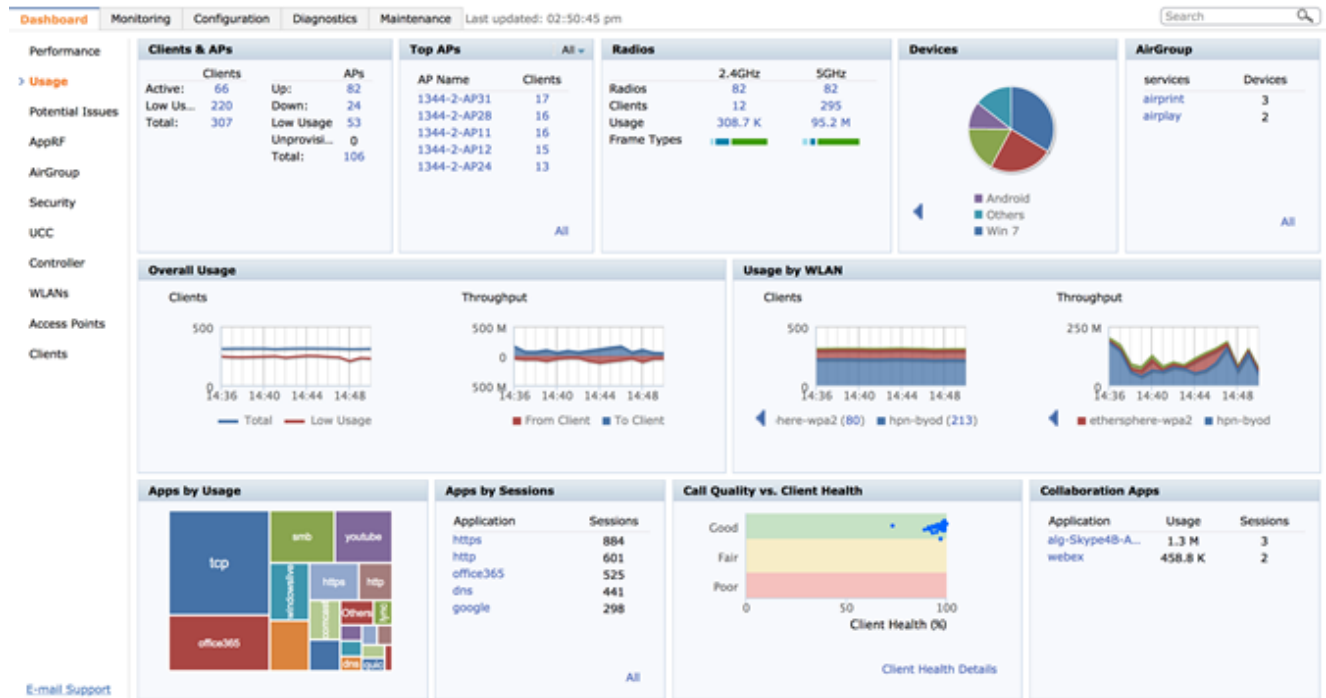
- The performance dashboard in [Figure 40](#) provides real-time visibility into various performance metrics on the system. This feature provides a quick health overview of the clients and APs and also drills down to an individual client or AP if any RF related issue needs troubleshooting. The feature provides further insight into throughput metrics of the system and Wi-Fi quality.

Figure 40 Performance Dashboard



- [Figure 41](#) provides detailed information of an AP, client, and application usage. You can further drill down to monitor client throughput, usage by WLAN, usage by applications, and related information.

Figure 41 Usage



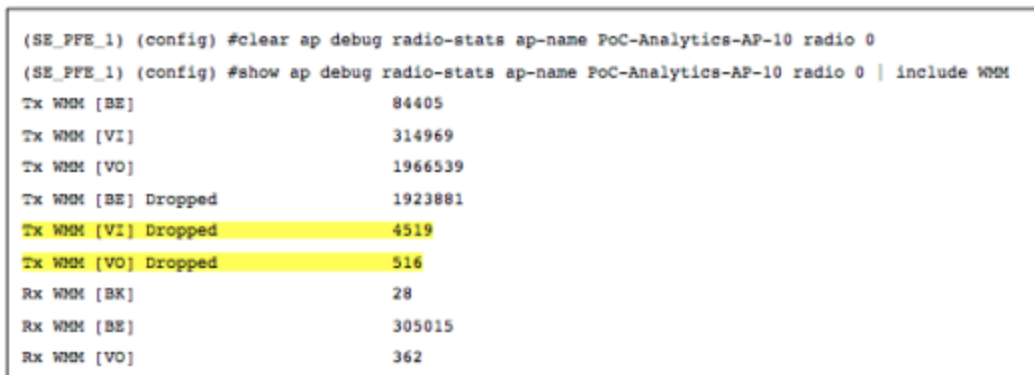
AP Troubleshooting

If the QoS is appropriately applied by the controller and users are still experiencing SfB issues use the following troubleshooting steps:

- RF packet captures provides 802.11 header related information and also helps in determining whether SfB traffic is sent from the AP to the client with the appropriate WMM-AC priority.
- The controller allows you to monitor radio statistics and provides details on the number of transmitted/dropped packets in WMM VO/VI queues. The number of packets dropped for SfB voice/video traffic should be low since this traffic gets prioritized over BE/BK traffic. If the count of the voice/video packet dropped is high, QoS does not apply to the AP.

The following figure illustrates an AP debug screen. Reset the AP debug counter and initiate new SfB voice/video calls on that AP to verify voice/video Tx WMM packet drop counters.

Figure 42 AP Debug Screen



```
(SE_PFE_1) (config) #clear ap debug radio-stats ap-name PoC-Analytics-AP-10 radio 0
(SE_PFE_1) (config) #show ap debug radio-stats ap-name PoC-Analytics-AP-10 radio 0 | include WMM
```

Tx WMM [BE]	84405
Tx WMM [VI]	314969
Tx WMM [VO]	1966539
Tx WMM [BE] Dropped	1923881
Tx WMM [VI] Dropped	4519
Tx WMM [VO] Dropped	516
Rx WMM [BK]	28
Rx WMM [BE]	305015
Rx WMM [VO]	362

Execute the following command for statistics on individual clients – `show ap debug client-stats <client-MAC>`.

RF Troubleshooting

- RF packet captures provide visibility to 802.11 headers to determine if SfB traffic is sent with the correct WMM-AC priority. If the wireless client is tagging the traffic, ensure that the WMM-AC upstream traffic priority from the client matches the DSCP tag configured on the client.

Also, ensure that the SfB traffic type is marked with the correct WMM-AC priority in the downstream direction from the AP to the client.

- RF packet captures provide useful information such as packet retries/failures, data rates, beacon rates, and so on. These RF environment attributes can be helpful to troubleshoot SfB related issues.

Wired Network Troubleshooting

- End-to-end QoS helps achieve optimum SfB performance. Ensure that the switches/routers in the wired network honor the QoS settings. There is a known issue with some of the wired switches such as Cisco 3750 that can reset the DSCP tag to 0 for all egress traffic if QoS is not enabled on that switch. Packet capture on the wired network will show DSCP tagging details.
- Ensure that the wired network has adequate bandwidth to handle the volume of SfB traffic. SfB bandwidth usage varies, but is predictable. For network bandwidth requirements of SfB codecs see [Network bandwidth requirements for media traffic in SfB Server 2013](#).

SfB Troubleshooting Using UCC Dashboard and CLI Commands

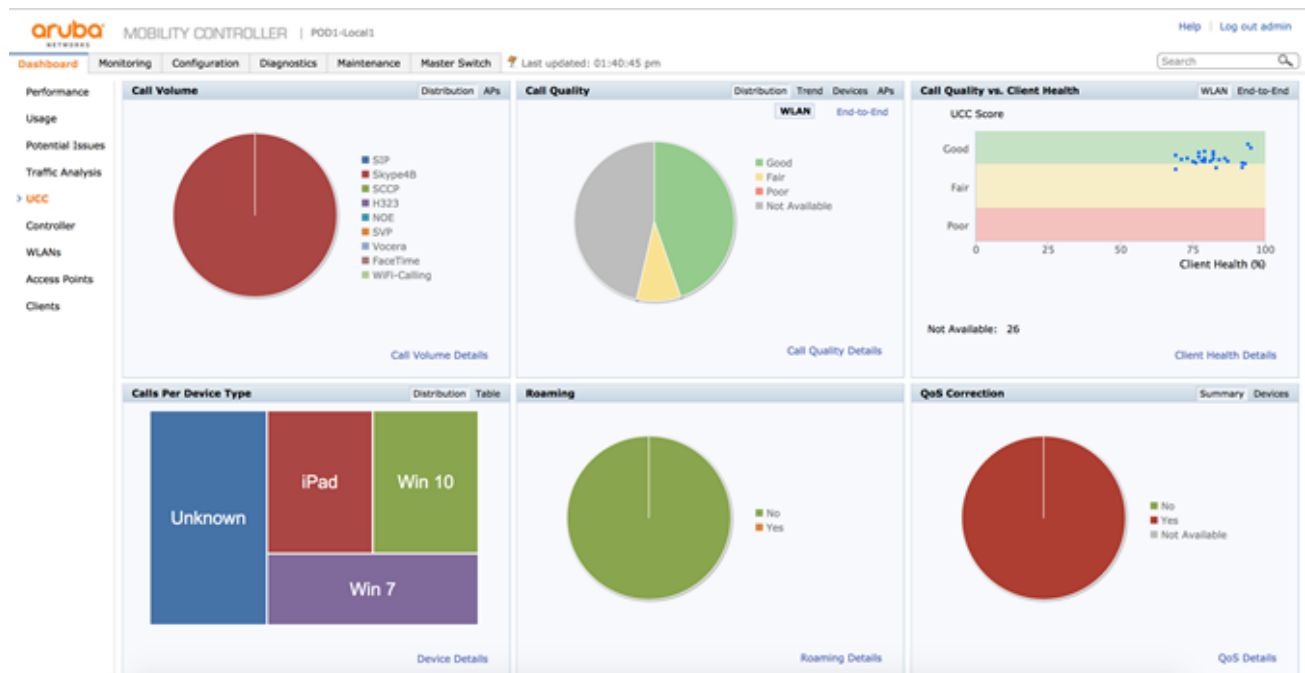
This section includes the following topics:

- [UCC Dashboard on page 76](#)
- [CLI Commands for SfB Troubleshooting on page 83](#)
- [UCC Troubleshooting on AirWave 8.2.1 on page 85](#)

UCC Dashboard

ArubaOS 6.4 provides a dashboard tab that displays system and client visibility into SfB calls. To access the new dashboard tab navigate to **Dashboard > UCC**.

Figure 43 UCC Dashboard



From the main UCC dashboard you can view system-wide UCC counters and statistics for call volume, call quality, call/client health correlation, per device call counters, call roaming statistics, and QoS correction statistics.

This section includes the following topics:

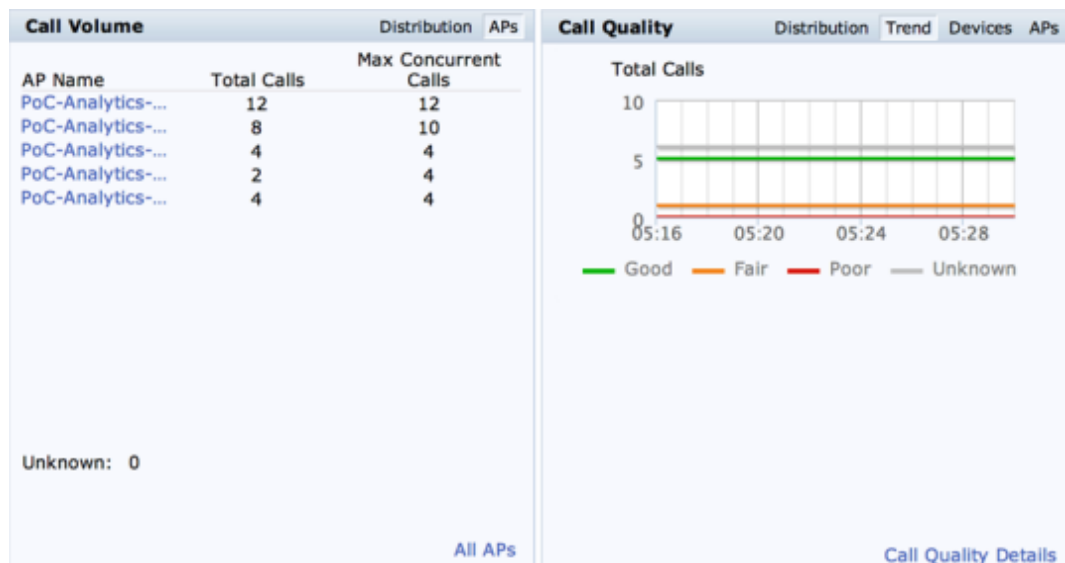
- [Call Distribution per AP and Call Quality Trend on page 77](#)
- [Call Quality per Device and Call Quality per AP on page 78](#)
- [WLAN Call Quality vs. Client Health Co-relation on page 78](#)
- [End-to-End Call Quality vs. Client Health Co-relation on page 79](#)
- [Call Detail Records on page 79](#)
- [WLAN Call Metrics on page 80](#)
- [End-to-End Call Metrics on page 80](#)
- [QoS Correction on page 81](#)
- [Per Client Troubleshooting on page 81](#)

Call Distribution per AP and Call Quality Trend

From the call volume section you can view:

- Call distribution by an AP.
- Trending call quality using the call quality feature.

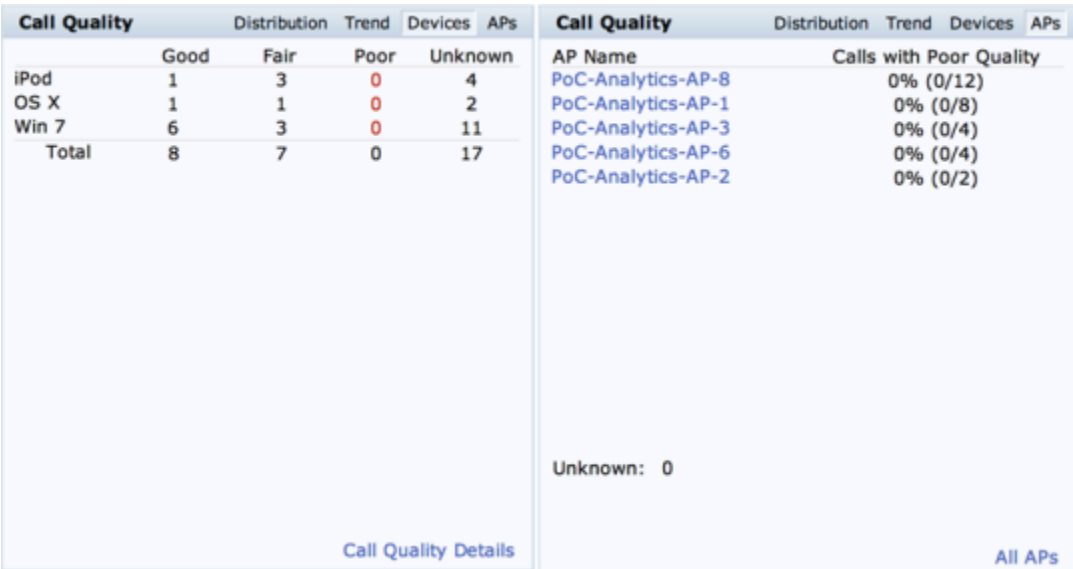
Figure 44 *Call Distribution per AP and Call Quality Trend*



Call Quality per Device and Call Quality per AP

Additional Call Quality tabs show quality by device types and poor calls by AP.

Figure 45 Call Quality per Device and Call Quality per AP



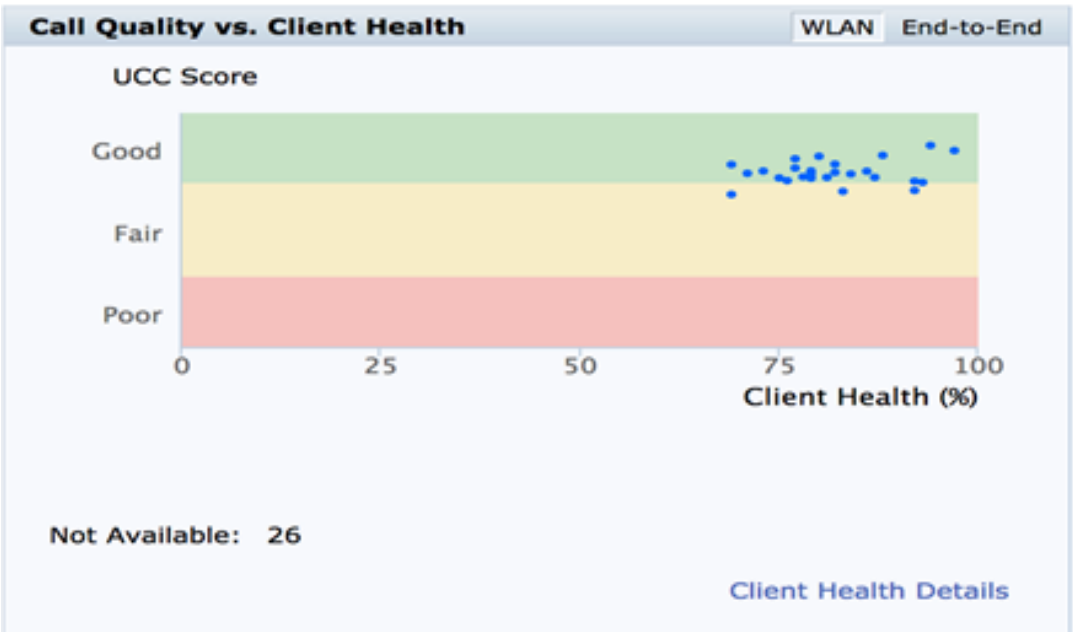
WLAN Call Quality vs. Client Health Co-relation

Aruba's SfB integration provides the ability to correlate call quality data with client health (Wi-Fi quality). The call quality co-relation can be done between:

- WLAN call metrics score (UCC score) and client health.
- End-to-end call metrics (MOS score) and client health.

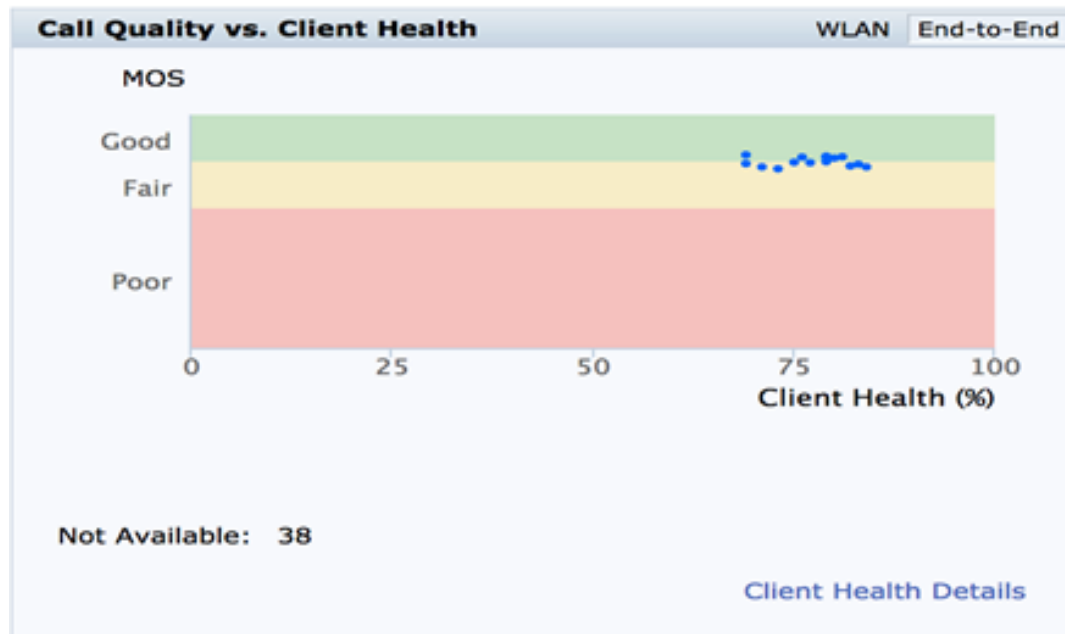
The correlation scatter plot in Figure 46 shows call metrics and Wi-Fi quality at a glance to quickly identify calls that have an issue.

Figure 46 WLAN Call Quality vs. Client Health Co-relation



End-to-End Call Quality vs. Client Health Co-relation

Figure 47 End-to-End Call Quality vs. Client Health Co-relation



Call Detail Records

Below are the snapshots from the controller UCC dashboard, which show:

- Call detail records.
- WLAN call metrics such as UCC score.
- End-to-end call metrics such as Mean Opinion Score (MOS), packet loss, jitter, delay, and so on.
- QoS correction parameters, which show that controller is able to correct the QoS tags depending on the traffic type such as voice or video.

Figure 48 Call Detail Records

Dashboard Monitoring Configuration Diagnostics Maintenance Master Switch Last updated: 02:11:45 pm										
Performance Wireless Call List (56)										
Usage	CDR ID	IP Address	Station MAC	Client Name	Destination IP	Called Party	ALG	Health(%)	State	Application
Potential Issues	1	10.70.218.12	60:45:bd:cf:a5:b0	john	10.70.218.13	jane	Skype48	78	Success	Voice
Traffic Analysis	2	10.70.218.13	60:45:bd:d1:ca:80	jane	10.70.218.12	john	Skype48	79	Success	Voice
> UCC	3	10.70.218.12	60:45:bd:cf:a5:b0	john	10.70.218.13	jane	Skype48	78	Success	Video
Controller	4	10.70.218.13	60:45:bd:d1:ca:80	jane	10.70.218.12	john	Skype48	79	Success	Video
WLANs	5	10.70.218.13	60:45:bd:d1:ca:80	jane	10.70.218.12	john	Skype48	--	Success	Voice
Access Points	6	10.70.218.12	60:45:bd:cf:a5:b0	john	10.70.218.13	jane	Skype48	--	Success	Voice
Clients	7	10.70.218.12	60:45:bd:cf:a5:b0	john	10.70.218.13	jane	Skype48	--	Success	Video
	8	10.70.218.13	60:45:bd:d1:ca:80	jane	10.70.218.12	john	Skype48	--	Success	Video
	9	10.70.218.12	60:45:bd:cf:a5:b0	john	10.70.218.13	jane	Skype48	84	Success	Voice
	10	10.70.218.12	60:45:bd:cf:a5:b0	john	10.70.218.13	jane	Skype48	84	Success	Video
	11	10.70.218.13	60:45:bd:d1:ca:80	jane	10.70.218.12	john	Skype48	73	Success	Voice
	12	10.70.218.13	60:45:bd:d1:ca:80	jane	10.70.218.12	john	Skype48	73	Success	Video
	13	10.70.218.12	60:45:bd:cf:a5:b0	john	10.70.218.13	jane	Skype48	77	Success	Voice
	14	10.70.218.12	60:45:bd:cf:a5:b0	john	10.70.218.13	jane	Skype48	77	Success	Video
	15	10.70.218.13	60:45:bd:d1:ca:80	jane	10.70.218.12	john	Skype48	69	Success	Voice
	16	10.70.218.13	60:45:bd:d1:ca:80	jane	10.70.218.12	john	Skype48	69	Success	Video
	17	10.70.218.14	a4:67:06:2a:ce:f3	Luke	10.70.218.11	user1	Skype48	86	Success	Voice

WLAN Call Metrics

WLAN call metrics is captured below. UCC score is a WLAN call metrics that is proprietary to Aruba and is calculated on the controller. Packet loss, jitter, and delay are monitored on the controller for a client for a specific call leg. UCC score is calculated based on these call metrics parameters.

UCC score is only available for Voice calls.

Figure 49 WLAN Call Metrics

Dashboard

Monitoring

Configuration

Diagnostics

Maintenance

Master Switch

Last updated: 02:11:45 pm

Performance

Usage

Potential Issues

Traffic Analysis

> UCC

Controller

WLANs

Access Points

Clients

Wireless Call List (56)

CDR ID	Application	UCC Score	UCC Band	WLAN		
				Delay (msec)	Jitter (msec)	Packet Loss(%)
1	Voice	72.73	Good	1.02	0.1	4.12
2	Voice	72.1	Good	1.05	0.14	0.57
3	Video	--	Not Available	--	--	--
4	Video	--	Not Available	--	--	--
5	Voice	--	Good	--	--	--
6	Voice	--	Fair	--	--	--
7	Video	--	Not Available	--	--	--
8	Video	--	Not Available	--	--	--
9	Voice	73.93	Good	2.3	0.68	0.52
10	Video	--	Not Available	--	--	--
11	Voice	75.15	Good	0.81	0.09	1.17
12	Video	--	Not Available	--	--	--
13	Voice	80.42	Good	1.14	0.1	0
14	Video	--	Not Available	--	--	--
15	Voice	77.96	Good	2.21	0.02	0
16	Video	--	Not Available	--	--	--

End-to-End Call Metrics

End-to-end call metrics is captured below. End-to-end call metrics such as MOS is received from SfB Server infrastructure through SfB SDN API on the controller.

MOS score is only available for Voice calls.

Figure 50 End-to-End Call Metrics

Dashboard	Monitoring	Configuration	Diagnostics	Maintenance	Master Switch	Last updated: 02:12
Performance	Wireless Call List (60)					
Usage	CDR ID	MOS	MOS Band	Delay (msec)	End-to-End	
Potential Issues					Jitter (msec)	Packet Loss(%)
Traffic Analysis	1	--	Not Available	17	8	1.48
> UCC	2	4.09	Good	15	9	0.4
Controller	3	--	Not Available	20	8	2.51
WLANs	4	--	Not Available	23	1	0.48
Access Points	5	4.06	Good	40	7	0.13
Clients	6	--	Not Available	39	8	0
	7	--	Not Available	10	6	2.45
	8	--	Not Available	15	1	0.18
	9	3.88	Fair	42	7	0.5
	10	--	Not Available	14	11	1.05
	11	3.84	Fair	29	7	1.1
	12	--	Not Available	11	4	1.03
	13	--	Not Available	36	6	0.16
	14	--	Not Available	38	14	0.35
	15	4.14	Good	22	10	1.45
	16	--	Not Available	31	10	1.23
	17	--	Not Available	15	8	0.18

QoS Correction

QoS correction is captured below. Controller applies the correct QoS values depending on traffic type such as Voice or video.

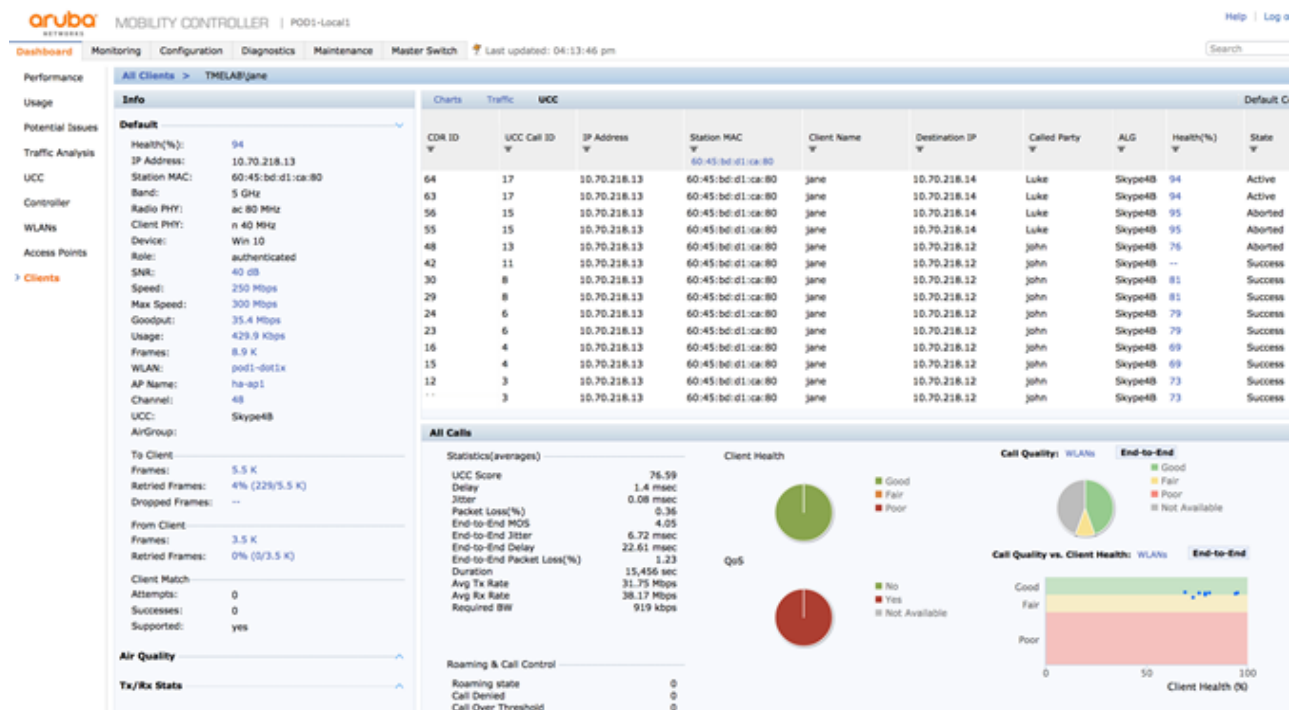
Figure 51 QoS Correction

Dashboard	Monitoring	Configuration	Diagnostics	Maintenance	Master Switch	Last updated: 1
Performance	Wireless Call List (60)					
Usage	CDR ID	Client WMM AC	Modified WMM AC	Client DSCP	Modified DSCP	
Potential Issues	1	0	6	0	46	
Traffic Analysis	2	0	6	0	46	
> UCC	3	0	5	0	34	
Controller	4	0	5	0	34	
WLANs	5	0	6	0	46	
Access Points	6	0	6	0	46	
Clients	7	0	5	0	34	
	8	0	5	0	34	
	9	0	6	0	46	
	10	0	5	0	34	
	11	0	6	0	46	
	12	0	5	0	34	
	13	0	6	0	46	
	14	0	5	0	34	
	15	0	6	0	46	
	16	0	5	0	34	
	17	0	6	0	46	

Per Client Troubleshooting

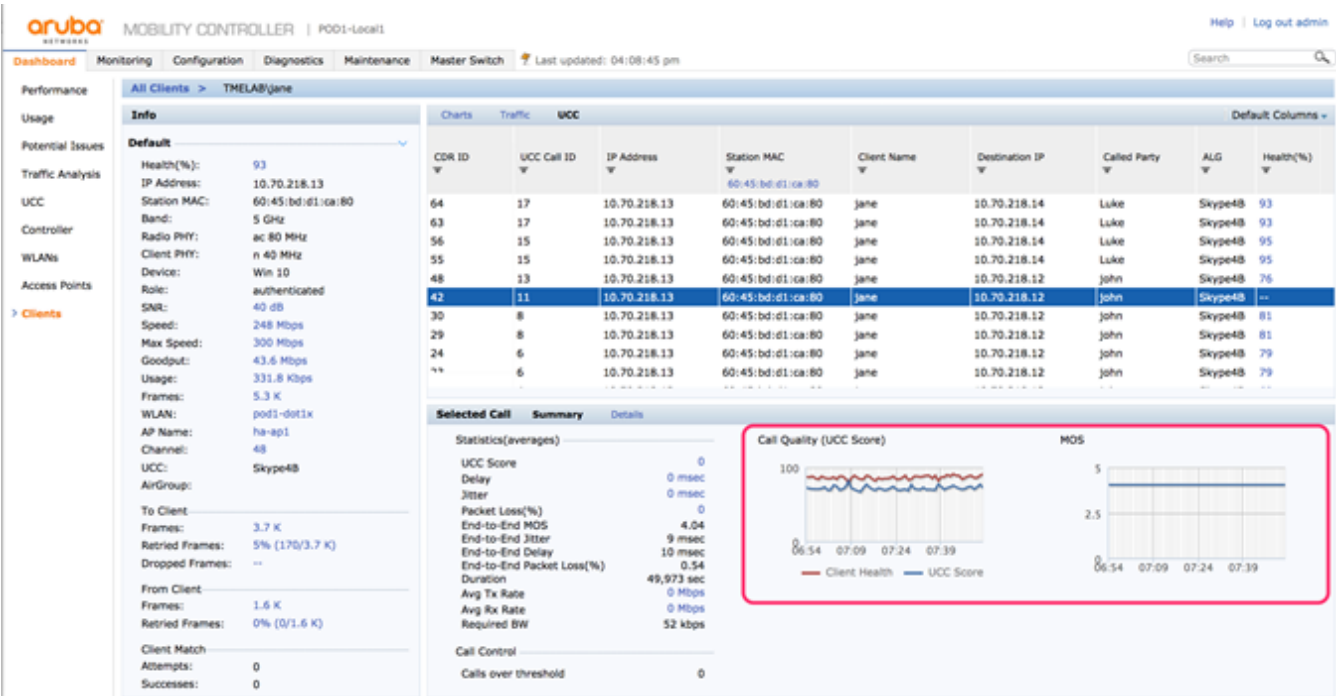
The UCC dashboard provides a root cause analysis of bad calls by allowing you to search for a user or device and obtain details about the device, call, network, and location.

Figure 52 Per Client Troubleshooting



Per Client Call Quality Trend

Figure 53 Per Client Call Quality Trend



CLI Commands for SfB Troubleshooting

The following troubleshooting commands are used to gather communication between the controller and SfB server, SfB call status, and call detail records.

- **show ucc trace-buffer skype4b** - This command is used to record activities of SfB clients. A maximum of 256 entries are recorded in a circular buffer to save memory. Events such as establishing voice, video, desktop sharing, and file transfer are recorded. Each CLI entry display includes IP, MAC, client name, time stamp, called-party, media-type, AP name, and call status. The purpose of this command is to keep track of individual sessions with respect to their handling on the Wi-Fi network.

Figure 54 *show ucc trace-buffer skype4b*

```
(POD1-Local1) #show ucc trace-buffer skype4b
```

Skype4B Voice Client(s) Message Trace												
Client IP	Client MAC	Client Name	Direction	Event Time	BSSID	Called To	CAC-Status	Media Type	AP Name	Src Port	Dest Port	Call Status
10.70.218.14	a4:67:06:2a:ce:f3	Luke	OG	Aug 26 10:25:10	18:64:72:40:b3:b0	john	PASS	Voice/Video	ha-ap1	25922/29656	15821/16921	After call update
10.70.218.14	a4:67:06:2a:ce:f3	Luke	OG	Aug 26 10:25:10	18:64:72:40:b3:b0	john	PASS	Voice/Video	ha-ap1	25922/29656	15821/16921	Before call update
10.70.215.241	0a:46:d7:f1:00:00	john	IC	Aug 26 10:25:10	00:00:00:00:00:00	Luke	PASS	Voice/Video		15821/16921	25922/29656	After call update
10.70.215.241	0a:46:d7:f1:00:00	john	IC	Aug 26 10:25:10	00:00:00:00:00:00	Luke	PASS	Voice/Video		15821/16921	25922/29656	Before call update
10.70.215.241	0a:46:d7:f1:00:00	john	IC	Aug 26 10:24:58	00:00:00:00:00:00	Luke	PASS	Voice/Video		15821/16921	25922/29656	After call update
10.70.215.241	0a:46:d7:f1:00:00	john	IC	Aug 26 10:24:58	00:00:00:00:00:00	Luke	PASS	Voice		15821	25922	Before call update
10.70.218.14	a4:67:06:2a:ce:f3	Luke	OG	Aug 26 10:24:58	18:64:72:40:b3:b0	john	PASS	Voice/Video	ha-ap1	25922/29656	15821/16921	After call update
10.70.218.14	a4:67:06:2a:ce:f3	Luke	OG	Aug 26 10:24:58	18:64:72:40:b3:b0	john	PASS	Voice	ha-ap1	25922	15821	Before call update
10.70.215.241	0a:46:d7:f1:00:00	john	IC	Aug 26 10:24:57	00:00:00:00:00:00	Luke	PASS	Voice		15821	25922	After call update
10.70.215.241	0a:46:d7:f1:00:00	john	IC	Aug 26 10:24:57	00:00:00:00:00:00	Luke	PASS	Voice		15821	25922	Before call update
10.70.218.14	a4:67:06:2a:ce:f3	Luke	OG	Aug 26 10:24:57	18:64:72:40:b3:b0	john	PASS	Voice	ha-ap1	25922	15821	After call update
10.70.218.14	a4:67:06:2a:ce:f3	Luke	OG	Aug 26 10:24:57	18:64:72:40:b3:b0	john	PASS	Voice	ha-ap1	25922	15821	Before call update
10.70.215.241	0a:46:d7:f1:00:00	john	IC	Aug 26 10:24:52	00:00:00:00:00:00	Luke	PASS	Voice		15821	25922	Start of call
10.70.218.14	a4:67:06:2a:ce:f3	Luke	OG	Aug 26 10:24:52	18:64:72:40:b3:b0	john	PASS	Voice	ha-ap1	25922	15821	Start of call
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:36	18:64:72:40:b3:b0	user1	PASS	Voice/Video	ha-ap1	25574/27964	18280/28580	InCallQuality Update
10.70.215.240	0a:46:d7:f0:00:00	user1	OG	Aug 26 10:24:36	00:00:00:00:00:00	jane	PASS	Voice/Video		18280/28580	25574/27964	InCallQuality Update
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:36	18:64:72:40:b3:b0	user1	PASS	Voice/Video	ha-ap1	25574/27964	18280/28580	InCallQuality Update
10.70.215.240	0a:46:d7:f0:00:00	user1	OG	Aug 26 10:24:36	00:00:00:00:00:00	jane	PASS	Voice/Video		18280/28580	25574/27964	InCallQuality Update
10.70.215.240	0a:46:d7:f0:00:00	user1	OG	Aug 26 10:24:36	00:00:00:00:00:00	jane	PASS	Voice/Video		18280/28580	25574/27964	InCallQuality Update
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:36	18:64:72:40:b3:b0	user1	PASS	Voice/Video	ha-ap1	25574/27964	18280/28580	InCallQuality Update
10.70.215.240	0a:46:d7:f0:00:00	user1	OG	Aug 26 10:24:36	00:00:00:00:00:00	jane	PASS	Voice/Video		18280/28580	25574/27964	InCallQuality Update
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:36	18:64:72:40:b3:b0	user1	PASS	Voice/Video	ha-ap1	25574/27964	18280/28580	InCallQuality Update
10.70.215.240	0a:46:d7:f0:00:00	user1	OG	Aug 26 10:24:36	00:00:00:00:00:00	jane	PASS	Voice/Video		18280/28580	25574/27964	InCallQuality Update
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:23	00:00:00:00:00:00	jane	PASS	Voice/Video		18280/28580	25574/27964	Before call update
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:23	18:64:72:40:b3:b0	user1	PASS	Voice/Video	ha-ap1	25574/27964	18280/28580	After call update
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:23	18:64:72:40:b3:b0	user1	PASS	Voice/Video	ha-ap1	25574/27964	18280/28580	Before call update
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:19	18:64:72:40:b3:b0	user1	PASS	Voice/Video	ha-ap1	25574/27964	18280/28580	After call update
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:19	18:64:72:40:b3:b0	user1	PASS	Voice	ha-ap1	25574	18280	Before call update
10.70.215.240	0a:46:d7:f0:00:00	user1	OG	Aug 26 10:24:19	00:00:00:00:00:00	jane	PASS	Voice/Video		18280/28580	25574/27964	After call update
10.70.215.240	0a:46:d7:f0:00:00	user1	OG	Aug 26 10:24:19	00:00:00:00:00:00	jane	PASS	Voice		18280	25574	Before call update
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:19	18:64:72:40:b3:b0	user1	PASS	Voice	ha-ap1	25574	18280	After call update
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:19	18:64:72:40:b3:b0	user1	PASS	Voice	ha-ap1	25574	18280	Before call update
10.70.215.240	0a:46:d7:f0:00:00	user1	OG	Aug 26 10:24:19	00:00:00:00:00:00	jane	PASS	Voice		18280	25574	After call update
10.70.215.240	0a:46:d7:f0:00:00	user1	OG	Aug 26 10:24:19	00:00:00:00:00:00	jane	PASS	Voice		18280	25574	Before call update
10.70.218.13	60:45:bd:d1:ca:80	jane	IC	Aug 26 10:24:01	18:64:72:40:b3:b0	user1	PASS	Voice	ha-ap1	25574	18280	Start of call
10.70.215.240	0a:46:d7:f0:00:00	user1	OG	Aug 26 10:24:01	00:00:00:00:00:00	jane	PASS	Voice		18280	25574	Start of call

- **show ucc client-info** - This command provides details about clients that are actively using SfB. An entry is created for clients that have actively participated in voice, video, desktop-sharing, or file-sharing sessions.

Figure 55 *show ucc client-info*

```
(POD1-Local1) (config) #show ucc client-info
```

Client Status:									
Client IP	Client MAC	Client Name	ALG	Server(IP)	Registration State	Call Status	AP Name	Flags	Device Type
10.70.218.13	60:45:bd:d1:ca:80	jane	Skype4B		REGISTERED	In-Call	ha-ap1		Win 10
10.70.218.12	60:45:bd:cf:a5:b0	john	Skype4B		REGISTERED	In-Call	ha-ap1		Win 10
10.70.218.11	24:77:03:c6:be:6c	user1	Skype4B		REGISTERED	In-Call	ha-ap1		Win 7
10.70.218.14	a4:67:06:2a:ce:f3	Luke	Skype4B		REGISTERED	In-Call	ha-ap1		iPad

Flags: V - Visitor, A - Away, W - Wired, R - Remote, B - Blocked, E - External

- **show ucc client-info** **stalf** the filter with station Media Access Control (MAC) is applied on this command, it provides a detailed report specific to that client as shown in [Figure 56](#) below.

Figure 56 show ucc client-info sta

```
(P001-Local1) (config) #show ucc client-info sta 60:45:bd:d1:ca:80
```

Station Report:

Client IP	Client MAC	Client Name	AP-Name	SNR	Avg Tx Rate(Mbps)	Tx Drop(%)	Tx Retry(%)	Avg Rx Rate(Mbps)	Rx Retry(%)	Un-steerable (reason)
10.70.218.13	60:45:bd:d1:ca:80	jane	ha-ap1	44	55.10	0.06	2.52	46.21	0.00	NA

Active Calls:

CDR ID	UCC Call ID	Client IP	Client Name	ALG	Dir	Called To	Dur(sec)	Orig-Time	Status	Call Type	Client Health	UCC Score	UCC-Band	MOS	MOS-Band
84	22	10.70.218.13	jane	Skype4B	IC	Luke	512	Aug 26 10:37:28	ACTIVE	Video	97	NA	NA	NA	NA
83	22	10.70.218.13	jane	Skype4B	IC	Luke	512	Aug 26 10:37:28	ACTIVE	Voice	97	85.41	Good	NA	NA

Call History:

CDR ID	UCC Call ID	Client IP	Client Name	ALG	Dir	Called To	Dur(sec)	Orig-Time	Status	Reason	Call Type	Client Health	UCC Score	UCC-Band	MOS	MOS-Band
72	19	10.70.218.13	jane	Skype4B	IC	user1	684	Aug 26 10:24:19	SUCC	Terminated	Video	95	NA	NA	NA	NA
70	19	10.70.218.13	jane	Skype4B	IC	user1	702	Aug 26 10:24:01	SUCC	Terminated	Voice	95	85.47	Good	4.22	Good
64	17	10.70.218.13	jane	Skype4B	IC	Luke	6876	Aug 25 14:14:12	ABORTED	Inactivity	Video	92	NA	NA	NA	NA
63	17	10.70.218.13	jane	Skype4B	IC	Luke	6876	Aug 25 14:14:12	ABORTED	Inactivity	Voice	92	86.15	Good	4.06	Good
56	15	10.70.218.13	jane	Skype4B	IC	Luke	13700	Aug 25 10:25:50	ABORTED	Inactivity	Video	95	NA	NA	NA	NA
55	15	10.70.218.13	jane	Skype4B	IC	Luke	13700	Aug 25 10:25:50	ABORTED	Inactivity	Voice	95	85.13	Good	4.10	Good
48	13	10.70.218.13	jane	Skype4B	IC	john	8190	Aug 25 07:55:09	ABORTED	Inactivity	Voice	76	71.10	Good	4.09	Good

- **show ucc call-info cdrs** - This command provides the call detail records (CDRs) for SfB voice, video, desktop sharing, and file transfer call. It also displays WLAN call quality metrics such as UCC score and end-to-end call quality metrics such as MOS that is received from SfB server.

Figure 57 show ucc call-info cdrs

```
(P001-Local1) #show ucc call-info cdrs
```

CDR:

CDR ID	UCC Call ID	Client IP	Client MAC	Client Name	ALG	Dir	Called to	Dur(sec)	Orig Time	Status	Reason	Call Type	Client Health	UCC Score	UCC-Band	MOS	MOS-Band
76	20	10.70.215.241	NA	john	Skype4B	IC	Luke	175	Aug 26 10:24:58	ACTIVE	NA	Video	0	NA	NA	NA	NA
75	20	10.70.218.14	a4:67:06:2a:ce:f3	Luke	Skype4B	OG	john	175	Aug 26 10:24:58	ACTIVE	NA	Video	78	NA	NA	NA	NA
74	20	10.70.215.241	NA	john	Skype4B	IC	Luke	181	Aug 26 10:24:52	ACTIVE	NA	Voice	0	NA	NA	NA	NA
73	20	10.70.218.14	a4:67:06:2a:ce:f3	Luke	Skype4B	OG	john	181	Aug 26 10:24:52	ACTIVE	NA	Voice	78	81.71	Good	NA	NA
72	19	10.70.218.13	60:45:bd:d1:ca:80	jane	Skype4B	IC	user1	214	Aug 26 10:24:19	ACTIVE	NA	Video	95	NA	NA	NA	NA
71	19	10.70.215.240	NA	user1	Skype4B	OG	jane	214	Aug 26 10:24:19	ACTIVE	NA	Video	0	NA	NA	NA	NA
70	19	10.70.218.13	60:45:bd:d1:ca:80	jane	Skype4B	IC	user1	232	Aug 26 10:24:01	ACTIVE	NA	Voice	95	86.87	Good	4.21	Good
69	19	10.70.215.240	NA	user1	Skype4B	OG	jane	232	Aug 26 10:24:01	ACTIVE	NA	Voice	0	NA	NA	3.97	Good
68	18	10.70.218.11	24:77:03:c6:be:6c	user1	Skype4B	IC	john	483	Aug 25 14:19:27	SUCC	Terminated	Video	76	NA	NA	NA	NA
67	18	10.70.218.11	24:77:03:c6:be:6c	user1	Skype4B	IC	john	483	Aug 25 14:19:27	SUCC	Terminated	Voice	76	75.76	Good	4.06	Good
66	18	10.70.218.12	60:45:bd:cf:a5:b0	john	Skype4B	OG	user1	483	Aug 25 14:19:27	SUCC	Terminated	Video	93	NA	NA	NA	NA
65	18	10.70.218.12	60:45:bd:cf:a5:b0	john	Skype4B	OG	user1	483	Aug 25 14:19:27	SUCC	Terminated	Voice	93	81.73	Good	4.10	Good
64	17	10.70.218.13	60:45:bd:d1:ca:80	jane	Skype4B	IC	Luke	6876	Aug 25 14:14:12	ABORTED	Inactivity	Video	92	NA	NA	NA	NA
63	17	10.70.218.13	60:45:bd:d1:ca:80	jane	Skype4B	IC	Luke	6876	Aug 25 14:14:12	ABORTED	Inactivity	Voice	92	86.15	Good	4.06	Good
62	17	10.70.218.14	a4:67:06:2a:ce:f3	Luke	Skype4B	OG	jane	6876	Aug 25 14:14:12	ABORTED	Inactivity	Video	86	NA	NA	NA	NA
61	17	10.70.218.14	a4:67:06:2a:ce:f3	Luke	Skype4B	OG	jane	6876	Aug 25 14:14:12	ABORTED	Inactivity	Voice	86	88.56	Good	NA	NA

- **show ucc call-info cdrs detail** - The call info call detail records (CDRs) detail option provides additional visibility to detail WLAN and end-to-end call metrics, RF statistics such as SNR, Tx/Rx packet retries, and data rates, and so on.

Figure 58 show ucc call-info cdrs detail

```
(P001-Local1) (config) #show ucc call-info cdrs detail
```

CDR-Detail:

CDR ID	UCC Call ID	AP Name	Re-Assoc	UCC Score	UCC-Band	WLAN Delay(ms)/Jitter(ms)/PktLoss(%)	SNR	Avg Tx Rate(Mbps)	Tx Drop(%)	Tx Retry(%)	Avg Rx Rate(Mbps)	Rx Retry(%)	MOS	MOS-Band	End-to-End
84	22	ha-ap1	0	NA	NA	NA/NA/NA	43	55.09	0.06	2.52	46.17	0.00	NA	NA	NA/2.00/0.32
83	22	ha-ap1	0	85.74	Good	0.54/0.01/0.01	43	55.09	0.06	2.52	46.17	0.00	NA	NA	NA/8.00/0.43
82	22	ha-ap1	0	NA	NA	NA/NA/NA	37	19.00	0.09	10.71	43.64	4.39	NA	NA	9.00/2.00/0.14
81	22	ha-ap1	0	80.66	Good	0.64/0.06/0.00	37	19.00	0.09	10.71	43.64	4.39	NA	NA	14.00/4.00/0.00
80	21	ha-ap1	0	NA	NA	NA/NA/NA	43	35.81	0.34	3.41	40.75	0.02	NA	NA	21.00/7.00/0.20
79	21	ha-ap1	0	85.21	Good	0.47/0.01/0.02	43	35.81	0.34	3.41	40.75	0.02	NA	NA	8.00/7.00/0.85
78	21	ha-ap1	0	NA	NA	NA/NA/NA	40	20.03	0.48	14.67	63.65	0.04	NA	NA	NA/8.00/0.33
77	21	ha-ap1	0	85.21	Good	0.53/0.01/0.03	40	20.03	0.48	14.67	63.65	0.04	3.85	Good	NA/9.00/2.57
76	20	NA	0	NA	NA	NA/NA/NA	NA	NA	NA	NA	NA	NA	NA	NA	NA/0.00/1.94
75	20	ha-ap1	0	NA	NA	NA/NA/NA	36	19.01	0.09	10.73	43.65	4.38	NA	NA	15.00/7.00/0.11
74	20	NA	0	NA	NA	NA/NA/NA	NA	NA	NA	NA	NA	NA	NA	NA	NA/9.00/0.27
73	20	ha-ap1	0	81.69	Good	0.67/0.05/0.17	36	19.01	0.09	10.73	43.65	4.38	NA	NA	9.00/4.00/0.11
72	19	NA	0	NA	NA	NA/NA/NA	40	55.12	0.06	2.51	46.24	0.00	NA	NA	23.00/1.00/0.04
71	19	NA	0	NA	NA	NA/NA/NA	NA	NA	NA	NA	NA	NA	NA	NA	29.00/11.00/0.00
70	19	ha-ap1	0	85.47	Good	0.57/0.00/0.16	40	55.12	0.06	2.51	46.24	0.00	4.22	Good	27.00/2.00/0.02

UCC Troubleshooting on AirWave 8.2.1

Aruba controllers running ArubaOS 6.4 and later versions send UCC data to AirWave. The following set of UCC data is available on AirWave:

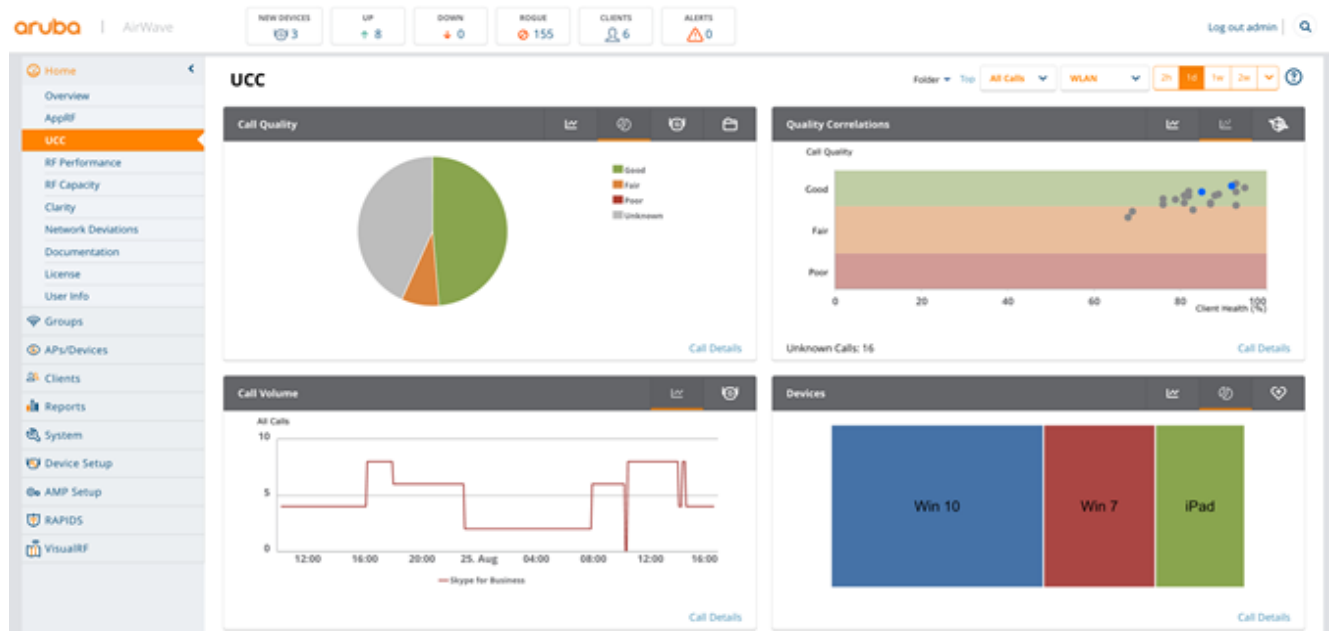
- **Real time call quality (UCC score) Analysis** - Includes call quality trend, call quality distribution per AP.
- **Call Detail Records** - Displays client details, call traffic type, WMM, and DSCP details.
- **Call quality co-relation** - Displays real time call quality vs. client health co-relation.
- **Call quality visibility per device type** - Displays device models, OS, Wi-Fi driver version, speaker and microphone glitch rates for the end device.

This section includes the following topics:

- [UCC Dashboard on page 85](#)
- [Call Detail Records on page 86](#)
- [End-to-end Call Quality Analysis on page 86](#)

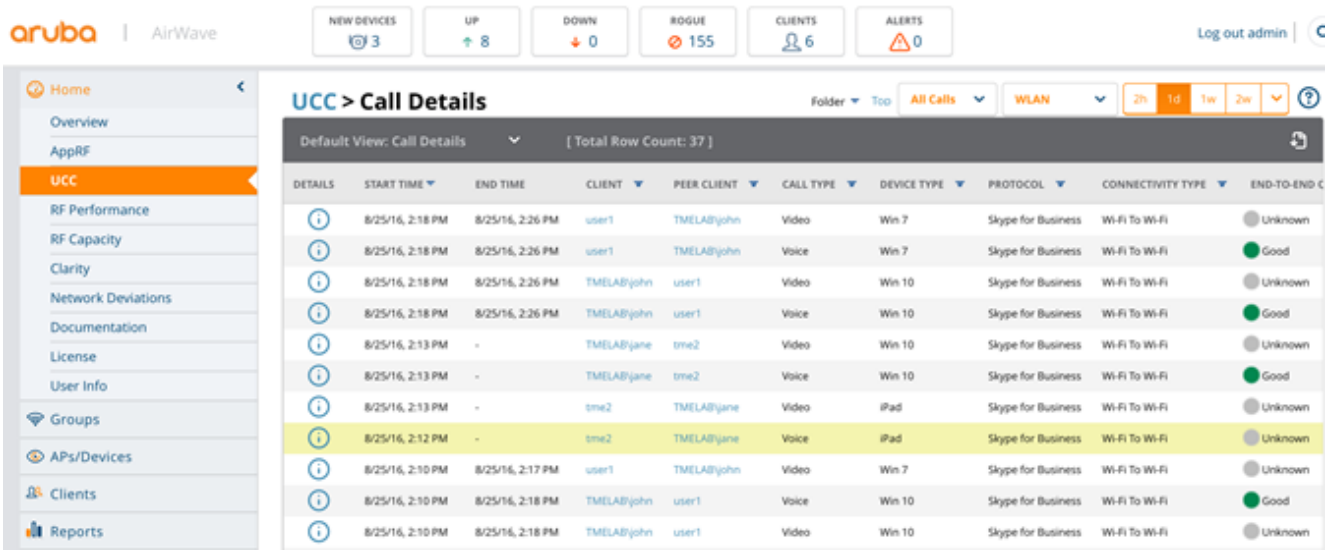
UCC Dashboard

Figure 59 UCC Dashboard



Call Detail Records

Figure 60 Call Detail Records



End-to-end Call Quality Analysis

Figure 61 Client Device

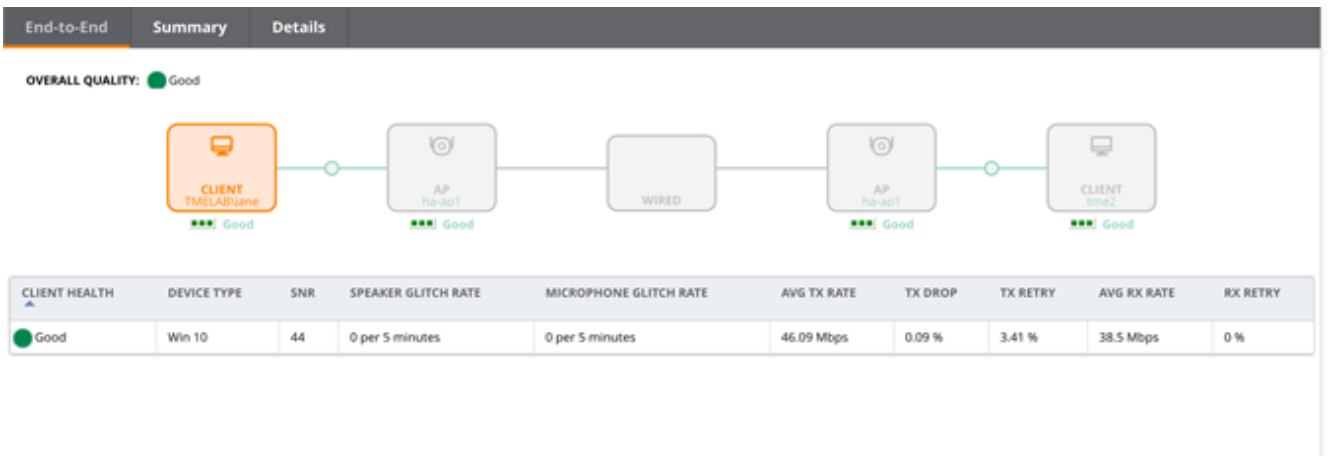


Figure 62 Access Point

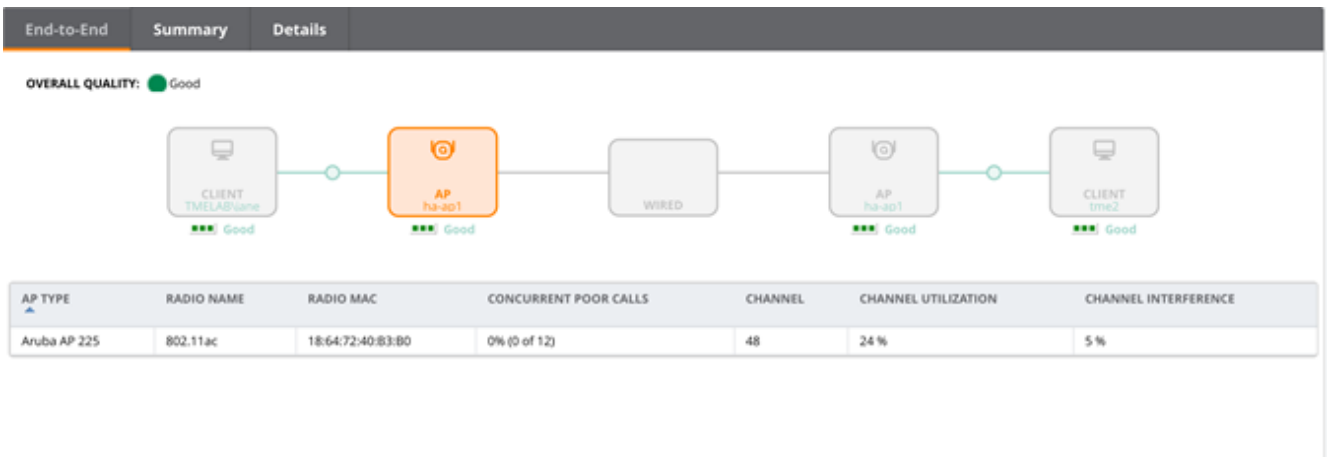


Figure 63 Call Quality Summary and Call Quality Trend



Figure 64 End-to-end, WLAN, and Client Device Microphone Call Metrics

End-to-End	Summary	Details
End To End		WLAN
MOS Score:	4.1	WLAN Delay: 0.52 msec
End To End Delay:	0	WLAN Jitter: 0.01 msec
End To End Jitter:	7 msec	WLAN Packet Loss: 0.26 %
End To End Packet Loss:	0.58 %	SNR: 44
Recieve Listen MOS:	0	Channel Utilization: 24 %
Send Listen MOS:	0	Channel: 48
Healer Packet Drop Ratio:	0	Channel Interference: 5 %
Burst Gap Duration:	0	Avg Tx Rate: 46.09 Mbps
Burst Gap Density:	0	Tx Drop: 0.09 %
Burst Duration:	0	Tx Retry: 3.41 %
Burst Density:	0	Avg Rx Rate: 38.5 Mbps
		Rx Retry: 0
		Required Bandwidth: -
		Microphone Details
		Microphone: Front LifeCam
		Capture Device Driver: Microsoft: 1.0.104.0
		Microphone Glitch Rate: 0
		Microphone timestamp error: 0.02 msec
		Echo Percentage Before Noise Canc... 0
		Echo Percentage After Noise Canc... 0

Figure 65 Client Device End Point Details and Speaker Call Metrics

End-to-End	Summary	Details			
Receive Listen MOS: 0		Channel: 48	Echo Percentage After Noise Canc... 0		
Send Listen MOS: 0		Channel Interference: 5 %			
Healer Packet Drop Ratio: 0		Avg Tx Rate: 46.09 Mbps			
Burst Gap Duration: 0		Tx Drop: 0.09 %			
Burst Gap Density: 0		Tx Retry: 3.41 %			
Burst Duration: 0		Avg Rx Rate: 38.5 Mbps			
Burst Density: 0		Rx Retry: 0			
		Required Bandwidth: -			

Speaker Details

Speaker:	Speakers (High Definition Audio Devi...
Render Device Driver:	Microsoft: 1.0.104.0
Speaker Glitch Rate:	0
Recieve Noise Level:	-67 dBov
Recieve Signal Level:	-23 dBov
Speaker timestamp error:	0

End Point Details

Client IP:	10.70.218.13
Peer IP Address:	10.70.218.14
Wifi Device Driver:	Microsoft Wi-Fi Direct Virtual Adapte...
Wifi Device Driver Version:	Microsoft: 10.0.10586.0;Marvell Semi...
OS:	Windows 10.0.10586 SP: 0.0 Type: 1[...
CPU:	Intel(R) Core(TM) i5-3317U CPU @ 1...
CPU Cores:	2
CPU Processing Speed:	1.696 GHz
Client Link Speed:	0.006 Gbps
User Agent:	UCCAPI/16.0.4339.1000 OC/16.0.435...
Source Pool:	pool.tmelab.net
MAC Address:	60:45:BD:D1:CA:80

Figure 66 In Call Quality Metrics Minute by Minute Analysis

End-to-End	Summary	Details						
START TIME ▼	MOS SCORE	END TO END DELAY (MSEC)	END TO END JITTER (MSEC)	END TO END PACKET LOSS (%)	UCC SCORE	WLAN DELAY (MSEC)	WLAN JITTER (MSEC)	WLAN PAI
8/25/16, 2:12 PM	4.1	0	7	0.58	85.13	0.52	0.01	0.26
8/25/16, 2:12 PM	4.1	0	7	0.58	85.13	0.52	0.01	0.26
8/25/16, 2:12 PM	4.1	0	9	0.41	85.97	0.5	0	0.02
8/25/16, 2:11 PM	0	0	7	0.58	85.97	0.5	0	0.02
8/25/16, 2:11 PM	0	0	7	0.58	89.84	0.44	0	0.06
8/25/16, 2:09 PM	0	0	7	0.58	86.7	0.48	0.02	0.2
8/25/16, 2:08 PM	0	0	7	0.58	85.08	0.49	0	0.33
8/25/16, 2:07 PM	0	0	7	0.58	86.24	0.43	0	0.48
8/25/16, 2:06 PM	0	0	7	0.58	89.51	0.37	0	0
8/25/16, 2:05 PM	0	0	7	0.58	89.47	0.38	0	0
8/25/16, 2:04 PM	0	0	7	0.58	90.27	0.41	0	0.03
8/25/16, 2:03 PM	0	0	7	0.58	90.48	0.42	0	0
8/25/16, 2:02 PM	0	0	7	0.58	90.38	0.4	0	0.03
8/25/16, 2:01 PM	0	0	7	0.58	89.32	0.45	0	0.15

The above data is useful to troubleshoot a SfB issue on a per client basis. AirWave stores historical data and can provide insight to call quality and call volume trend over a period of time.

SfB Troubleshooting on Network Optimizer

Network Optimizer provides several tools for troubleshooting the activity in a network using SfB. The three main tools are the session details view, the location heat map, and the Top 10 reporting system.

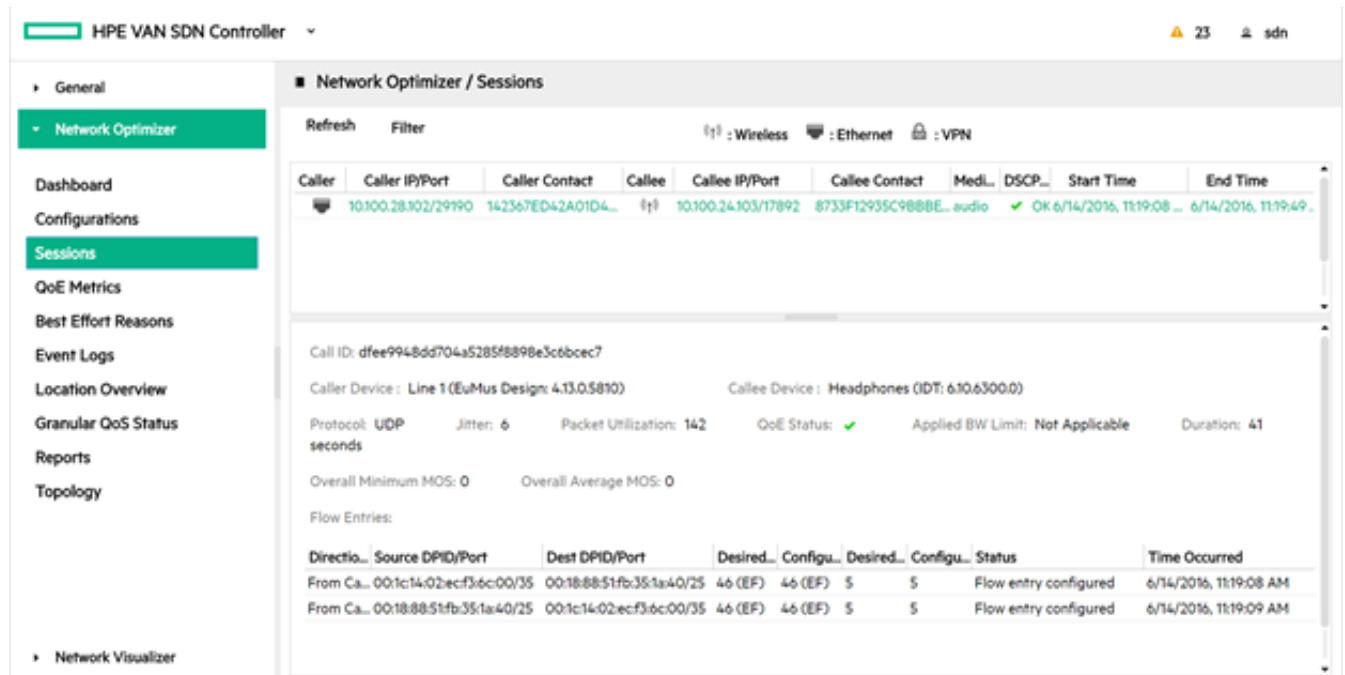
This section includes the following topics:

- [Session Details on page 89](#)
- [Location Heat Map on page 90](#)
- [Top 10 Reports on page 91](#)
- [OpenFlow Troubleshooting on page 92](#)

Session Details

The session details panel provides details on the calls placed that Network Optimizer has received from the Skype for Business SDN API. Details include call quality, MOS, Jitter, and much other information. One topic to note is that when wireless or VPN users are connected, Network Optimizer also displays these by showing a related icon, such as in [Figure 67](#).

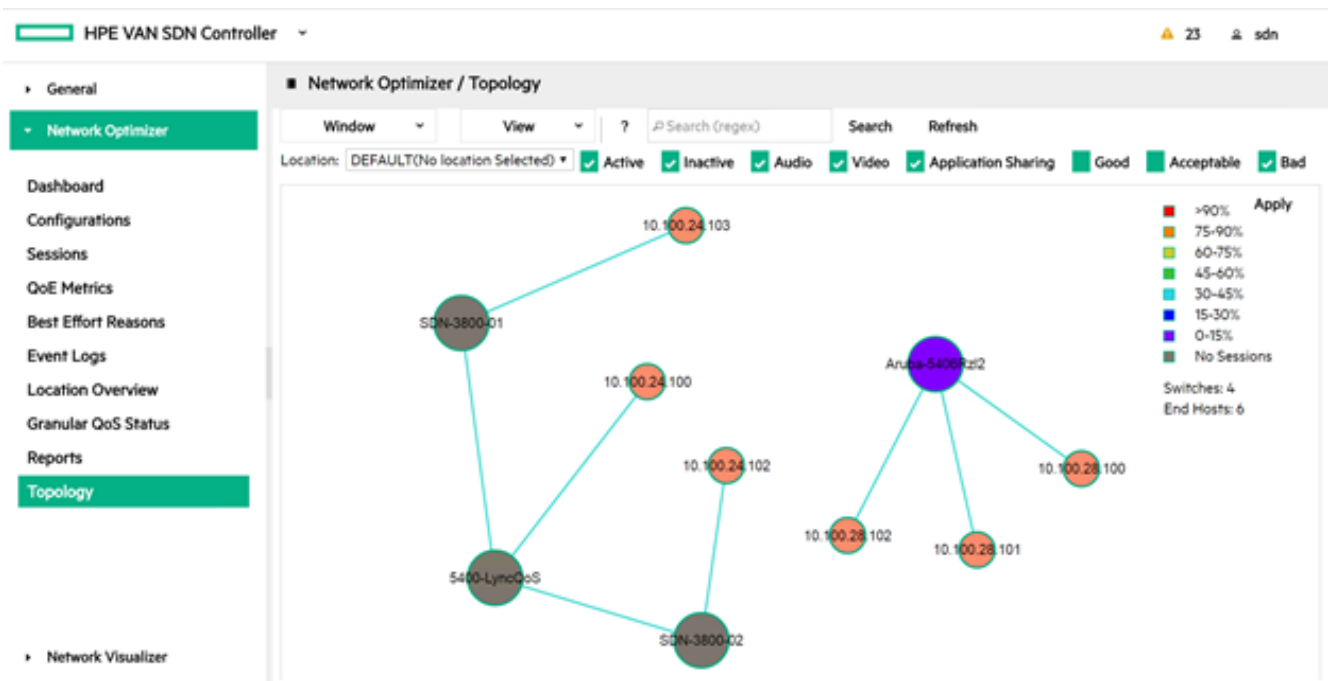
Figure 67 Session Details



Location Heat Map

The location heat map is in the Topology viewer for Network Optimizer. The Network Optimizer topology heat map provides a quick overview of where the trouble spots are in the network. This greatly increases the ability to dive in and troubleshoot where in the network issues may be occurring.

Figure 68 Location Heat Map



Top 10 Reports

New in Network Optimizer 1.4 is the built in reporting system. Particularly of interest is the ability to generate the Top 10 switches with the most number of bad calls, or calls below a specific MOS score. This provides user with the ability to quickly generate a report of the 10 switches with the poorest Skype4B performance and communicate it to the rest of the administration team.

Figure 69 *Top 10 Reports*

HPE VAN SDN Controller

General

Network Optimizer

Dashboard

Configurations

Sessions

QoE Metrics

Best Effort Reasons

Event Logs

Location Overview

Granular QoS Status

Reports

Topology

Network Optimizer / Reports

Report Categories

- Mean Opinion Score(MOS) distribution
- Top 10 switches with lowest MOS score
- Top 10 switches with highest unacceptable calls
- QoE details

Report Type

Table

Start time

End time

Average MOS

eg. 2.5 (MOS <= 2.5)

Generate Report & Download

Figure 70 *Sample Top 10 Report*

Created: Mon 30 Jan 2017 07:29:32 AM IST

Top 10 switches with lowest average MOS score

From: Sun 29 Jan 2017 07:00:00 AM IST To: Mon 30 Jan 2017 07:29:31 AM IST

IP Address	DataPathId	HW version	Serial Number	Number of lowest MOS sessions(MOS < 4.0)
192.168.200.90	00:5a:14:58:d0:9b:8b:00	2920-48G-POE+ Switch	SG49FLZ5VJ	175
192.168.200.92	00:5c:84:34:97:02:db:25	3800-24G-PoE+-2XG Switch	SG2AG0Z1K2	100
192.168.200.99	00:01:78:48:59:15:85:46	HP A5500-24G EI Switch	CN46B9V0B9	100
192.168.200.1	00:00:00:00:00:00:00:01	Open vSwitch	None	97
192.168.200.1	00:00:00:00:00:00:00:04	Open vSwitch	None	50
192.168.200.1	00:00:00:00:00:00:00:05	Open vSwitch	None	50
192.168.200.1	00:00:00:00:00:00:00:02	Open vSwitch	None	50
192.168.200.1	00:00:00:00:00:00:00:03	Open vSwitch	None	50
192.168.200.1	00:00:00:00:00:00:00:06	Open vSwitch	None	50
192.168.200.1	00:00:00:00:00:00:00:07	Open vSwitch	None	50

OpenFlow Troubleshooting

Network Optimizer adds two flows for every call as well as a flow for signaling to each Skype for Business FE server configured. See below for the flow details for a voice call between two clients and the FE server signaling.

Figure 71 *OpenFlow Troubleshooting*

Flows for Data Path ID: 00:18:88:51:fb:35:1a:40						
					Summary	Ports
▶ 100	35010	204	0	eth_type: ipv4 ipv4_src: 10.100.28.102 ipv4_dst: 10.100.24.103 ip_proto: udp udp_src: 9486 udp_dst: 21884	apply_actions: set_field: [ip_dscp: 46] set_field: [vlan_pcp: 5] output: NORMAL	
▶ 100	35010	4110	0	eth_type: ipv4 ipv4_src: 10.100.24.103 ipv4_dst: 10.100.28.102 ip_proto: udp udp_src: 21884 udp_dst: 9486	apply_actions: set_field: [ip_dscp: 46] set_field: [vlan_pcp: 5] output: NORMAL	
▶ 100	35000	3535	0	eth_type: ipv4 ipv4_dst: 10.15.155.52	apply_actions: set_field: [ip_dscp: 24] set_field: [vlan_pcp: 3] output: NORMAL	

To view a similar output on the switch, the command “show openflow <instance name> flows” can be used to view the details directly from the switch CLI. Below is an output of the switch CLI for one of the above flows.

Figure 72 *Switch CLI Output*

```
Flow 11
Match
Incoming Port : Any
Source MAC : Any
Source MAC Mask : 000000-000000
Destination MAC Mask : 000000-000000
VLAN ID : Any
Source IP Address : 10.100.28.102/32
Destination IP Address : 10.100.24.103/32
IP Protocol : UDP
IP ECN : Any
Source Port : 9486
Source Port Range : NA
Destination Port Range : NA
TCP Flags : NA
TCP Mask : NA
Ethernet Type : IP
Destination MAC : Any
VLAN Priority : Any
Destination Port : 21884
Attributes
Priority : 35010
Hard Timeout : 0 seconds
Byte Count : NA
Flow Table ID : 100
Cookie : 0x9999
Hardware Index: 18
Duration : 582 seconds
Idle Timeout : 60 seconds
Packet Count : 839
Controller ID : 1
Instructions
Apply Actions
Modify IP DSCP : 46
Modify VLAN PCP : 5
Normal
```

This appendix provides information on installing and configuring SfB over the Aruba network. It includes the following sections:

- [SfB SDN API Installation and Configuration Guidelines on page 93](#)
- [Aruba Controller SfB Heuristics Configuration on page 104](#)
- [Heuristics Enhancements with ArubaOS 6.4.x on page 106](#)
- [Aruba Instant SfB Heuristics Configuration on page 107](#)
- [Network Optimizer SDN API Configuration on page 108](#)
- [Creating QoS Policy on a Windows Client on page 109](#)
- [Managing QoS from SfB Server through Group Edit Policy on page 110](#)
- [Network Bandwidth Requirements for Different Codecs on page 110](#)

SfB SDN API Installation and Configuration Guidelines

This section includes the following topics:

- [SfB Server Side Configuration on page 93](#)
- [Configuring Aruba Controller for SDN API Interoperability on page 96](#)
- [Enhancements with ArubaOS 6.4 Onwards on page 103](#)
- [Aruba Controller Configuration for AirWave 8.x UCC Integration on page 104](#)

SfB Server Side Configuration

SfB Dialog Listener must be installed and configured on the SfB front end server. If there are multiple front end servers, SfB Dialog Listener must be installed on each front end server.

SfB SDN Manager must be installed on a separate Windows 2008/2012 server and not on the SfB front end server. SDN managers can be configured in a pool to provide load sharing and automatic failover. SfB dialog listeners need to be configured to point to the SfB SDN Manager pool. Aruba controller is considered as a subscriber to the SfB SDN manager and controller information need to be configured on the SfB SDN manager.

Get the latest SfB SDN API 2.4.1 from the [Microsoft site](#).



For more information on the SfB Dialog listener and SfB SDN manager installation instructions, refer to the SDN API 2.4.1 documentation.

Configuration

Configure the SDN manager, dialog listener, and subscriber from the SDN manager PowerShell.

We recommend installing the SDN manager before the SDN dialog listener.

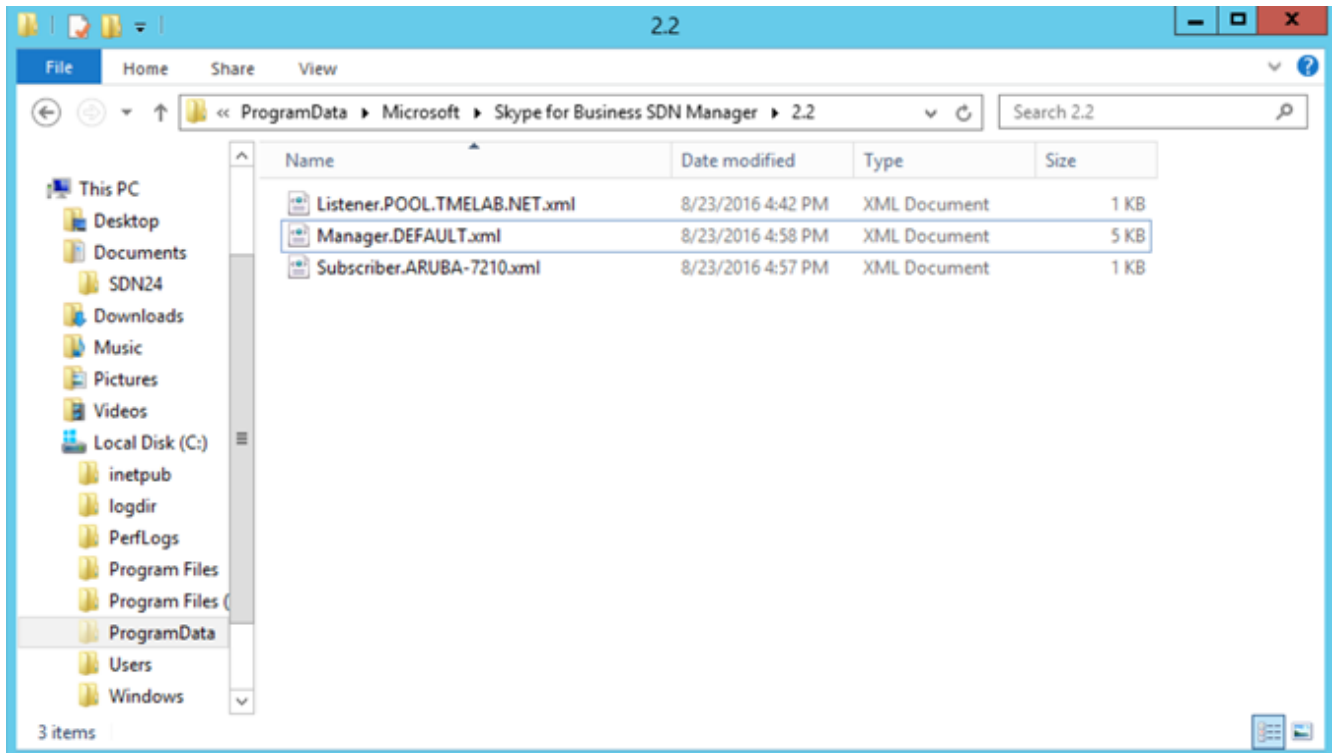
This section includes the following topics:

- [SDN Manager Configuration on page 94](#)
- [Dialog Listener Configuration on page 94](#)
- [Subscriber Configuration on page 95](#)
- [Subscriber Backward Compatibility on page 96](#)

SDN Manager Configuration

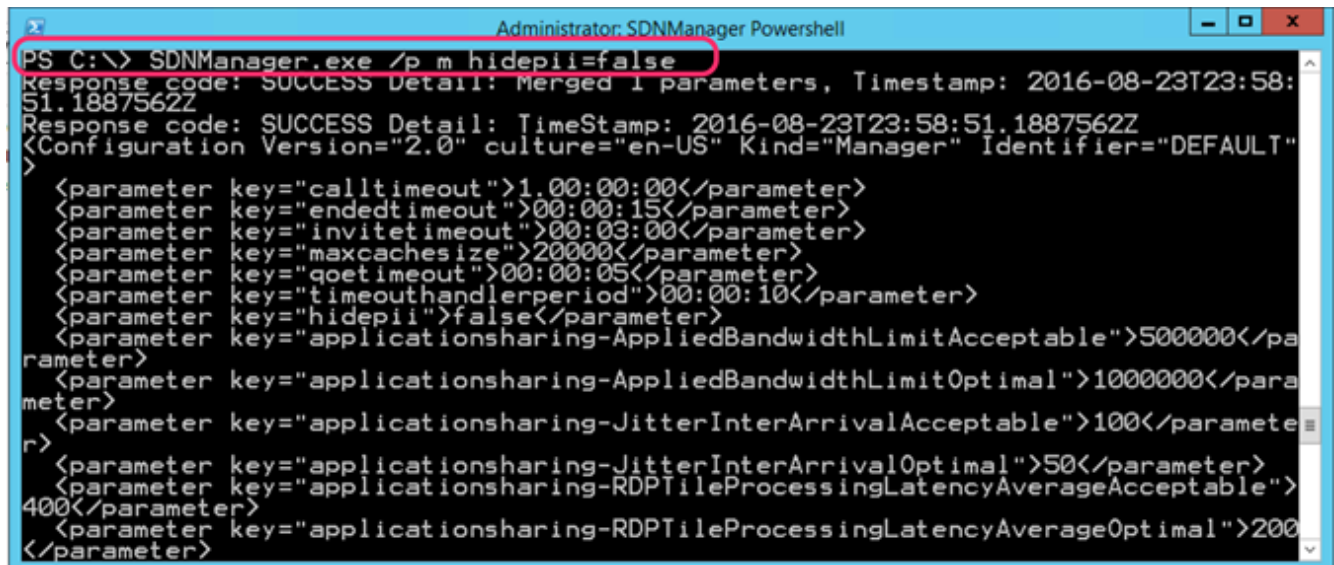
After the SDN manager installation is complete, the default configuration is saved in the following path as described in .

Figure 73 SDN Manager Configuration



By default, on SDN manager "hidepii" is set to True, which means the SfB client details will not be sent to the subscribers. The following configuration sets "hidepii" to False.

Figure 74 hidepii is False

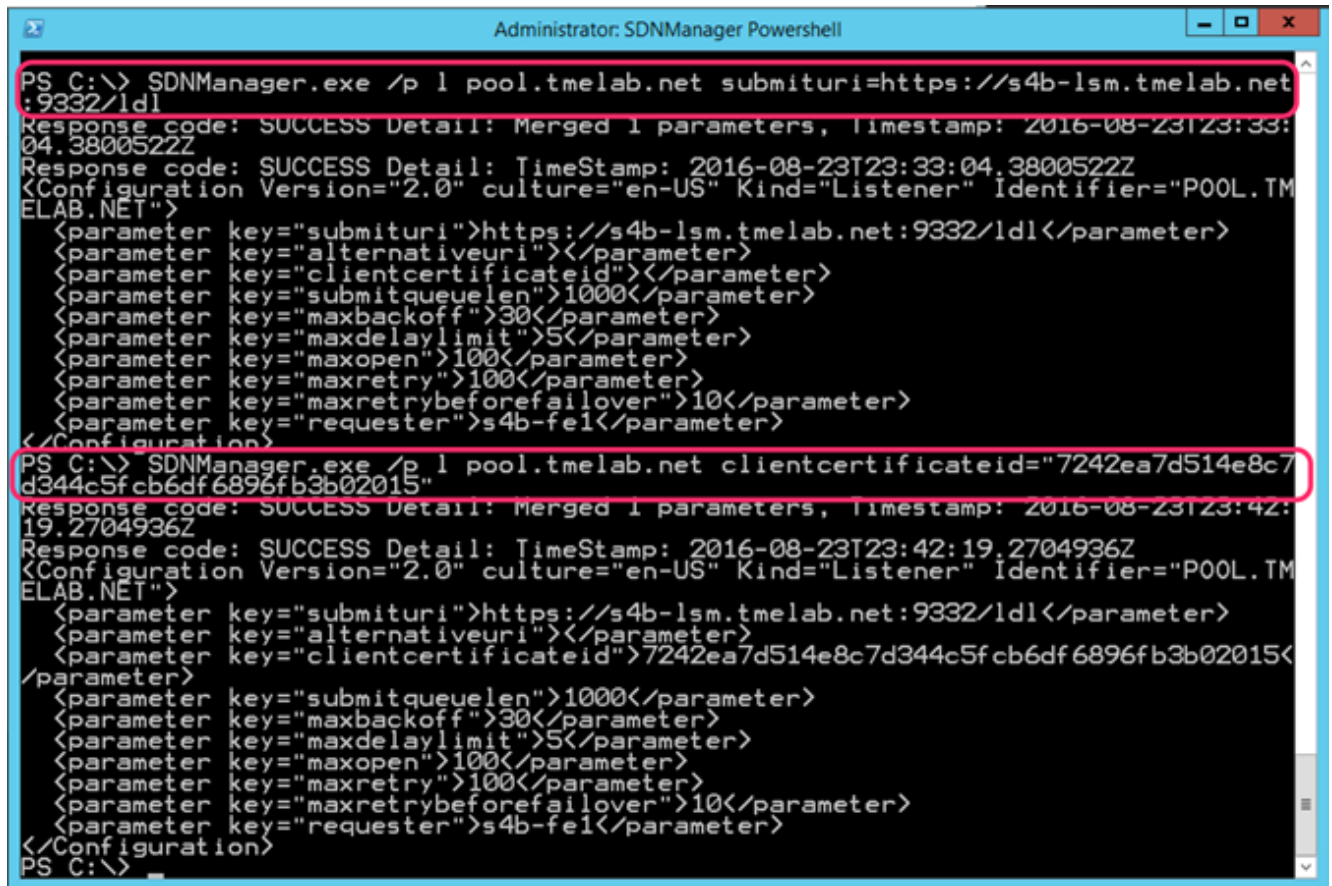


Dialog Listener Configuration

The SDN manager fully qualified domain name (FQDN) should be entered in the SubmitURL field. In this example, Dialog listener uses "https" based communication with SDN manager as shown below.

The thumbprint of Dialog listener client certificate is entered in certificateid field.

Figure 75 *Dialog Listener Configuration*



```
Administrator: SDNManager Powershell

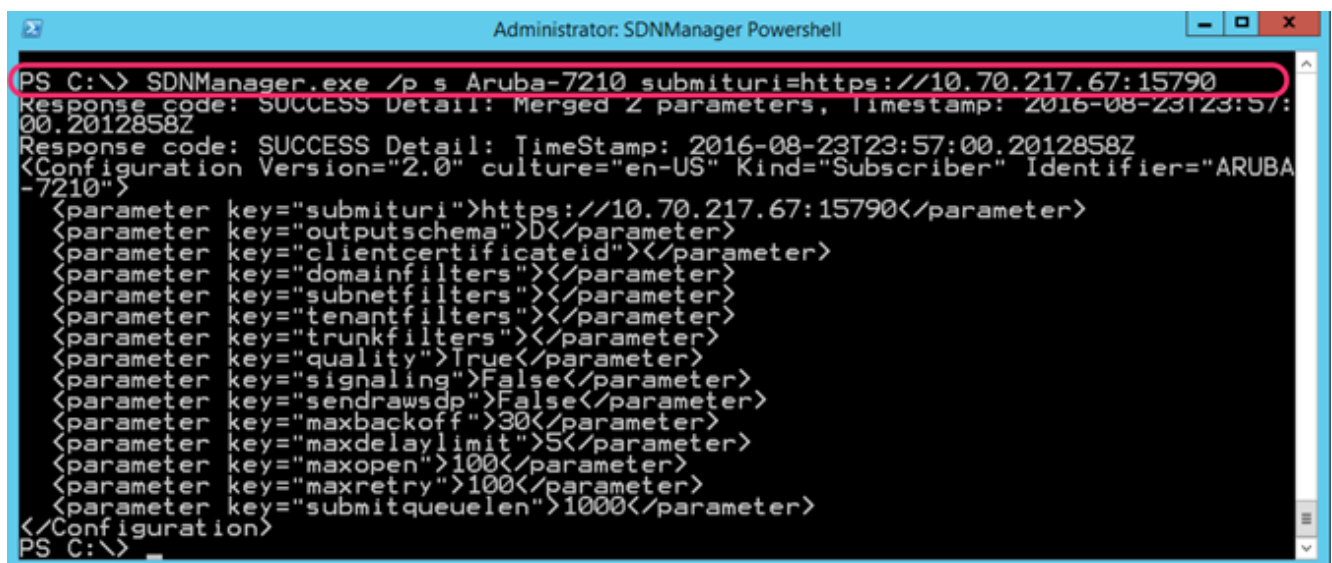
PS C:\> SDNManager.exe /p l pool.tmelab.net submituri=https://s4b-lsm.tmelab.net:9332/ldl
Response code: SUCCESS Detail: Merged 1 parameters, Timestamp: 2016-08-23T23:33:04.3800522Z
Response code: SUCCESS Detail: TimeStamp: 2016-08-23T23:33:04.3800522Z
<Configuration Version="2.0" culture="en-US" Kind="Listener" Identifier="P00L.TMELAB.NET">
  <parameter key="submituri">https://s4b-lsm.tmelab.net:9332/ldl</parameter>
  <parameter key="alternativeuri"></parameter>
  <parameter key="clientcertificateid"></parameter>
  <parameter key="submitqueuelen">1000</parameter>
  <parameter key="maxbackoff">30</parameter>
  <parameter key="maxdelaylimit">5</parameter>
  <parameter key="maxopen">100</parameter>
  <parameter key="maxretry">100</parameter>
  <parameter key="maxretrybeforefailover">10</parameter>
  <parameter key="requester">s4b-fe1</parameter>
</Configuration>

PS C:\> SDNManager.exe /p l pool.tmelab.net clientcertificateid="7242ea7d514e8c7d344c5fcb6df6896fb3b02015"
Response code: SUCCESS Detail: Merged 1 parameters, Timestamp: 2016-08-23T23:42:19.2704936Z
Response code: SUCCESS Detail: TimeStamp: 2016-08-23T23:42:19.2704936Z
<Configuration Version="2.0" culture="en-US" Kind="Listener" Identifier="P00L.TMELAB.NET">
  <parameter key="submituri">https://s4b-lsm.tmelab.net:9332/ldl</parameter>
  <parameter key="alternativeuri"></parameter>
  <parameter key="clientcertificateid">7242ea7d514e8c7d344c5fcb6df6896fb3b02015</parameter>
  <parameter key="submitqueuelen">1000</parameter>
  <parameter key="maxbackoff">30</parameter>
  <parameter key="maxdelaylimit">5</parameter>
  <parameter key="maxopen">100</parameter>
  <parameter key="maxretry">100</parameter>
  <parameter key="maxretrybeforefailover">10</parameter>
  <parameter key="requester">s4b-fe1</parameter>
</Configuration>
PS C:\>
```

Subscriber Configuration

Aruba controller IP address and SDN port number is configured in subscriber field. In this configuration, SDN manager uses “https” based configuration to communicate with the subscriber.

Figure 76 *Subscriber Configuration*



```
Administrator: SDNManager Powershell

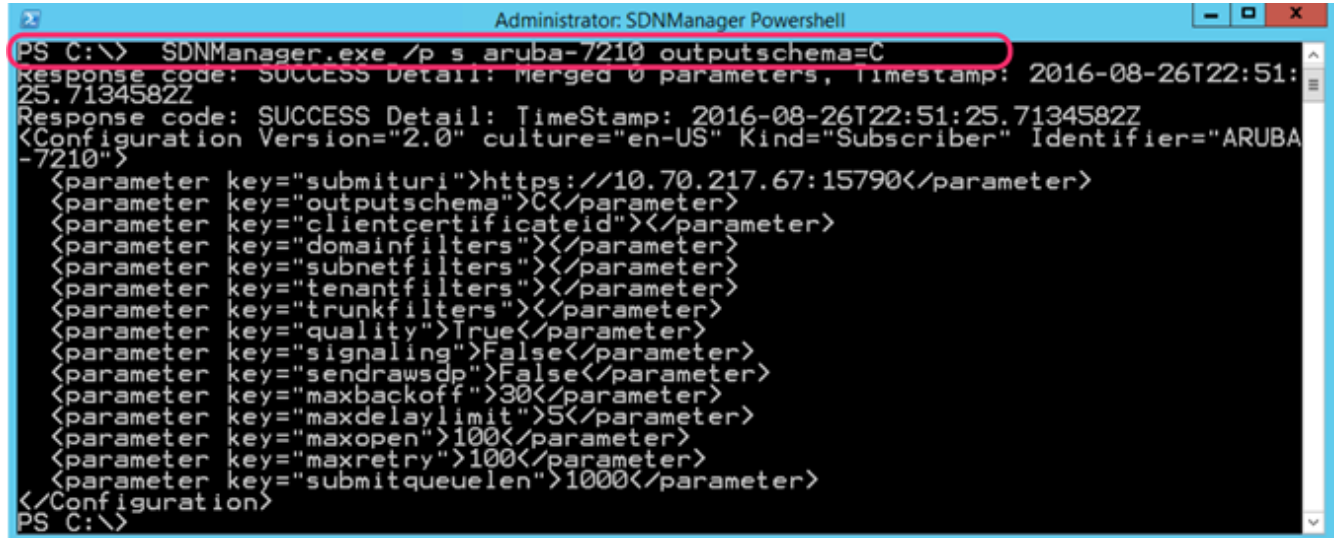
PS C:\> SDNManager.exe /p s Aruba-7210 submituri=https://10.70.217.67:15790
Response code: SUCCESS Detail: Merged 2 parameters, Timestamp: 2016-08-23T23:57:00.2012858Z
Response code: SUCCESS Detail: TimeStamp: 2016-08-23T23:57:00.2012858Z
<Configuration Version="2.0" culture="en-US" Kind="Subscriber" Identifier="ARUBA-7210">
  <parameter key="submituri">https://10.70.217.67:15790</parameter>
  <parameter key="outputschema">D</parameter>
  <parameter key="clientcertificateid"></parameter>
  <parameter key="domainfilters"></parameter>
  <parameter key="subnetfilters"></parameter>
  <parameter key="tenantfilters"></parameter>
  <parameter key="trunkfilters"></parameter>
  <parameter key="quality">True</parameter>
  <parameter key="signaling">False</parameter>
  <parameter key="sendrawsdp">False</parameter>
  <parameter key="maxbackoff">30</parameter>
  <parameter key="maxdelaylimit">5</parameter>
  <parameter key="maxopen">100</parameter>
  <parameter key="maxretry">100</parameter>
  <parameter key="submitqueuelen">1000</parameter>
</Configuration>
PS C:\>
```

Subscriber Backward Compatibility

ArubaOS v6.4.3 is not compatible with new SDN XML Schema-D. Schema-C provides backward compatibility to ArubaOS v6.4.3.

Configure Schema-C as shown in [Figure 77](#).

Figure 77 Schema-C



```
Administrator: SDNManager Powershell
PS C:\> SDNManager.exe /p s aruba-7210 outputschema=C
Response code: SUCCESS Detail: Merged 0 parameters, Timestamp: 2016-08-26T22:51:25.7134582Z
Response code: SUCCESS Detail: TimeStamp: 2016-08-26T22:51:25.7134582Z
<Configuration Version="2.0" culture="en-US" Kind="Subscriber" Identifier="ARUBA-7210">
  <parameter key="submituri">https://10.70.217.67:15790</parameter>
  <parameter key="outputschema">C</parameter>
  <parameter key="clientcertificateid"></parameter>
  <parameter key="domainfilters"></parameter>
  <parameter key="subnetfilters"></parameter>
  <parameter key="tenantfilters"></parameter>
  <parameter key="trunkfilters"></parameter>
  <parameter key="quality">True</parameter>
  <parameter key="signaling">False</parameter>
  <parameter key="sendrawsdp">False</parameter>
  <parameter key="maxbackoff">30</parameter>
  <parameter key="maxdelaylimit">5</parameter>
  <parameter key="maxopen">100</parameter>
  <parameter key="maxretry">100</parameter>
  <parameter key="submitqueuelen">1000</parameter>
</Configuration>
PS C:\>
```

Configuring Aruba Controller for SDN API Interoperability

The following instructions only highlight the SDN API specific SfB ALG configurations. Heuristics based SfB classification does not require integration with Microsoft. It can provide QoS to SfB voice/video traffic, but does not provide insight into Microsoft SfB End-to-End call quality. For more information on the Media Classification heuristics technique, visit <http://support.arubanetworks.com> and refer to ArubaOS 6.1 or later versions of the user guide.

Controller Configuration for SDN API Communication

Aruba controllers can be configured to listen for HTTP (XML) and HTTPS (XML) messages from SfB server SDN API. You can configure the controller through:

- WebUI
- CLI Configuration

This section includes the following topics:

- [Configuring Aruba Controllers to Listen for HTTP \(XML\) Messages on page 96](#)
- [Configuring Aruba Controllers to Listen for HTTPS \(XML\) Messages on page 97](#)
- [Uploading a Certificate to the Server on page 99](#)
- [Uploading a Root Server Certificate on page 99](#)
- [Configuring Aruba Controller to read SIP Signaling Message sent by SfB Clients on Port 5061 on page 100](#)
- [Configuring SfB Signaling Traffic on Aruba Controller on page 101](#)
- [Configuration Specific to ArubaOS 6.3 on page 102](#)

Configuring Aruba Controllers to Listen for HTTP (XML) Messages

To configure a Aruba controller using the WebUI navigate to **Management > General** and configure **SfB Listening Port**.

Figure 78 Configure SfB Listening Port

MANAGEMENT

- > General
 - Administration
 - Certificates
 - SNMP
 - Logging
 - Clock
 - Guest Provisioning
 - Captive Portal
 - SMTP
 - Bandwidth Calculator
 - Threshold
- ADVANCED SERVICES
 - Redundancy
 - AirGroup
 - IP Mobility
 - Stateful Firewall
 - External Services
 - VPN Services
 - Wired Access
 - All Profiles

[E-mail Support](#)

Server Certificate Default

IDP Server Certificate

Server Certificate Default

Configure Cipher LOW/MEDIUM/HIGH

Web Server Ciphers High

LCD Menu

Menu	<input checked="" type="radio"/> enable	<input type="radio"/> disable
Maintenance	<input checked="" type="radio"/> enable	<input type="radio"/> disable
Halt-system	<input checked="" type="radio"/> enable	<input type="radio"/> disable
Reload-system	<input checked="" type="radio"/> enable	<input type="radio"/> disable
Media-eject	<input checked="" type="radio"/> enable	<input type="radio"/> disable
Factory-default	<input checked="" type="radio"/> enable	<input type="radio"/> disable
Upload-config	<input checked="" type="radio"/> enable	<input type="radio"/> disable
Upgrade-image	<input checked="" type="radio"/> enable	<input type="radio"/> disable
Partition1	<input checked="" type="radio"/> enable	<input type="radio"/> disable
Partition0	<input checked="" type="radio"/> enable	<input type="radio"/> disable

Configure Lync

Web lync listening port HTTP 15790

Execute the following command to configure the port number on which SDN API will send HTTP (XML) messages to the controller.

```
#configure terminal
(config) #web-server
(Web Server Configuration) #web-SfB-listen-port http 15790
```

In the above example, Aruba controller uses 15790 listening port for HTTP (XML) messages.

Configuring Aruba Controllers to Listen for HTTPS (XML) Messages

A server certificate must be generated and installed on the controller before configuring it to receive SfB SDN API messages using HTTPS.

The server certificate must contain the FQDN of the controller, must be signed by a CA, and the root certificate must be installed on both the controller and the SDN manager.

Follow the steps below to generate a server certificate and configure the controller Web server to use HTTPS:

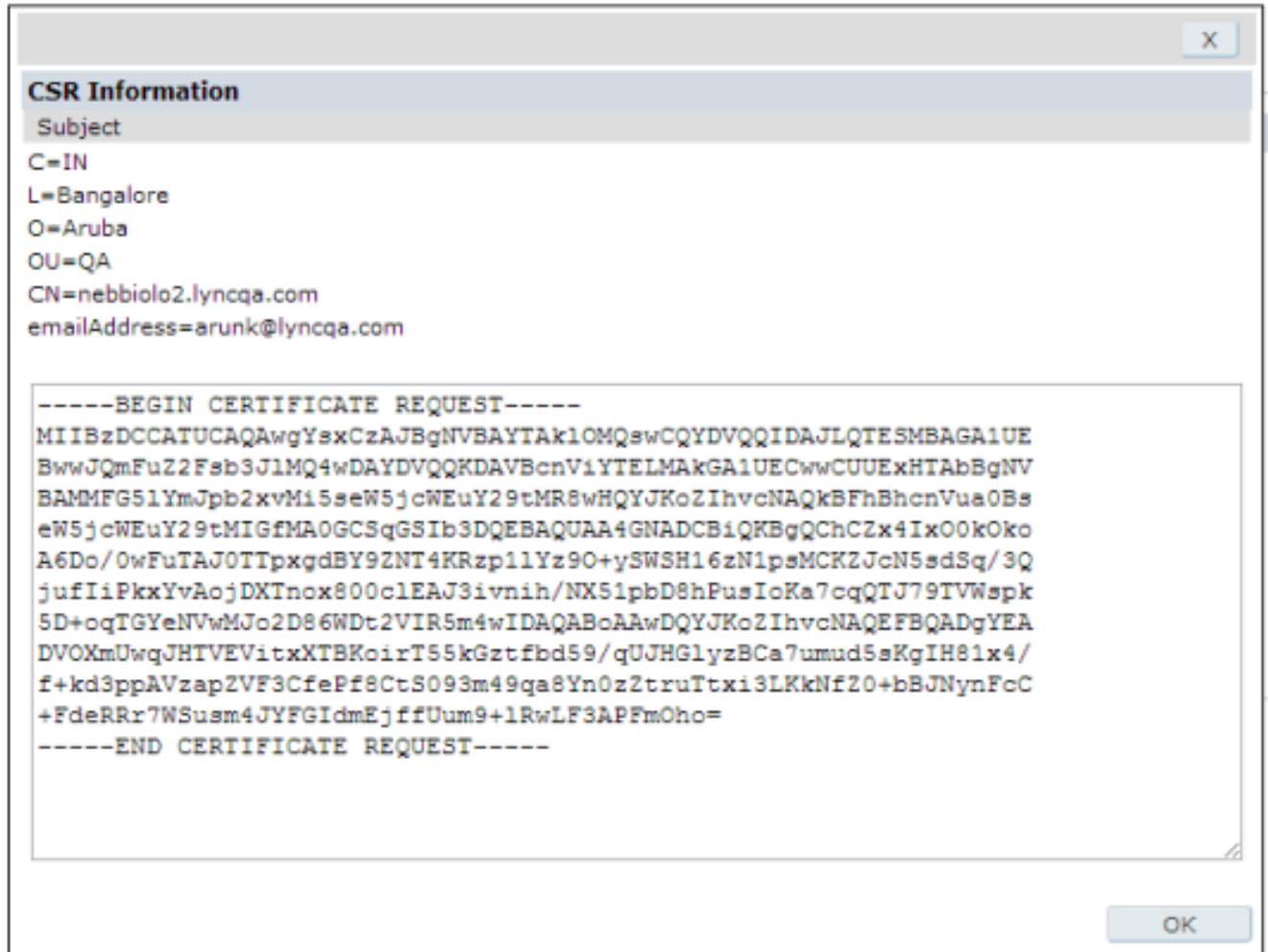
1. Navigate to **Configuration > Management > Certificates** in the controller Web UI and click the **CSR** tab.
2. Fill in the signing request information and click **Generate New**.



Ensure that the Common Name (CN) for the CSR corresponds to the FQDN of the controller, and the LSM is able to resolve the IP of the FQDN.

3. Click the **View Current** button to view the signing request after the CSR is generated.

Figure 79 *Signing Request*



4. Copy the certificate request and generate a server certificate from the certificate authority.
5. Navigate to the certification server.
6. Click the **Request a certificate** link.
7. Click the **Advanced certificate request** link.
8. Click the **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file** link.
9. Paste the certificate request obtained from the controller in the **Saved Request** box.
10. Choose the **Web server** option from the **Certificate Template** drop-down menu.
11. Click the **Submit** button.

Figure 80 *Submit Certificate Request*

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	<pre>-----BEGIN CERTIFICATE REQUEST----- MIIBzDCCATUCAwQYsxCzAJBgNVBAYTAk1OMQsw BwwJQmFuZ2Fsb3JlMQ4wDAYDVQQKDAVBcnViYTEL BAMMFg51YmJpb2xvMi5seW5jcWEuY29tMR8wHQYJ eW5jcWEuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GN A6Do/OwFuTAJ0TTpxgdBY9ZNT4KRzp1lYz90+ySW</pre>
---	---

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

Uploading a Certificate to the Server

1. Download and save the server certificate.
2. Download the root certificate for the CA.
3. Navigate to **Configuration > Management > Certificates** and click the **Upload** tab.
4. Enter the **Certificate Name** and select **Certificate Filename** using the **Choose File** button.
5. Click **Upload**.

Figure 81 *Upload Certificate*

Management > Certificates > Upload

Upload	CSR	Revocation CheckPoint
Upload a Certificate		
Certificate Name	nebbiolo2.lyncqa.com	
Certificate Filename	Choose File nebbiolo2-lyncqa-com.cer	
Passphrase (optional)		For import purpose only,
Retype Passphrase		
Certificate Format	DER	
Certificate Type	Server Cert	
Upload Reset		

Uploading a Root Server Certificate

Follow the steps in [Uploading a Certificate to the Server on page 99](#) to upload the root certificate to the controller, and select **Trusted CA** from the **Certificate Type** drop-down list box.

1. Navigate to **Configuration > Management > General** and select **WebUI Management Authentication Method** to view the server certificate that was uploaded in [Uploading a Certificate to the Server on page 99](#).
2. Install the root certificate for the CA on the SfB server manager.

Figure 82 Root Server Certificate

Management > Certificates > Upload

Upload | CSR | Revocation CheckPoint

Upload a Certificate

Certificate Name:

Certificate Filename:

Passphrase (optional): For import purpose only,

Retype Passphrase:

Certificate Format:

Certificate Type:

3. To configure an Aruba controller using the Web UI go to **Management > General** and configure **SfB Listening Port**.

Figure 83 SfB Listening Port

WebUI Management Authentication Method

Username and Password: ☒

Client Certificate: ☐

Server Certificate:

WebUI Idle Logout Timer

User session timeout: (seconds)

Captive Portal Certificate

Server Certificate:

IDP Server Certificate

Server Certificate:

Configure Cipher LOW/MEDIUM/HIGH

Web Server Ciphers:

Configure Lync

Web lync listening port:

In the above example, the Aruba controller is listening on port 15790 for HTTPS (XML) messages. On the SDN manager configuration, configure the web service URL as the FQDN of the controller. In this example, it is **nebbiolo2.SfBqa.com**. Ensure a record is added for the controller host name in the DNS server.

To configure an Aruba controller using a CLI execute the following command to configure the port number on which SDN API will be sending HTTPS (XML) messages to Aruba controller.

```
#configure terminal
(config) #web-server
(Web Server Configuration) #web-SfB-listen-port https 15790
```

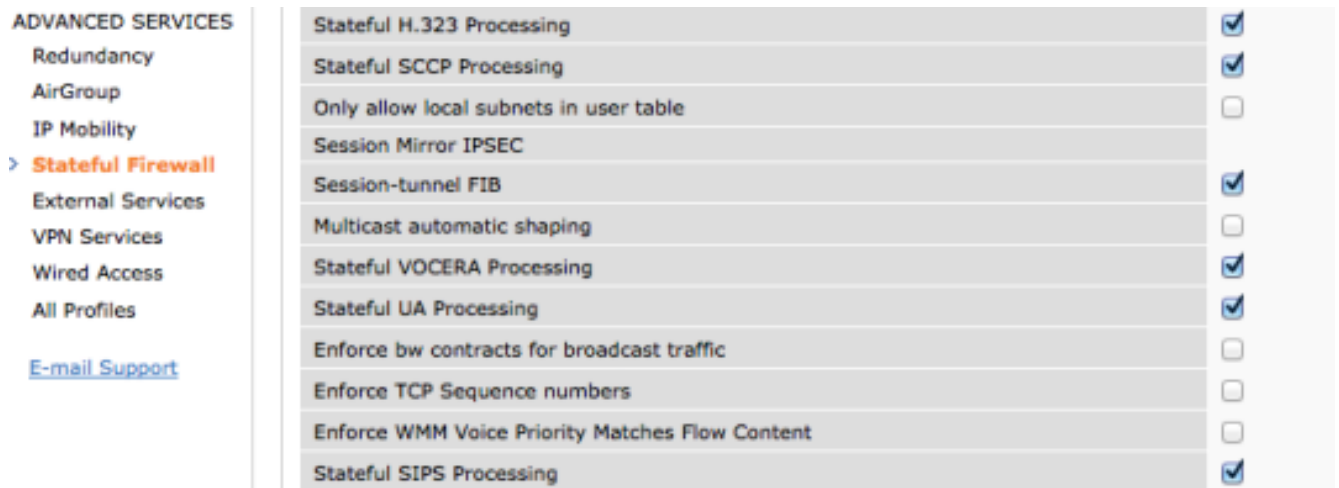
Configuring Aruba Controller to read SIP Signaling Message sent by SfB Clients on Port 5061

Stateful SIPs processing is enabled by default in ArubaOS 6.3.1. If Stateful SIPs is disabled, you can enable the same using the Web UI and CLI.

To enable Stateful SIPs processing using the Web UI:

1. Go to the **Configuration** page.
2. Under **Advanced Services** select **Global Settings**.
3. Select the **Stateful SIPS Processing** check box.
4. Click **Apply**.

Figure 84 *Stateful SIPS Processing*



Execute the following, to enable Stateful SIPS processing using the CLI:

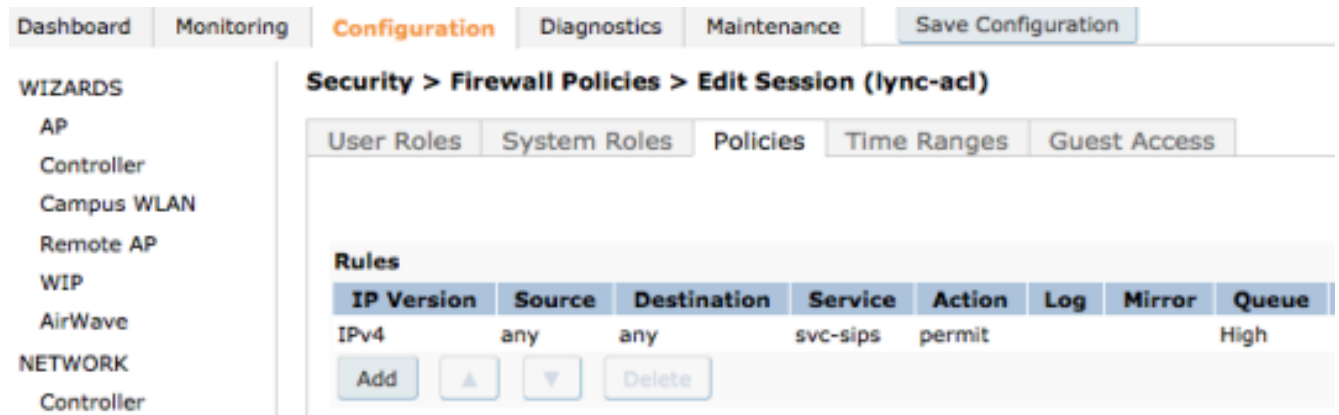
```
#configure terminal
(config) #no firewall disable-stateful-sips-processing
```

Configuring SfB Signaling Traffic on Aruba Controller

Ensure that SfB signaling traffic is permitted (TCP Port 5061) in SfB ACL. This ACL should be mapped to the user role to allow SfB signaling traffic. To view SfB ACL in the WebUI:

1. Click on the **Configuration** tab.
2. Select **Security > Firewall Policies**.

Figure 85 *Firewall Policies*



The following example indicates SfB ACL assigned to a test user role.

```
netservice svc-sips tcp 5061 alg sips !
ip access-list session SfB-acl
any any svc-sips permit queue high !
```

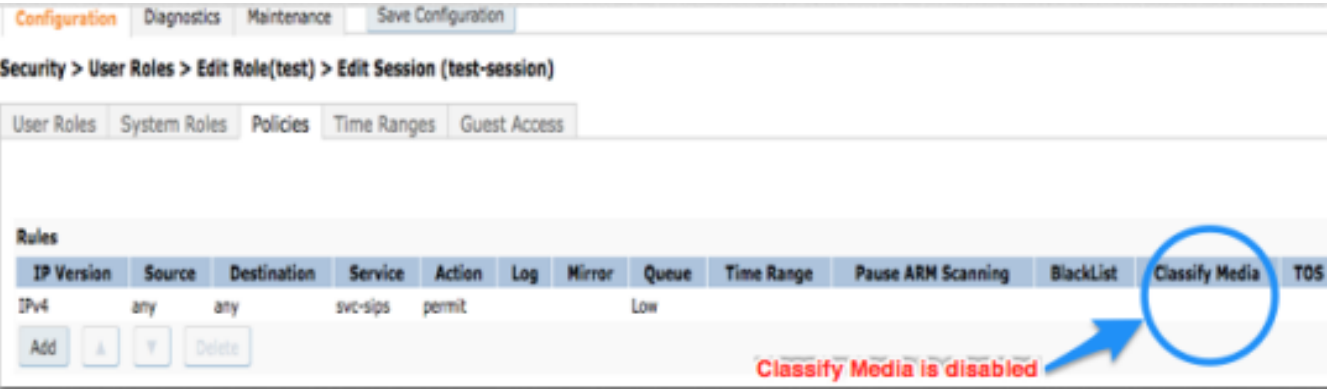
```
user-role test access-list session SfB-acl
```

Configuration Specific to ArubaOS 6.3

Removing media-classification CLI from Aruba Controller: Heuristics based detection of SfB traffic is not compatible with the API detection method and must be turned off. The **Classify Media** option must not be enabled in the svc-sips ACL that is applied to the user role.

The following figure helps you determine if **Classify Media** is configured in an **ip access-list session** that is associated to an user-role.

Figure 86 Classify Media



Executing the following CLI command helps in determining if **Classify Media** is configured in an **ip access-list session** that is associated to a test user-role.

Figure 87 CLI Classify Media

```
#show rights test
Derived Role = 'test'
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      Type      Location
-----  -
1         test  session
test
-----
Priority  Source  Destination  Service      Action  TimeRange  Log  Expired  Queue
TOS  8021P  Blacklist  Mirror  DisScan  ClassifyMedia  IPv4/6
-----  -
1         any    any          svc-sips     permit                                     Low
Yes 4
(→ Yes indicates that 'classify-
media' is configured)
Expired Policies (due to time constraints) = 0
```

Execute the following command to remove **Classify Media**, if it is configured in the **ip access-list session**.

```
#configure terminal
config) #ip access-list session test1
config-sess-test1)#no any any svc-sips permit
config-sess-test1)# any any svc-sips permit queue high
config-sess-test1)#
```

Enhancements with ArubaOS 6.4 Onwards

Following are some important points in ArubaOS 6.4:

- **Simultaneous enablement of SDN API and SfB heuristics** - In ArubaOS 6.4, both SfB SDN API and heuristics based classification/prioritization can be enabled simultaneously. If both these methods are enabled, SDN API based SfB classification is prioritized.
- **Dynamic opening of ports for SfB voice/video traffic** - If you are running an operating system prior to ArubaOS 6.4, UDP ports should be explicitly configured to allow SfB voice/video traffic. Execute the following command to configure UDP ports.

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

In ArubaOS 6.4, firewall sessions dynamically open up in datapath for SfB voice and video calls. For this session to open up, UDP port 3478 should be permitted in SfB ACL to allow Simple Traversal of UDP Through NAT (STUN) messages. SfB clients initiate a STUN connectivity check prior to media transmission. Once the STUN connectivity check is successful, media is transmitted.

Dynamic opening of ports is not available for SfB desktop sharing and file transfer calls. An administrator should open the TCP ports used by these applications.

In ArubaOS 6.4, a new feature is introduced to dynamically open the high range UDP ports for voice and video. The operation of this feature varies for heuristics classification and SDN API.

When using heuristics or SDN API, UDP port 3478 should be permitted in the SfB ACL to allow STUN messages. SfB clients initiate STUN connectivity check prior to media transmission. Once the STUN connectivity check is successful and the traffic is confirmed as SfB media, those ports are opened for the duration of the session. Dynamic opening of ports is not done for SfB desktop sharing and file transfer. As a result an ACL that permits those features must be defined. By default SfB selects a port from the full dynamic TCP range for file transfer and desktop sharing. For more information on the ports required, refer to <http://technet.microsoft.com/en-us/library/gg398833.aspx>.



Dynamic opening of ports is only triggered when there is a deny rule in place for the UDP port SfB is attempting to use.

Aruba Controller Configuration for AirWave 8.x UCC Integration

Aruba controllers running ArubaOS 6.4 or later can send UCC data to AirWave. AirWave can display the UCC Dashboard, End-to-End, WLAN call quality metrics, and device endpoint speaker and microphone glitch rate information. AirWave Management Platform (AMP) server information needs to be configured on the controller to enable the controller to send UCC data to AirWave.

Aruba Controller SfB Heuristics Configuration

Configuring Aruba controller SfB heuristics involves:

- [Configuring the Aruba Mobility Controller to Detect SfB Traffic on page 104](#)
- [Configuring the Aruba Mobility Controller to Detect SfB Online Traffic on page 105](#)
- [Verifying Operation of Heuristics Detection of SfB Traffic on page 106](#)
- [Default DSCP-WMM Mapping for Heuristics on page 106](#)

Configuring the Aruba Mobility Controller to Detect SfB Traffic

The Mobility controller can detect SfB traffic through packet inspection using an ACL configured in a user role. Using the classify media option in the ACL enables you to inspect the SfB traffic.

The classify media option tells the controller to monitor the call control ports and then sample UDP traffic to detect a SfB call. To ensure optimal performance only a few packets are sampled. Once a call is detected, the Mobility controller prioritizes the stream on the AP.

Following are some recommendations while configuring the controller.

- Set up a netdestination alias for SfB FE servers by executing the following command:

```
netdestination SfB-servers
host 192.168.10.10
```


host 192.168.20.10 !

- Create an ACL to monitor the SfB call setup traffic. Laptop clients will communicate on 5061 and mobile on 443.



Ensure that the SfB clients can communicate with other SfB clients using standard RTP ports (UDP 1024 -65,535) or to the RTP ports as configured on the SfB server. For more information, see <http://technet.microsoft.com/en-us/library/jj204760.aspx>.

Execute the following command:

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

- Apply the ACL to the user role used for SfB traffic by executing the following command:

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



Administrators must configure an ACL to allow TCP based non-RTP SfB traffic such as desktop sharing and file transfer. This traffic is not prioritized by heuristics, but ACL ensures that the traffic is not blocked.

Configuring the Aruba Mobility Controller to Detect SfB Online Traffic

Clients that connect to Microsoft Office 365 for SfB use Port 443 to send call control to the SfB servers. As only a small number of packets are inspected, applying the ACL has minimal impact on the controller even though all https sessions are inspected. Listed below are a few recommendations to be followed while configuring a controller.

- Create an ACL to monitor the SfB call setup by executing the following command:

```
ip access-list session SfB-365-control
any any tcp 443 permit classify-media
!
ip access-list session SfB-rtp
any any udp 1024 65535 permit
!
```

- Apply the ACL to the user role used for SfB traffic by executing the following command:

```
user-role SfB-user
access-list session SfB-365-control
access-list session SfB-rtp
```

Verifying Operation of Heuristics Detection of SfB Traffic

Once heuristics detection is configured on the Mobility controller and users are assigned with roles the SfB detection ACL, the Mobility controller begins to identify and prioritize the SfB traffic.



Additional commands to monitor SfB traffic via the SDN API were introduced from ArubaOS 6.3. When using heuristics these commands do not display SfB call or client information.

To verify the operation of the heuristics detection, start a SfB 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-SfB-Client>
```

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

For heuristics, **UCC Dashboard** shows **WLAN Call metrics** and **QoS correction** details. It does not have End-to-end call metrics details.

Default DSCP-WMM Mapping for Heuristics

If no DSCP-WMM mapping is configured on the controller, SfB voice/video traffic is marked with default DSCP tags.

Table 12: *Default DSCP Tag for SfB Heuristics*

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

Heuristics Enhancements with ArubaOS 6.4.x

The following features are introduced in ArubaOS 6.4:

- [Enable SDN API and SfB Heuristics Simultaneously on page 106](#)
- [Dynamic Opening of Ports for SfB Voice/Video Traffic on page 106](#)
- [Classification of SfB Voice and Video Traffic on page 107](#)

Enable SDN API and SfB Heuristics Simultaneously

In ArubaOS 6.4.0, both SfB SDN API and heuristics based classification/prioritization can be enabled simultaneously. If both methods are enabled SDN API based SfB classification will take priority.

Dynamic Opening of Ports for SfB Voice/Video Traffic

If you are running an operating system prior to ArubaOS 6.4.0, UDP ports should be explicitly configured to allow SfB voice/video traffic using the following command:

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

In ArubaOS 6.4, firewall sessions dynamically open up in datapath for SfB voice and video calls. For this session to open up, UDP port 3478 should be permitted in SfB ACL to allow STUN messages. SfB clients initiate a STUN

connectivity check prior to media transmission. Once the STUN connectivity check is successful, media is transmitted.

Dynamic opening of ports is not available for SfB desktop sharing and file transfer calls. An administrator should open the TCP ports used by these applications.

Classification of SfB Voice and Video Traffic

Skype for Business changed the way the media packets are transmitted. Prior to SfB, the media classification algorithm worked on the basis that the RTP and RTP Control Protocol (RTCP) streams are transmitted over separate sessions. SfB multiplexed RTCP and RTP packets over the same session and this broke the previous heuristics method.

SfB behavior is addressed with ArubaOS v6.4.4. No additional heuristics based configuration is needed to classify SfB calls.

Aruba Instant SfB Heuristics Configuration

Configuring the following access policies ensures that the SfB traffic is automatically detected and voice packets are marked with DSCP value of 56 and video packets are marked with DSCP of 40. It is recommended that the wired network honors the DSCP values configured in the wireless network to have End-to-end QoS.

- **SfB on premise based deployment** - For SfB server based deployments, configure the following access rule under WLAN setup in addition to any other ACLs that you may have and move it to the top of the list.

Figure 88 *SfB on Premise Based Deployment*

Rule type: Access control Action: Allow Service: sips Destination: to all destinations

Options: ☐ Log ☒ Classify media ☐ DSCP tag
☐ Blacklist ☒ Disable scanning ☐ 802.1p priority

OK Cancel

- **SfB online based deployment** - For SfB online (cloud) based deployments, configure the following access rule under WLAN setup in addition to any other ACLs that you may have and move it to the top of the list.

Figure 89 *SfB Online Based Deployment*

Rule type: Access control Action: Allow Service: https Destination: to all destinations

Options: ☐ Log ☒ Classify media ☐ DSCP tag
☐ Blacklist ☒ Disable scanning ☐ 802.1p priority

OK Cancel



Starting from Instant AP 6.4.0.2-4.1, IAP supports customization of Wi-Fi multimedia to DSCP mapping configuration for upstream (client to IAP) and downstream (IAP to client) traffic. Refer to Aruba Instant 6.4.0.2-4.1 CLI Reference Guide for additional details on DSCP-WMM configuration.

Network Optimizer SDN API Configuration

Submit URL for Network Optimizer is:

<https://sdn-controller-ip:8443/sdn/lynccqos/v1.0/session>

ArubaOS-Switch Configuration

All OpenFlow capable ArubaOS-Switch devices are capable of supporting Network Optimizer as well as several legacy HPE switches. To enable Network Optimizer on an ArubaOS-Switch device, the following OpenFlow commands are used to configure the switch to communicate to the controller. The management vlan (MGMT VLAN) used for OpenFlow connectivity to the VAN SDN Controller must have a routable or switch path to the controller that egresses the switch out of the management vlan.

Below is an example OpenFlow configuration for a 2920, for a tailored OpenFlow configuration see the Aruba Solution Exchange AOS-Switch: OpenFlow Configuration solution. <https://ase.arubanetworks.com/solutions/id/136>

openflow

controller-id 1 ip <controllerIP> controller-interface vlan <MGMT VLAN>

instance "<friendly name>"

member vlan <VLANS with Client Traffic, not MGMT VLAN>

controller-id 1

version 1.3 only

limit software-rate 700

connection-interruption-mode fail-standalone

enable

exit

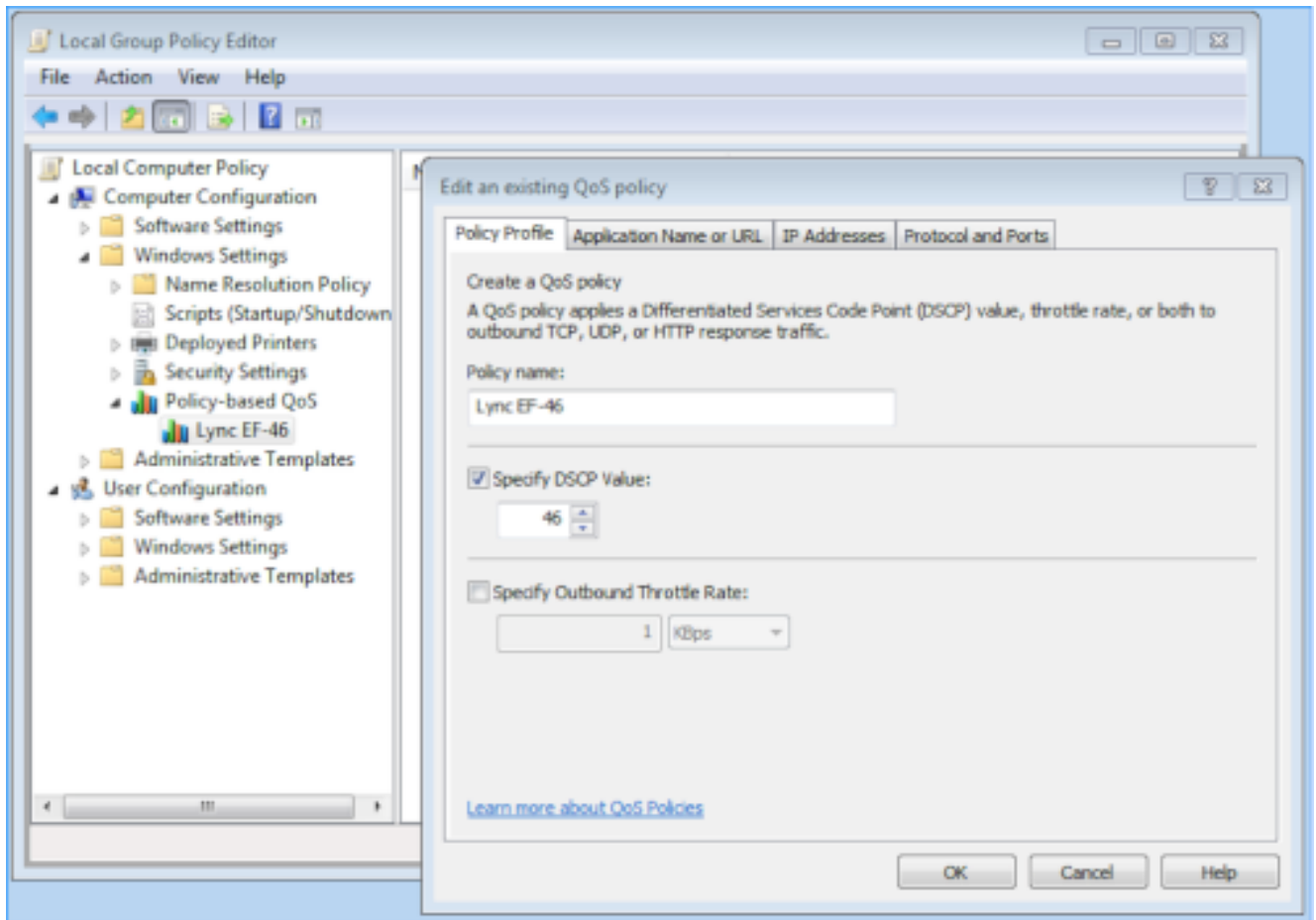
enable

exit

Creating QoS Policy on a Windows Client

The following policies apply to Windows Vista, Windows 7, and Windows 8 clients.

Figure 90 QoS Policy



To create an upstream QoS policy on Windows you must know the port ranges used for voice and video. The port ranges must be manually set on the SfB server to a specific range.

1. To create a QoS policy go to **gpedit.msc > Local Computer Policy > Computer Configuration > Windows Settings > Policy-based QoS**.

Create QoS policies by specifying the name of the executable application and the source/destination ports to which to apply QoS.

2. Make changes in the registry settings to avoid the limitation for Win7 to be domain-joined: [HKEY_LOCAL_MACHINE]
"Do not use NLA"="1" i.e., create a REG_SZ value binary value with name "Do not use NLA" and value "1"
3. Restart your computer.
4. Run the application and verify DSCP markings using the UCC dashboard or a packet capture tool.

Managing QoS from SfB Server through Group Edit Policy



For more information on managing QoS from SfB server through group edit policy see, <http://technet.microsoft.com/en-us/library/gg405409.aspx>.

Network Bandwidth Requirements for Different Codecs



For more information on network bandwidth requirements for different codecs see, <http://technet.microsoft.com/en-us/library/jj688118.aspx>.
