Voice Support on Aruba Controllers and Remote Access Points for Fixed Telecommuter Deployments

Version 1.0

ARUBA networks

Copyright

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (“GPL”), GNU Lesser General Public License (“LGPL”), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WEATHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY AND QUET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACUTALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURSHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Warning and Disclaimer

This guide is designed to provide information about wireless networking, which includes Aruba Network products. Though Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, this guide and the information in it is provided on an “as is” basis. Aruba assumes no liability or responsibility for any errors or omissions.

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY, AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice.

www.arubanetworks.com

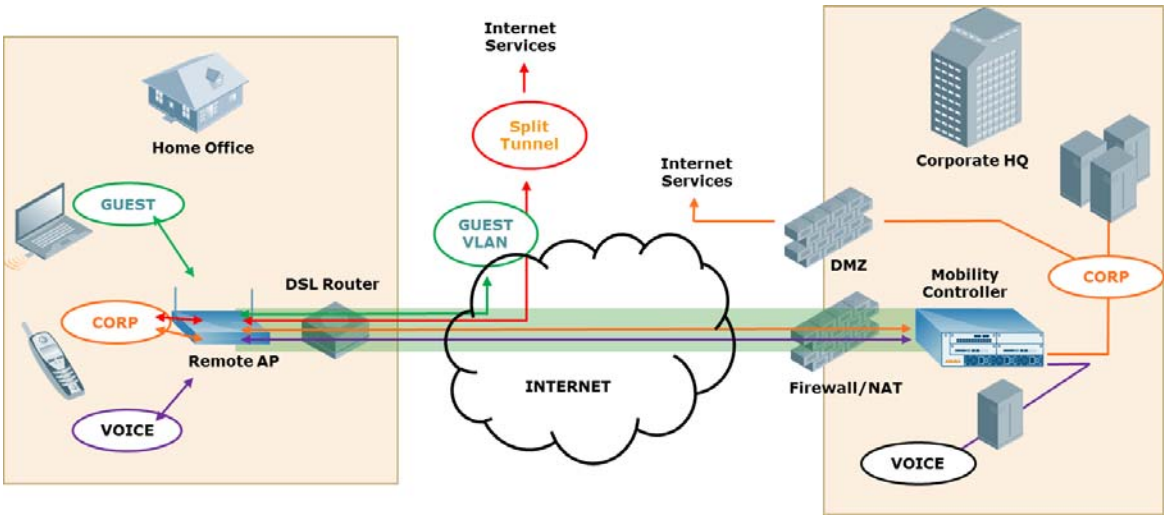
1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Table of Contents

Chapter 1: Introduction

This guide provides a brief description of the various bandwidth reservation and quality of service (QoS) options for supporting voice traffic in an Aruba remote access point (RAP) telecommuter deployment scenario. The Aruba remote access point (RAP) solution is a key component of the Aruba virtual branch network (VBN) architecture. The Aruba RAP deployment model meets the needs of fixed telecommuter and small branch office deployments while maintaining simplicity and ease of deployment. Aruba RAPs extend the corporate LAN to any remote location by enabling seamless wired or wireless data and voice wherever a user finds an Internet-enabled Ethernet port or 3G cellular connection. RAPs are ideally suited for small remote offices, home offices, telecommuters, mobile executives, and for business continuity applications.



Organizations with many fixed telecommuters typically have a requirement to extend a fully functional secure wired or wireless footprint (or both) into the employee home. One of the main requirements is to deliver full voice services to off-premises wired phones. Aruba RAPs provide secure access for VoIP phones (wired and wireless) to securely connect to the corporate voice server with dynamic, integrated QoS and voice prioritization features.

Aruba RAPs can be deployed in different forwarding modes (tunnel, split-tunnel, and decrypt-tunnel) to support voice. These forwarding modes in combination with user-defined policies significantly impact the call quality and call characteristics for a given data flow. This guide provides a general recommendation with an overview of the options that are available for voice deployments with different the forwarding modes. These recommendations should always be used in combination with the Validated Reference Design Guides.

Table 1 lists the current software versions for this guide.

Table 1 Aruba Software Versions

Product	Version
ArubaOS™ (mobility controllers)	6.1
ArubaOS (mobility access switch)	7.0
Aruba Instant™	1.1
MeshOS	4.2
AirWave®	7.3
AmigopodOS	3.3

Reference Material

- This guide assumes a working knowledge of Aruba products. A more in-depth discussion for this topic can be found in the *Aruba Virtual Branch Networks VRD* and the *Base Designs Lab Setup for Validated Reference Design.* These guides are available for free 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 outside the scope of the VRD series. The Aruba support site is located at: https://support.arubanetworks.com/. This site requires a user login and is for current Aruba customers with support contracts.

Chapter 2: Best Practices for Voice Deployment at Remote Sites

Aruba remote access points (RAPs) can be deployed with tunnel, decrypt tunnel (decrypt-tunnel), split-tunnel, or bridge mode SSIDs. Refer to the Aruba *Virtual Branch Networks Validated Reference Design* for a more detailed discussion of these forwarding modes.

This section provides a high level description of the different forwarding modes and helps to clarify why a specific forwarding mode is recommended for voice deployments with RAP.

Tunnel or split-Tunnel are the recommended modes for deploying RAPs where voice is a requirement. The description for bridge forwarding mode is provided below for sake of completeness.

Remote Access Point Forwarding Modes

Tunnel Forwarding Mode

In tunnel forwarding mode, all the 802.11 wireless traffic is Layer 2 encrypted from the client to the RAP. Then that traffic is forwarded through the IPsec tunnel to the controller. (No Layer 3 IPsec encryption is needed for these packets because they are already Layer 2 encrypted). Traffic from the wired ports is Layer 3 encrypted because it is forwarded into the IPsec tunnel in tunnel forwarding mode.

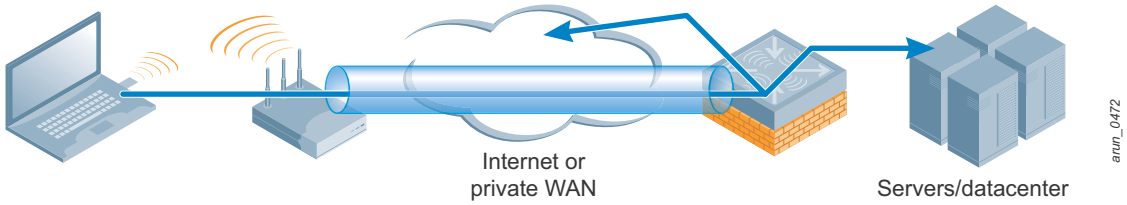


Figure 1 RAP in tunnel mode

Decrypt Tunnel Forwarding Mode

A decrypt tunnel mode SSID is similar to tunnel mode SSID where all the traffic is forwarded through a GRE tunnel to the controller. In decrypt tunnel mode, the wireless traffic is decrypted at the RAP, and then both wired and wireless traffic is forwarded to the controller with no encryption. The IPsec tunnel is configured such that the packets are AH encapsulated but are 'null' encrypted. This should only be considered when the RAP will connect over an existing VPN that provides QoS based queuing. In general, you should use either tunnel or split tunnel.

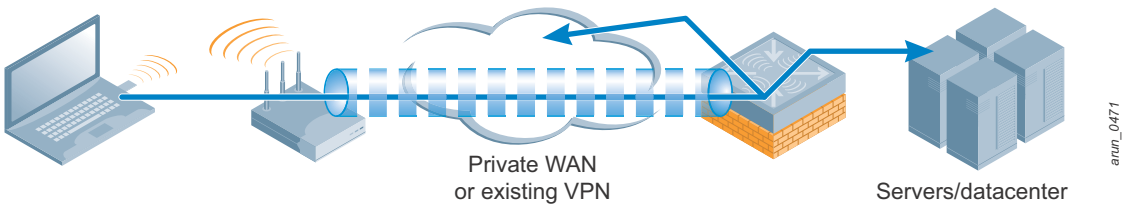


Figure 2 RAP in decrypt-tunnel mode

Decrypt tunnel mode is used when a VPN solution is already in place and if QoS is configured on the WAN facing router.

NOTE

Decrypt tunnel mode SSID should be used only when a VPN solution is already in place, otherwise all the traffic will be forwarded in the clear.

Split-Tunnel Forwarding Mode

In split-tunnel forwarding mode, the wireless traffic from the client to the AP is Layer 2 encrypted and decrypted on the RAP. Depending on the destination of the traffic (data center versus Internet) the traffic is then either Layer 3 re-encrypted and injected into the IPsec tunnel to forward to the controller or it is bridged locally. Traffic from wired phones is also Layer 3 encrypted on the RAP and injected into the IPsec tunnel. The Layer 3 encryption is done in hardware on the AP. Any other traffic is forwarded to the Internet or is locally switched according to the configured policies.

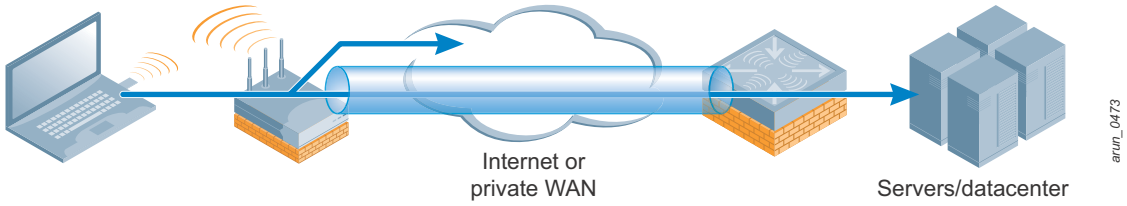


Figure 3 RAP in split-tunnel mode

Bridge Forwarding Mode

In bridge mode SSID, all the user traffic is locally bridged and only the control traffic is IPsec encrypted and forwarded inside the tunnel to the controller.

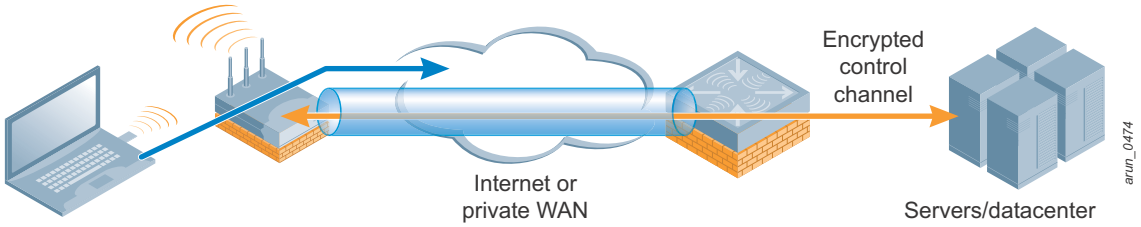


Figure 4 RAP in bridge mode

Voice Support in Different Forwarding Modes

The recommended deployment options for voice are split-tunnel, decrypt-tunnel, or tunnel mode. Bridge mode SSID is not a supported option because VoIP application-layer gateways (ALGs) are not supported in bridge mode. Additionally, in bridge mode, the user traffic is not tunneled back to the corporate headquarters or data center, so this topology will not work if the PBX is centralized.

A single SSID is generally recommended for both voice and data. However, a separate voice SSID in tunnel or decrypt-tunnel mode can also be created if mandated by the customer's security requirements.

The call voice quality is affected by loss, latency, and jitter. Loss causes dropped conversations and clipping. Latency causes delays in packet delivery and jitter is a variation of packet delay and occurs when voice packets are sent and received with timing variations. The section below describes Aruba's ALGs and the different settings that can be used to maintain the voice call quality in a RAP deployment.

Aruba Voice Manager

Aruba controllers have a built-in voice manager module that manages the voice ALG functions and the ALG functions. These ALGs are stateful (bi-directional). All ALGs operate in the control path and provide for deep packet inspection capability. For example, the voice ALG detects Session Initiation Protocol (SIP) packets and opens up the necessary ports (such as 5060) for voice traffic. The deep packet inspection and the dynamic port selections are a secure way of allowing only traffic that is intended to pass through.

ArubaOS on the Aruba controller supports ALGs for SIP, H323, Skinny Call Control Protocol (SCCP) or Skinny, Alcatel New Office Environment (NOE), Vocera, and Polycom SpectraLink Voice Protocol (SVP). The Aruba controller requires slightly different configurations for SIP and SVP (Polycom phones).

In addition to deep packet inspection, the voice manager on the controller also performs these tasks:

- Performs voice prioritization without any ACLs. (No manual creation of ACLs is performed and manual setting TOS values in the ACLs is not required).
- Automatically collects call statistics such as MOS, delay, latency, and CDR records for the voice calls.

Codecs

Codecs are used to convert an analog voice signal to a digitally encoded version and can also affect the quality of the voice call. Codecs vary in things like the sound quality, the bandwidth required, and the computational requirements. Each service, program, phone, or gateway typically supports several different codecs, and when they talk to each other, they negotiate which codec they will use.

- Using G.711 for VoIP provides the best voice quality and has the lowest latency. The downside is that G.711 takes more bandwidth then other codecs - approximately 87.2 Kb/s. However, with increasing broadband bandwidth, this may not be a major issue. G.711 is supported by most VoIP providers.
- G729 offers toll-quality speech at a reasonably low bit rate of 8 Kb/s and utilizes a bandwidth of 31.2 Kb/s. However, it is a more complex codec in terms of CPU processing time.

Bandwidth calculations for these codecs are described in Appendix A: VoIP Per-Call Bandwidth Calculations on page 17.

Aruba ALG-Lite

ALG-Lite is a module on the RAP that sends session add, session delete, and client identity messages from the RAP to the controller. ALG-Lite is a mechanism by which the signaling frames are forwarded to the main ALG module implemented on the controller. ALG-Lite is supported in split-tunnel mode but not in tunnel mode, and it does not need any configuration. All message processing happens in the main ALG on the controller.

ALG-Lite on the RAP does not do deep inspection of signaling messages because in most deployments the PBX sits in corporate network. Instead, this inspection happens on controller. For remote devices, signaling traffic reaches the controller and controller forwards this traffic to the control plane for deep inspection. The voice manager on the controller keeps track of local and remote devices.

Real Time Transport Protocol (RTP) defines a standard packet format for delivering audio and video over the Internet. RTP is defined in RFC 1889. Real Time Transport Control Protocol (RTCP) is defined in RFC 3550. RTP delivers the actual data and RTCP sends control packets to participants in a call to provide feedback on the quality of service being provided by RTP. For local devices, ALG-Lite opens ports for RTP/RTCP traffic in the controller data path. For remote devices, ALG-Lite opens ports in the controller data path and the AP data path. ALG-Lite is used to send these messages from the controller to the RAP.

Call Admission Control for Voice

Call Admission Control (CAC) can be configured on the controller. In general, CAC ensures good call quality for existing calls by not accepting any new calls if the system is overloaded. CAC is also useful in load balancing the calls between RAPs in a multi-RAP deployment. The controller has an overall view of all the voice sessions on the RAPs that are connected to it. If a RAP is overloaded with devices, it will not respond to the probes of the new device and the device moves to another RAP. The bandwidth calculator wizard on the controller helps the administrator to calculate the bandwidth requirements for different voice codecs and help in configuring CAC. CAC can be configured on the controller with the VoIP Call Admission Control profile and attached to an AP group**.** (**Advanced Services > All Profile Management > QoS Profile > VoIP Call Admission Control profile**)

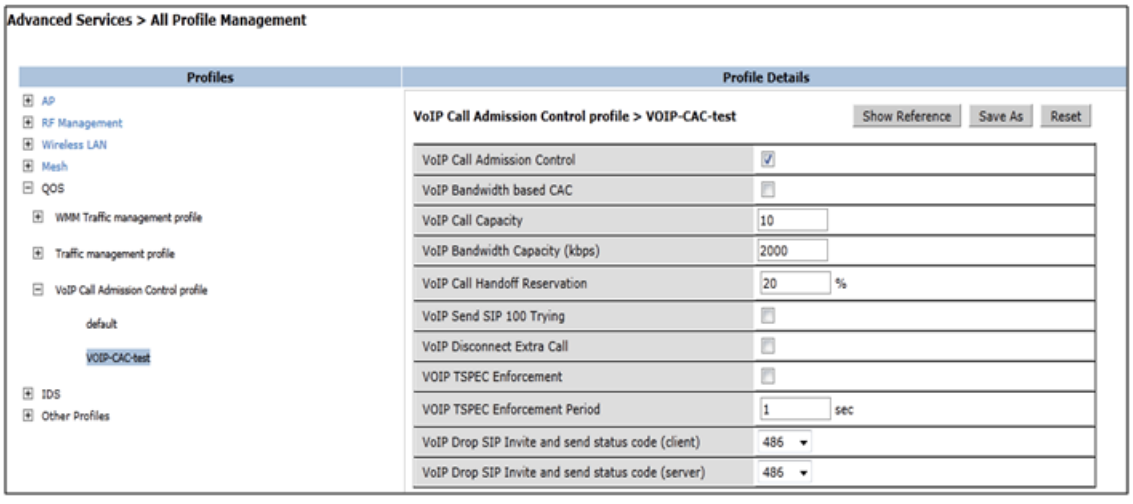


Figure 5 Configuring VoIP CAC

RAP Uplink Bandwidth Reservation

RAP uplink bandwidth reservation (UBR) configured in the AP system profile, allows an administrator to reserve a part of total uplink bandwidth on a RAP for a specific application, protocol, or port number. The UBR configured in the AP system profile of an AP group will apply to all RAPs that belong to this AP group. RAP uplink bandwidth reservation is supported in the split-tunnel mode and bridge mode SSIDs for wired and wireless traffic.

Bandwidth allocation requires the access control list (ACL) mechanism where session ACLs are used to identify the traffic. With the configuration of an ACL that prioritizes a voice subnet, the bandwidth allocation can reserve a portion on the uplink (to WAN) bandwidth for the traffic from the voice subnet. Before configuring any class of traffic for reservation to limit the traffic leaving RAP uplink, the administrator must know the available Internet uplink bandwidth. The uplink bandwidth reservation module is independent of the ALG.

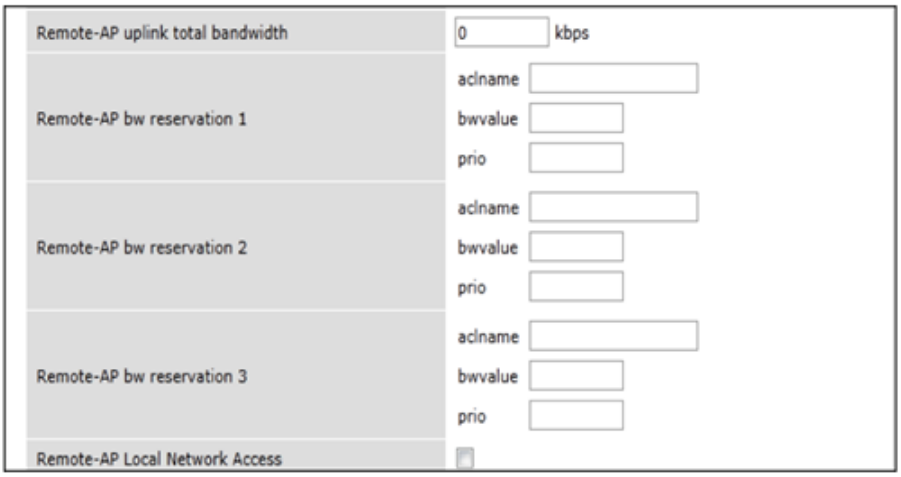


Figure 6 Configuring RAP uplink bandwidth reservation

WMM

Wi-Fi Multimedia™ (WMM®), also known as Wireless Multimedia Extensions (WME), is a Wi-Fi Alliance® interoperability certification based on the IEEE 802.11e standard. WMM provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four access categories: voice, video, best effort, and background. However, WMM does not provide guaranteed throughput. WMM is suitable for simple applications that require QoS such as VoIP on Wi-Fi phones (VoWLAN).

Type of service (ToS) and Diff-Serve Code Points (DSCP) are fields that the IP layer uses for QoS. These fields are used to mark types of traffic, for example, DSCP 46 for RTP (VoIP) or DSCP 26 for SIP (VoIP signaling). Marked packets are put into queues to apply QoS and prioritization over other kind of traffic, like email or web traffic.

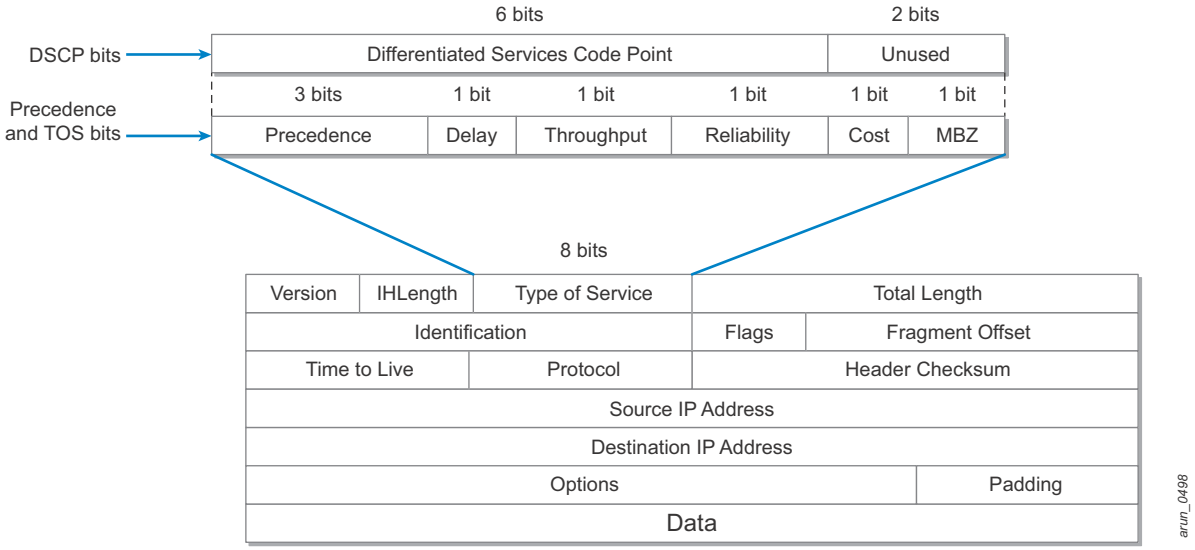


Figure 7 IP packet – TOS and DSCP bits

The 802.1p protocol is a subset of 802.1Q and operates at Layer 2. The .1p tag is used by .1Q (VLANs) to prioritize traffic according to the kind of VLANs. For example, if VLAN 100 is used for VoIP telephones, the 802.1p tag can be set to category number 4 (voice), so that intermediate devices (routers, switches, controllers) use the 802.1p field to select which VLAN traffic should be prioritized. Most VoIP phones automatically tag their traffic, for example, 802.1p=5 for voice at Layer 2 and DSCP=46 for RTP VoIP at Layer 3.

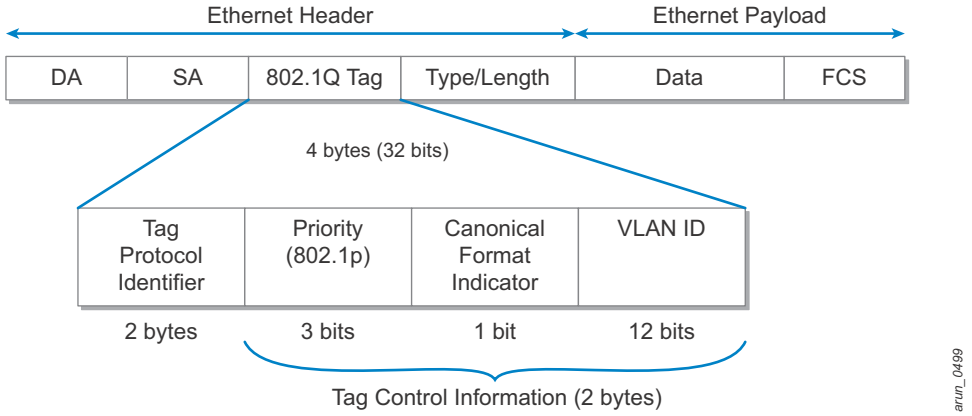


Figure 8 Ethernet data frame and 802.1p tagging

The Aruba WMM implementation is according to the standards, where 802.1p markings are converted to DSCP markings upstream and downstream on the RAP. 802.1p markings are also placed in the 802.1Q VLAN tag. It is important to ensure that all tags, .1p, DSCP, and WMM access categories, match in the upstream and downstream directions, and also across wired and wireless networks.

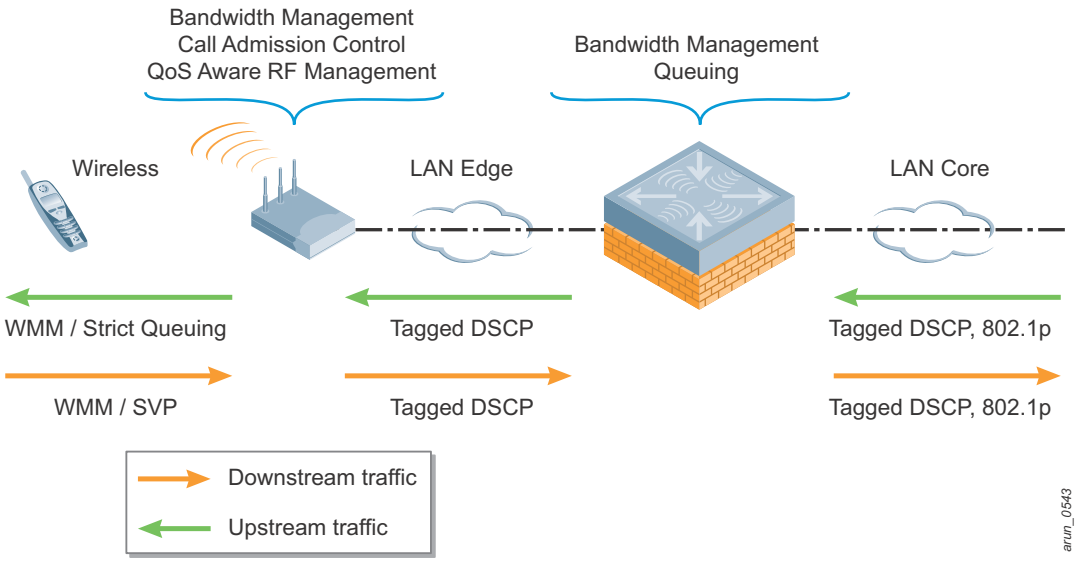


Figure 9 End-to-End QoS Support

Per-User Bandwidth Contracts

Bandwidth management is another QoS mechanism that helps ensure adequate bandwidth for user traffic. The per-user bandwidth contract ensures that no single user can access more than the bandwidth defined by the contract.

Per-user bandwidth contracts can be configured on a per-user basis or on a per-role basis. When configured on a per-role basis, the total configured bandwidth is shared among all devices that inherit that role. A bandwidth contract that is configured per-role is shared among all devices in that role. When configured on a per-user basis, the configured bandwidth is available for each user in that role. For example, a 2 Mb/s bandwidth contract per-user means that 2 Mb/s is available for each user in that role. The bandwidth contracts are effective only for traffic from RAP to controller or controller to RAP.

In addition to these configurations, any voice deployment also depends on the location of the PBX or SIP server. In split-tunnel mode, when the “Remote-AP Local Network Access” parameter is checked in the AP system profile, calls between voice devices on the same RAP are switched locally. The call statistics for these calls continue to be sent to the controller over the control channel (secure tunnel).

Airtime Fairness

Airtime fairness for traffic from the RAP to the client (downstream direction) does not apply to voice traffic because voice traffic has the highest priority. The voice session bypasses the airtime fairness algorithm completely because voice frames have strict priority into the hardware queue.

Airtime fairness has the added benefit in most cases that the channel is less busy when fair access is enabled, which should facilitate smoother or better quality voice deployments. Airtime Fairness works for tunnel mode SSID and the general recommendation is to enable fair access for such deployments.

Airtime fairness is configured in the QOS profile. (Advanced Services > All Profile Management > QoS Profile > Traffic management Profile > Station Shaping Policy)

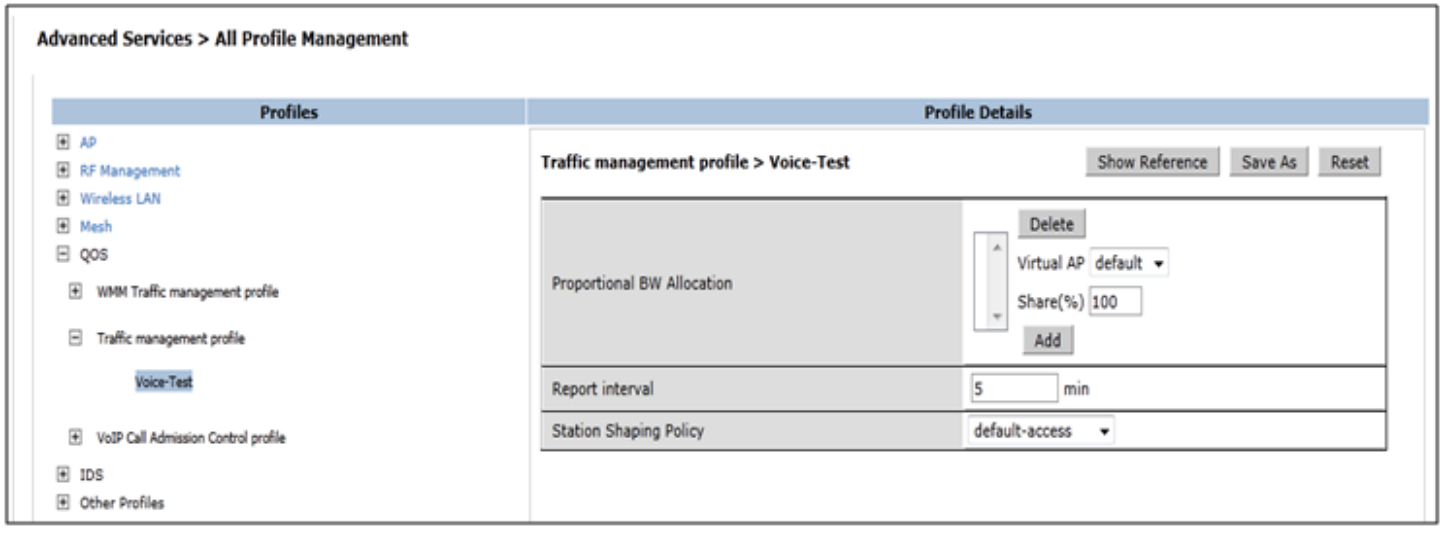


Figure 10 Configuring Airtime Fairness

Summary

Other parameters are not under the control of the wireless network, such as the WAN latency. The scale and performance of the routing and switching of the core network are also not under the control of the wireless network. Table 2 summarizes the points that have been discussed in the earlier sections.

Table 2 RAP Forwarding Modes and Voice QoS Support

Feature	RAP Forwarding Modes		
	Tunnel Mode	Split-Tunnel Mode	Decrypt-Tunnel Mode
Call Admission Control	Yes	Yes	Yes
WMM	Yes	Yes	Yes
Per User Bandwidth Contracts	Yes	Yes	Yes
RAP Uplink Bandwidth Reservation	No	Yes	No
Voice ALGs on Controller	Yes	Yes	Yes
ALG-Lite on RAP	No	Yes	No
Voice call statistics (MOS, latency)	Yes	Yes	Yes
Airtime Fairness	Yes	No	Yes
Mobility (Layer 2 Roaming)	Yes	No	Yes

Figure 11 summarizes the design recommendations based on general requirements for deployment.

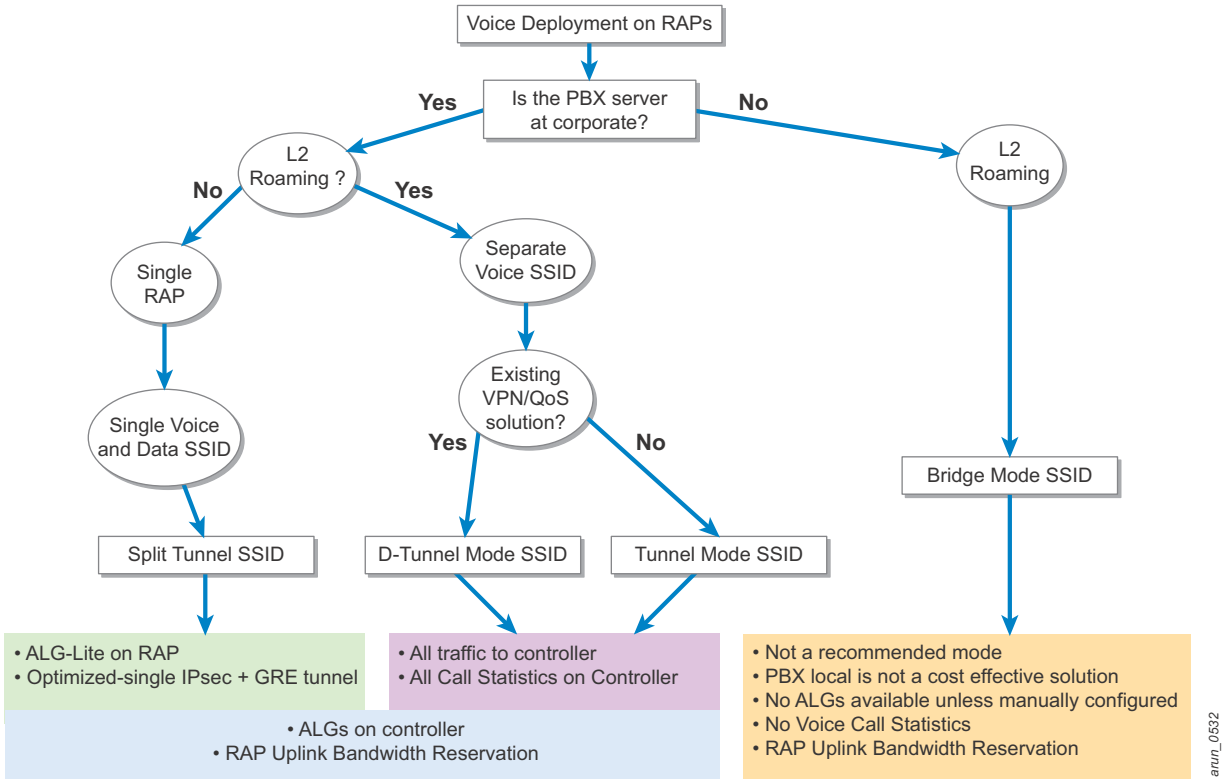


Figure 11 Deployment options for RAP and Voice

Appendix A: VoIP Per-Call Bandwidth Calculations

This appendix explains voice codec bandwidth calculations and shows the different protocol header sizes that are used for the calculations:

Bandwidth Calculation Formulas

total packet size = (Layer 2 header) + (IP/UDP/RTP header) + (voice payload size)

packets per second (PPS) = (codec bit rate) ÷ (voice payload size)

bandwidth = total packet size * PPS

Layer 2 header can be Multilink Point-to-Point Protocol (MP), Frame Relay Forum (FRF), or Ethernet.

The approximate protocol header sizes used in these calculations are as follows:

- 40 bytes for IP (20 bytes) / User Datagram Protocol (UDP) (8 bytes) / Real-Time Transport Protocol (RTP) (12 bytes)
- Compressed Real-Time Transport Protocol (cRTP) reduces the IP/UDP/RTP headers to 2 or 4 bytes (cRTP is not available over Ethernet).
- 6 bytes Layer 2 Header for MP or FRF
- 1 byte for the end-of-frame flag on MP and Frame Relay frames
- 18 bytes for Ethernet Layer 2 headers, including 4 bytes of Frame Check Sequence (FCS) or Cyclic Redundancy Check (CRC)

Sample Bandwidth Calculation for G.711 and for G.729

The required bandwidth for a G.711 call (64 Kb/s codec bit rate) with Ethernet L2 header and the default 160 bytes of voice payload is:

- total packet size (bytes) = (18 bytes Ethernet Layer 2 header) + (40 bytes IP) + (voice payload of 160 bytes) = 218 bytes
- total packet size (bits) = (218 bytes) * 8 bits per byte = 1744 bits
- voice payload size = (160 bytes default voice payload) * 8 bits per byte = 1280 bits
- packets per second (PPS) = (64 Kb/s codec bit rate) ÷ (1280 bits) = 50 pps
- bandwidth per call = (1744 bits voice packet size) * 50 pps = 87.2 Kb/s

The required bandwidth for a G.729 call (8 Kb/s codec bit rate) with cRTP, MP and the default 20 bytes of voice payload is:

- total packet size (bytes) = (18 bytes Ethernet Layer 2 header) + (40 bytes IP) + (voice payload of 20 bytes) = 78 bytes
- total packet size (bits) = (78 bytes) * 8 bits per byte = 624 bits
- voice payload size = (20 bytes default voice payload) * 8 bits per byte = 160 bits
- PPS = (8 Kb/s Codec bit rate) ÷ (160 bits) = 50 pps
- bandwidth per call = (624 bits voice packet size) * 50 pps = 31.2 Kb/s

Appendix B: Contacting Aruba Networks

Contacting Aruba Networks

Web Site Support	
Main Site	http://www.arubanetworks.com
Support Site	https://support.arubanetworks.com
Software Licensing Site	https://licensing.arubanetworks.com/login.php
Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Validated Reference Design Contact and User Forum	
Validated Reference Designs	http://www.arubanetworks.com/vrd
VRD Contact Email	referencedesign@arubanetworks.com
AirHeads Online User Forum	http://airheads.arubanetworks.com

Telephone Support	
Aruba Corporate	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support	
• United States	+1-800-WI-FI-LAN (800-943-4526)
• Universal Free Phone Service Numbers (UIFN):	
▪ Australia	Reach: 1300 4 ARUBA (27822)
▪ United States	1 800 9434526 1 650 3856589
▪ Canada	1 800 9434526 1 650 3856589
▪ United Kingdom	BT: 0 825 494 34526 MCL: 0 825 494 34526

Telephone Support

● Universal Free Phone Service Numbers (UIFN):	
■ Japan	IDC: 10 810 494 34526 * Select fixed phones IDC: 0061 010 812 494 34526 * Any fixed, mobile & payphone KDD: 10 813 494 34526 * Select fixed phones JT: 10 815 494 34526 * Select fixed phones JT: 0041 010 816 494 34526 * Any fixed, mobile & payphone
■ Korea	DACOM: 2 819 494 34526 KT: 1 820 494 34526 ONSE: 8 821 494 34526
■ Singapore	Singapore Telecom: 1 822 494 34526
■ Taiwan (U)	CHT-I: 0 824 494 34526
■ Belgium	Belgacom: 0 827 494 34526
■ Israel	Bezeq: 14 807 494 34526 Barack ITC: 13 808 494 34526
■ Ireland	EIRCOM: 0 806 494 34526
■ Hong Kong	HKTI: 1 805 494 34526
■ Germany	Deutsche Telkom: 0 804 494 34526
■ France	France Telecom: 0 803 494 34526
■ China (P)	China Telecom South: 0 801 494 34526 China Netcom Group: 0 802 494 34526
■ Saudi Arabia	800 8445708
■ UAE	800 04416077
■ Egypt	2510-0200 8885177267 * within Cairo 02-2510-0200 8885177267 * outside Cairo
■ India	91 044 66768150